
ИНСТРУМЕНТАРИЙ
ХАКЕРА
С. А. Бабин
Примеры взлома
Атаки на Wi-Fi
Кража паролей в социальных сетях
Бесплатные программы
Хакинг без специальных средств
Защита от хакеров
bhv

С. А. Бабин

ИНСТРУМЕНТАРИЙ ХАКЕРА

Санкт-Петербург
«БХВ-Петербург»
2014

УДК 004
ББК 32.973.26-018.2
Б12

Бабин С. А.

Б12 Инструментарий хакера. — СПб.: БХВ-Петербург, 2014. — 240 с.: ил. — (Глазами хакера)

ISBN 978-5-9775-3314-0

Оригинальное изложение материала позволит читателю понять методы обеспечения защиты информации как на личных компьютерах, так и в профессиональных системах. Описаны основные принципы подбора инструментария хакера. Приведено множество примеров взлома и сокрытия следов: перехват паролей, атаки на Wi-Fi-роутеры, подмена MAC-адресов, способы оставаться невидимым в Интернете. В противовес злоумышленнику описаны методы защиты с помощью соответствующих программных инструментов. Даны рекомендации, как поступать, чтобы не лишиться своих денег при дистанционном банковском обслуживании.

Книга может быть использована в качестве практического руководства для начальной подготовки специалистов информационной безопасности. За счет подробного описания настроек, качественной визуализации материала, преобладания ориентированности на Windows-системы (для примеров с Unix подробно описывается каждый шаг), она также будет интересна и понятна любому пользователю персонального компьютера: от старшеклассника и студента до профессионала.

Для пользователей ПК

УДК 004
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зав. редакцией	*Екатерина Капалыгина*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Марины Дамбиевой*

Подписано в печать 28.02.14.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 19,35.
Тираж 1500 экз. Заказ №
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

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

ISBN 978-5-9775-3314-0

Оглавление

Введение

Существует множество литературы о хакерах. Сразу оговоримся — речь идет о хакерах в плохом значении этого слова. Конечно же, все эти труды пишутся не для того, чтобы формировать новых, юных злоумышленников, тем более что сами хакеры, как правило, такие книги вовсе и не читают. Цель авторов такого рода литературы (как и наша тоже) совершенно в другом: дать возможность обычным пользователям и специалистам информационных технологий лучше узнать врага.

Проблема в том, что за редким исключением подобные труды насыщены немалым объемом теоретического материала. Конечно же, по большому счету это не является недостатком! Но, в действительности, зачастую, начинающему читателю книг по указанной тематике хочется скорее пощупать все своими руками, а уж потом подвести под все это стройную концепцию. Поэтому здесь мы постарались рассказать о формировании инструментов хакера фактически на одних практических примерах. Кроме того, есть смысл поговорить только о программном инструменте, как наиболее широко применяемом, не затрагивая обширную тему аппаратных и программно-аппаратных средств.

Формирование набора инструментов — процесс длительный, и обозримого конца у него нет. Нет и каких-либо четких ограничений: например, взять те или иные лучшие программы по рекомендованному списку, и все — хакер готов. В реальной жизни хакер совершенствуется все время, используя софт самых различных производителей, для самых разных операционных систем. Поэтому, поднимая столь обширную тему, мы только попытаемся на практических примерах показать методологию формирования такого набора для различных направлений его применения. Так или иначе, чтобы понять принципы формирования инструментального кейса хакера, нам придется рассмотреть примеры некоторых атак.

При изложении материала мы не будем придумывать собственной классификации инструментария хакера. Вряд ли это необходимо! Просто изложим материал так, как это любят пользователи: "включи и играй" (plug and play). Без излишнего теоретизирования...

Так как книга рассчитана в том числе и на большой круг начинающих специалистов, то в основном мы старались все примеры ориентировать на получившие наибольшее распространение в нашей стране — операционные системы Windows! В тех же местах, где не обошлось без упоминаний UNIX-систем, специально каждая команда, каждый пример разъяснены самым наиподробнейшим образом, так что их может выполнить любой.

Книга будет полезна всем: начиная от интересующегося старшеклассника, студента (причем любого факультета, даже не связанного с информационной безопасностью), каждого пользователя домашнего компьютера (в особенности, если он применяет систему "клиент — банк"), программиста (в том числе занимающегося обслуживанием компьютеров в различных фирмах) и заканчивая специалистами, связанными с областью защиты информации.

Даже бизнесмен, который применяет в своей практике компьютер, задействованный в дистанционном банковском обслуживании, найдет здесь все необходимое, что требуется сделать для того, чтобы у него элементарно не украли все нажитое непосильным трудом.

Автор выражает признательность Рудикову Андрею Викторовичу (г. Кемерово) и Колмогорову Виктору Геннадьевичу (г. Красноярск), оказавшим большую помощь в подготовке материалов книги.

ГЛАВА 1

Захват пароля с применением атаки ARP-spoofing, или почему так просто украсть пароль для входа в социальную сеть "ВКонтакте"

Очень часто важнейшей целью любого хакера является раскрытие чужого пароля. Поэтому, возможно, есть смысл в первую очередь рассказать о деятельности хакера именно в области взлома парольной защиты.

Во всех классических учебниках по информационной безопасности неоднократно отмечалось, что подход к обеспечению безопасности должен быть комплексным.

Можно строить высокий барьер от злоумышленника, применяя самые дорогие системы защиты, но при этом предоставив врагу лазейку, не то что бы с дырой в этом "заборе", а вообще — оставляя часть периметра без ограды! Обойди, и пожалуйста: бери что хочешь! Какой же тогда был смысл затрачивать людские и материальные ресурсы?!

Возьмем для примера политику одного из продвинутых зарубежных университетов — университета Индианаполиса (University of Indianapolis, **http://is.uindy.edu/policies/password.php**):

University of Indianapolis Password PolicyIntroduction

Passwords are an important part of computer security. They are the first and sometimes last line of defense against would be criminals. A poorly chosen password or mishandled password can result in a temporary denial of computer services, identity theft, theft of university services and even financial loss. Appropriate password security is necessary to protect the University's academic interactions, business and research.

This policy describes the requirements necessary for creating and maintaining password security on all UIndy Accounts.

Policy Statement

All network devices and accounts must be secured with appropriate username and passwords. Whenever possible, systems will use UIndy Accounts stored in a central directory. All UIndy Accounts, including those used by faculty, staff, students, contractors and partners of the University, must be properly secured using the methods described in the following sections of this document.

Creating a Strong Password

The University of Indianapolis requires strong passwords on all UIndy Accounts. The University defines strong passwords as passwords that will take a computer at least 6 months to try all possible combinations of the letters, numbers and special characters contained in your password. The following are characteristics of a strong password:

- contains lower case and upper case letters (a-z and A-Z)
- contains numbers as well as letters
- contains special characters such as: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- is at least eight characters in length
- is not a word in any dictionary, English or other
- is not based on any bit of personal information: pet names, birth date, street names, etc
- is not based on anything to do with the University of Indianapolis, UIndy, Hounds, etc

Password Change Frequency

The University of Indianapolis requires all passwords to be changed every six months. This reduces the likelihood of the password being discovered and reduces the length of time a compromised account can be unknowingly used for criminal activity.

Password Storage

Choose passwords that are easy to remember so that it is not necessary to write it on any piece of paper. A password that is written on a sticky note attached to the bottom of the keyboard is as good as no password at all.

Password Confidentiality

Never tell another person your password. Your password should be kept completely confidential. Supervisors, coworkers, friends and family should never know your password. Likewise, it is inappropriate to ask another user for their password. If a person demands your password, refer the person to this document and/or contact the Office of the Chief Information Officer.

Periodic Scans

University of Indianapolis Information Systems will periodically employ password cracking techniques to determine the effectiveness of this password policy. Any passwords found to be weak during these scans will be immediately changed and the user notified.

Encryption

All University computer systems will store passwords in an encrypted form. As such, the Information Systems Help Desk cannot see or retrieve a password, only assist users in changing to a new password.

Compromised Accounts

If you suspect that a UIndy account has been compromised, report it to the Information Systems Help Desk immediately. Accounts that have been compromised will immediately have their password changed to prevent further losses.

Все вроде бы у них предусмотрено: и пароли сложные, и меняются они регулярно, и университет обязуется применять различные меры для обеспечения сохранности паролей.

Но, к сожалению, нет одной маленькой детали: запрета применять одни и те же пароли в разных системах.

В противоположность рассмотренному примеру приведем цитату из политики одной российской:

...

4.1.1. Строго запрещается использовать одинаковые пароли от учетных записей организации для любых ресурсов, за пределами компании (например: форумы, провайдеры, Internet-магазины).

4.1.2. В тех случаях, когда ресурс не поддерживает единую корпоративную систему авторизации (например, системы сторонних разработчиков, порталы для обучения), выбирайте пароли, отличные от пароля учетной записи компании.

...

Попробуем доказать сказанное. Предположим, что на небольшом предприятии имеется "продвинутый", хорошо обученный администратор сети. Все компьютеры защищены от несанкционированного доступа, как применением грамотно настроенных политик операционной системы, так и, казалось бы, "правильными" организационными мерами.

За исключением одного: администратор — тоже человек, и в действительности существо слабое (хотя, как правило, и самоуверенное). Поэтому он использует в разных системах один и тот же пароль. И для администрирования сети, и для личной почты, и в социальных сетях — везде, где только можно!

Если злоумышленник (или просто коллега по работе, но с меньшими правами) завладеет паролем на его почту, то получит доступ к самому важному: к ресурсам сети, которую администрирует наш незадачливый специалист.

В арсенале хакера есть тысяча и один способ как добыть пароль. Рассмотрим простейший пример получения почтового пароля, используя уязвимость IP-протокола версии 4, так называемую атаку ARP-spoofing!

Для начала вспомним, что ARP (Address Resolution Protocol, протокол определения адреса) применяется для динамического сопоставления IP-адресов аппаратным, т. е. физическим адресам, а именно тем адресам, которые используются во время работы сетевой картой. Физические адреса еще называют MAC-адресами.

Сейчас мы не будем выяснять, зачем и как это делается. Отметим только, что эффективность работы этого протокола зависит от ARP-кэша (ARP cache).

Для лучшего восприятия представим себе табличку соответствия IP- и физических адресов сетевых карт, которые применяются в каком-то сегменте сети. Время жизни записей в этой табличке ограничено, и их обновление производится в том числе с применением протокола ARP (если быть уж совершенно точным, есть еще обратный ARP, или RARP — reverse address resolution protocol, обратный протокол преобразования адреса).

Протокол ARP достаточно простой, и когда он был придуман, то особой его защиты предусмотрено не было. Идея атаки, о которой идет речь, заключается в следующем: чтобы атакующему переключить весь сетевой трафик между двумя хостами А и Б через себя, необходимо в кэш-таблицы этих хостов внести свои изменения, ввести их в заблуждение:

1. Хосту А сообщить , что IP-адрес хоста Б соответствует физическому адресу атакующего хоста.
2. Хосту Б сообщить, что IP-адрес хоста А соответствует физическому адресу атакующего хоста.

Таким образом, атакующий встает посередине между жертвами (атака man-in-the-middle), чтобы те ничего не заметили, даже не остановив трафика, замкнув его через себя. Остается только включить сниффер и анализировать трафик. Тем более что зачастую пароли даже не шифруются.

Для практики 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.

Устанавливаем на атакующем компьютере свободно распространяемую в Интернете замечательную программу Cain & Abel (Каин и Авель). Для того

чтобы в комплекте с программой работал сниффер, при инсталляции соглашаемся на установку входящей в комплект также свободно распространяемой программы Winpcap.

Примечание

На всякий случай отключим антивирусную программу и брандмауэры!

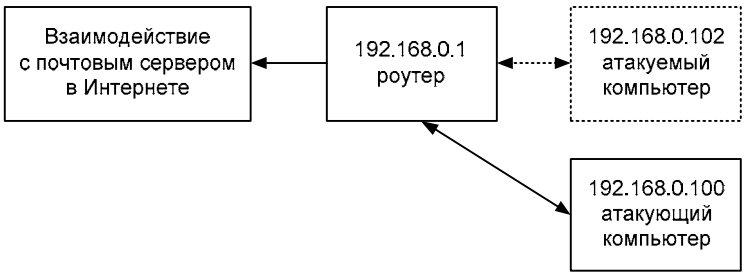

Рис. 1.1

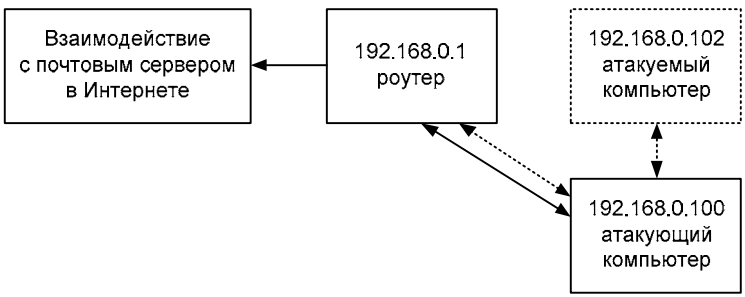

Рис. 1.2

Настраиваем сниффер 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 на значке 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 на значке большого плюса (+) на панели инструментов программы (рис. 1.5).

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

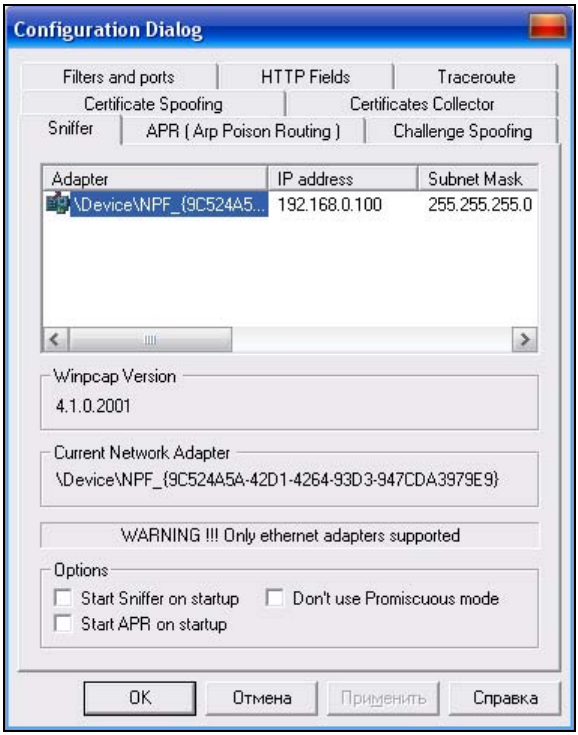
Configuration Dialog
Filters and ports
HTTP Fields
Traceroute
Certificate Spoofing
Certificates Collector
Sniffer
APR (Arp Poison Routing)
Challenge Spoofing
Adapter
IP address
Subnet Mask
\Device\NPF_{9C524A5...
192.168.0.100
255.255.255.0
Winpcap Version
4.1.0.2001
Current Network Adapter
\Device\NPF_{9C524A5A-42D1-4264-93D3-947CDA3979E9}
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

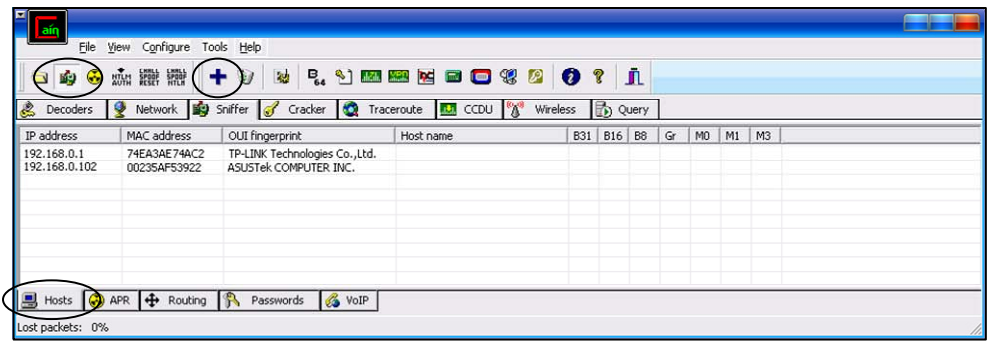
File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
IP address
MAC address
OUI fingerprint
Host name
B31
B16
B8
Gr
M0
M1
M3
192.168.0.1
74EA3AE74AC2
TP-LINK Technologies Co.,Ltd.
192.168.0.102
00235AF53922
ASUSTek COMPUTER INC.
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

Рис. 1.4

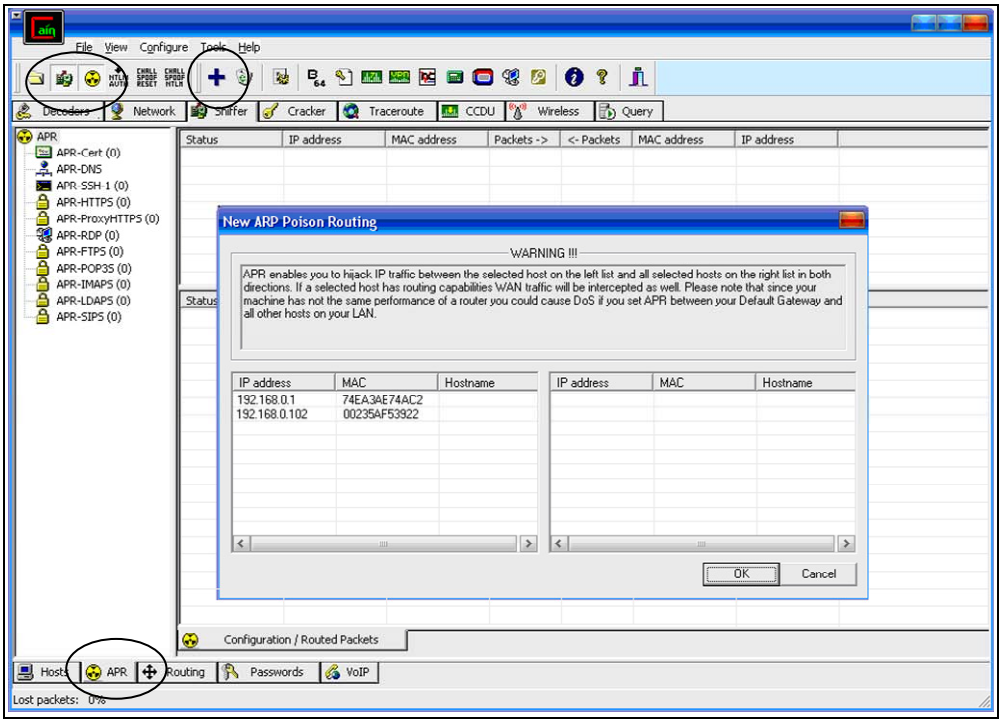
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (0)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
IP address
MAC address
Packets ->
<- Packets
MAC address
IP address
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
OK
Cancel
Configuration / Routed Packets
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

Рис. 1.5

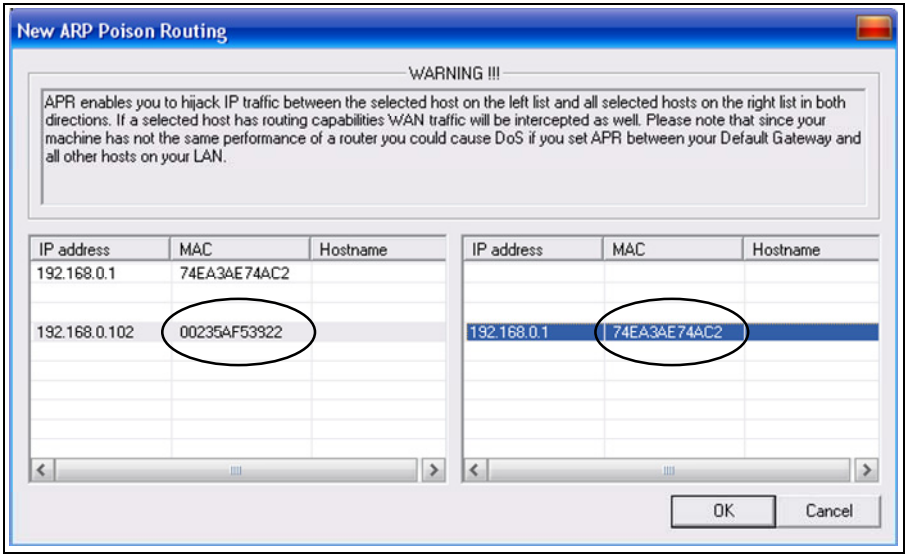
New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has 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
192.168.0.1
74EA3AE74AC2
OK
Cancel

Рис. 1.6

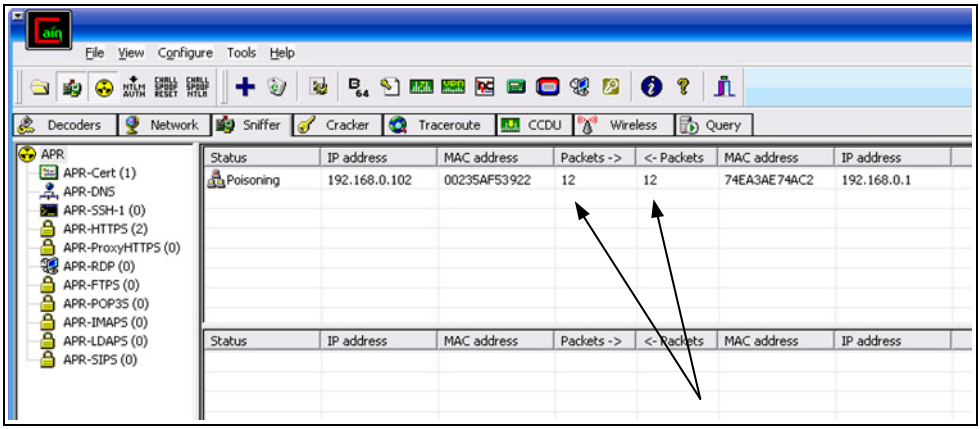

Рис. 1.7

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. В нашем случае, для проверки мы произведем вход на сервер **www.mail.ru**, используя учетную запись для адреса **babins@inbox.ru** с паролем arptest. Причем, вход осуществим по протоколу http с применением стандартного браузера (рис. 1.8).

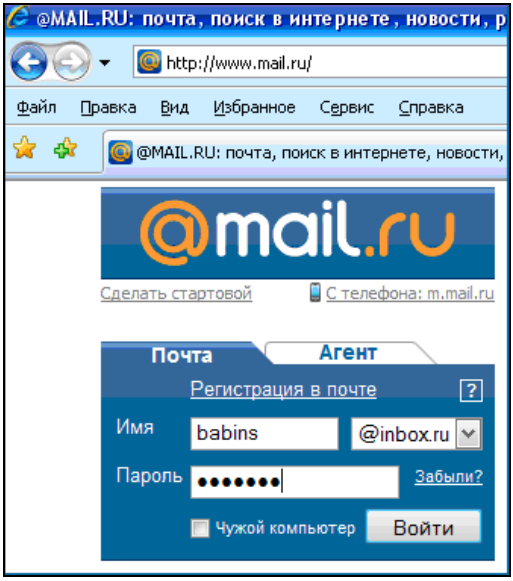

Рис. 1.8

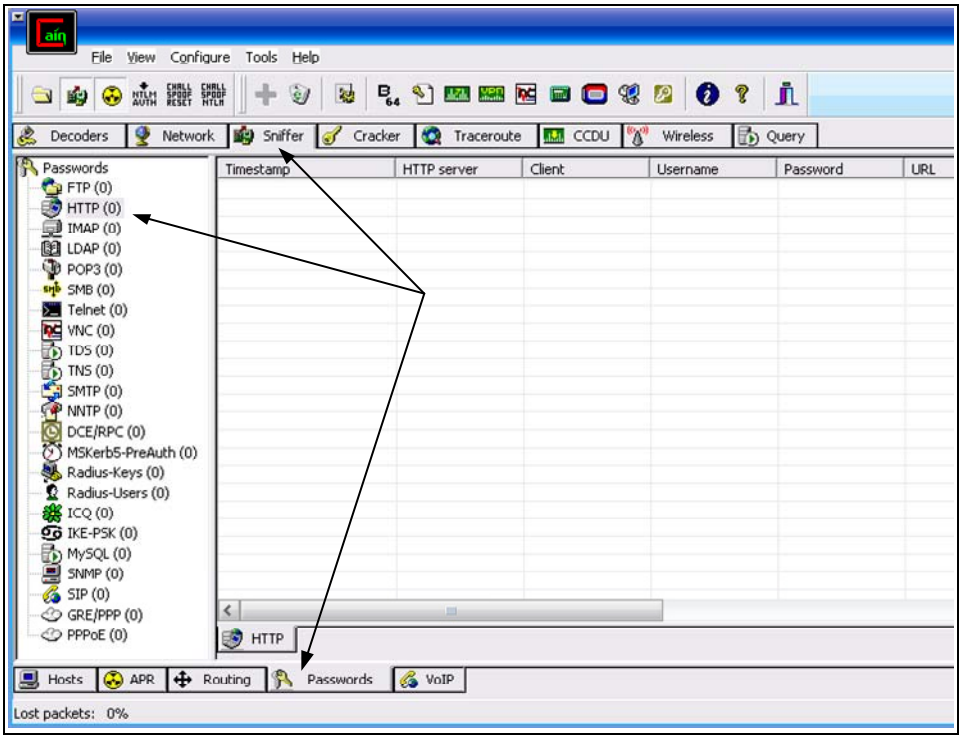

Рис. 1.9

Соответственно, искомый результат будем "ожидать" в разделе **HTTP | Password** вкладки **Sniffer** программы Cain & Abel (рис. 1.9).

Если бы с атакуемого компьютера почту брали каким-нибудь специализированным почтовым клиентом, то результат необходимо было ожидать уже в разделе соответствующему 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 и ожидаемый нами пароль arptest (рис. 1.10).

Таким образом, находясь в одном сегменте сети с жертвой, потенциальный хакер может полностью перехватывать нешифрованный трафик с атакуемого компьютера.

Мы доказали главное: использовать одинаковые пароли в различных системах весьма опасно. Перехватив пароль в более уязвимых системах, таким образом можно получить доступ и к более защищенным.

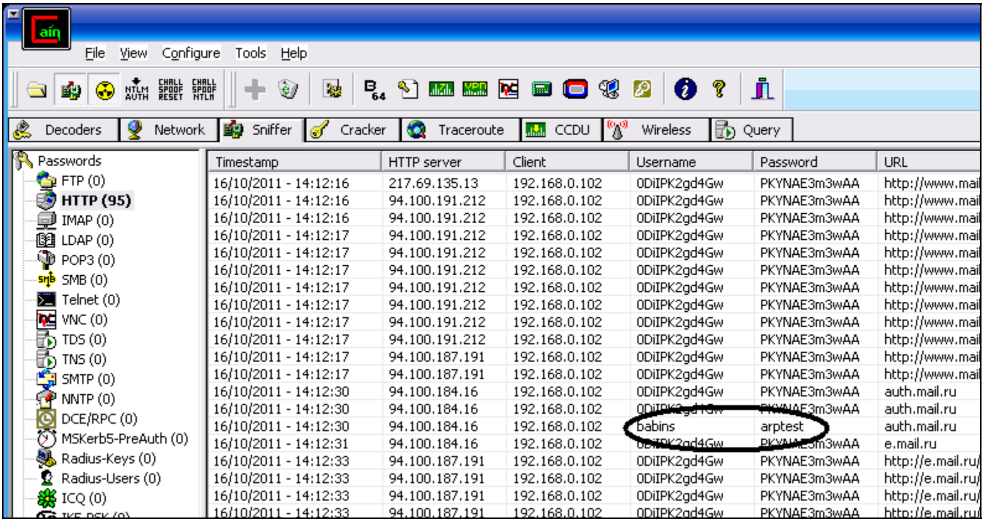

Рис. 1.10

В отношении рассматриваемого примера, хотелось бы еще добавить, что если авторизация жертвы на сайте почтового сервера происходит с поддержкой протокола SSL, т. е. с шифрованием, то нужно очень постараться, чтобы получить пароль.

И, если предположить, что, к примеру, в любимой школьниками социальной сети "ВКонтакте" (да и в любой другой) все же когда-то при авторизации будет применяться шифрованное соединение, то украсть этот пароль все равно очень просто. Причина — девяносто девять процентов пользователей использует одинаковые пароли: что в почте, что "ВКонтакте"...

Отметим также, что для проведения атаки ARP-spoofing можно применять и другие инструменты! Например, в этих целях хорошо подходит программа Iptools (автор — Эрван Л. (Erwan L.)). Правда, пароли в ней перехватываются не в автоматическом режиме, как это мы делали в программе Cain & Abel, а вручную, с помощью поиска в лог-файлах сниффера. Но, об этой программе мы расскажем несколько позже.

В рамках этой темы нельзя не упомянуть еще об одном замечательном бесплатном сниффере, имеющем большое количество функций и широко используемом хакерами. Это известная программа Wireshark (рис. 1.11, **http://www.wireshark.org**).

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 нахо-

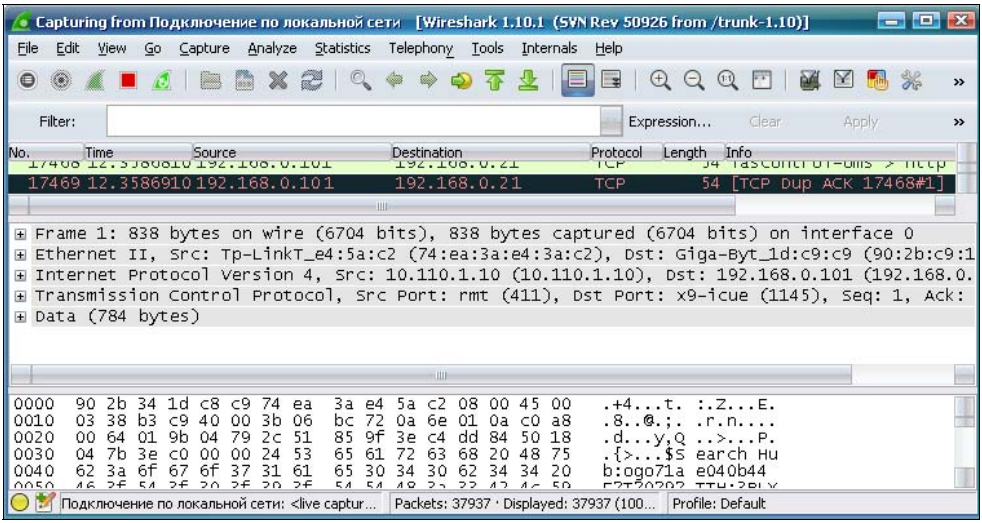

Рис. 1.11

дится в открытом доступе. Про все возможности этого сетевого анализатора протокола можно написать отдельную книгу.

А теперь приготовьтесь к еще более страшному открытию! Если хакер получил физический доступ к вашему компьютеру... — да даже не хакер, а просто ваш знакомый — то всё! У вас больше никаких секретов! А знаете, почему? Все ваши пароли в социальных сетях "Одноклассники", "ВКонтакте", для доступа к почте — куда угодно — увидит простенькая программка под на-

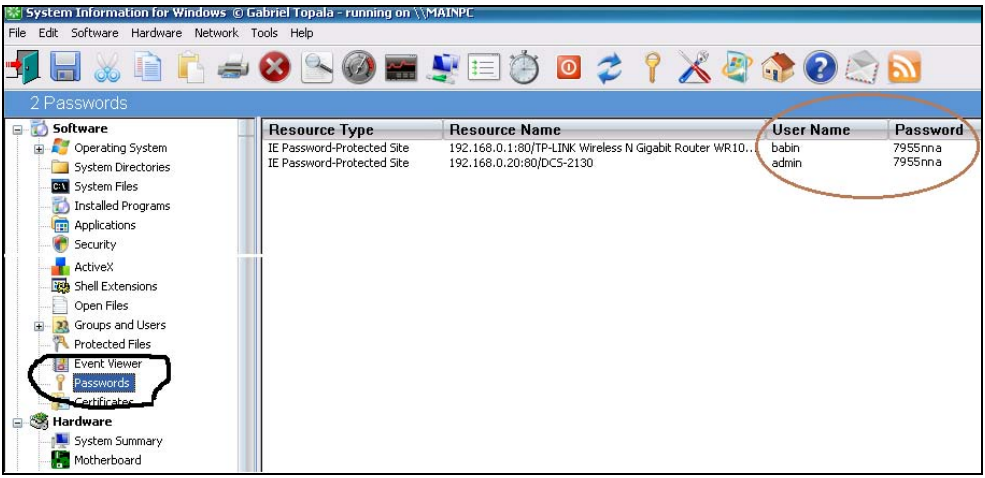

Рис. 1.12

званием SIW (System Information for Windows), которая может, например, считать анализировать cookies-файлы, а также кэши работы программ, для считывания имен и паролей, посещаемых вами сайтов (небольшие файлы, представляющие собой что-то типа идентификационной карточки пользователя) — рис. 1.12.

На этом можно было бы и закончить эту главу: т. к. от безысходности, что есть такие программы, как SIW (только нужна коммерческая версия), просто нет сил что-то еще комментировать... Получается, что безопасности нет, не было, и не будет?! Если это так, то обидно, конечно!..

ГЛАВА 2

Следы пребывания хакера

При рассмотрении этой темы обратим внимание на то, что кроме программ, которые общепринято относить непосредственно к хакерскому инструменту, в действительности хакер использует большой набор обычных утилит, входящих в любую операционную систему. В частности, здесь это: `ipconfig`, `arp` и др.

Как правило, злоумышленник пытается уничтожить доказательства своего пребывания в атакуемой им системе. Тем не менее на практике, даже при получении полного доступа, это не всегда ему удается. Причины могут быть разными. И, как ни странно, тем, кто ищет следы пребывания "чужого", на руку может сыграть даже "конструктивное несовершенство" своего устройства. Например, подобной причиной может быть отсутствие в бытовом, малобюджетном Wi-Fi-роутере возможности настройки времени действия IP-адреса, назначенного DHCP-сервером.

К слову сказать, употребление слова "несовершенство" здесь достаточно условное! Потому что именно небольшая цена и доступность этого устройства обуславливает его некоторое конструктивное упрощение.

Но попробуем на конкретном примере рассмотреть, как же это происходит. Для того чтобы не производить взлома чужой системы и не быть голословными, найдем незащищенный роутер домашнего применения. Для этого достаточно выйти на улицу с ноутбуком и походить возле многоэтажных домов, сканируя эфир.

Результаты не заставят себя ждать. Очень часто среди множества сетей находится незащищенная сеть. Хотя в нашем случае мы все же будем использовать тестовый вариант (рис. 2.1).

Без проблем установив сетевое соединение, получим динамический IP-адрес 192.168.1.54 (рис. 2.2).

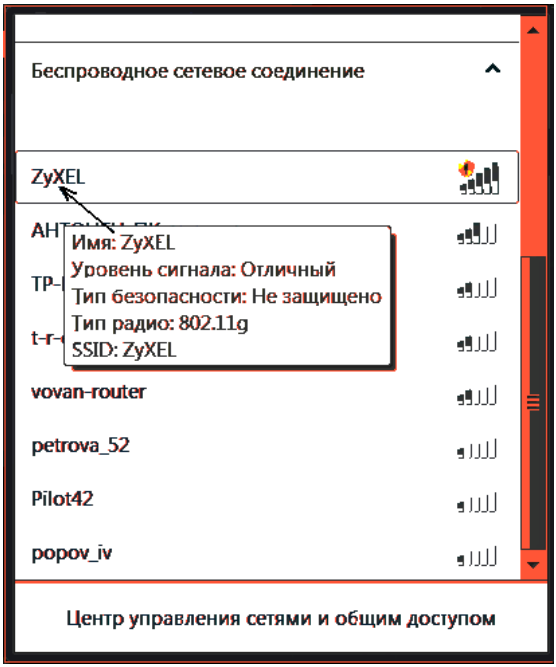
Беспроводное сетевое соединение
ZyXEL
Имя: ZyXEL
Уровень сигнала: Отличный
Тип безопасности: Не защищено
Тип радио: 802.11g
SSID: ZyXEL
vovan-router
petrova_52
Pilot42
popov_iv
Центр управления сетями и общим доступом

Рис. 2.1

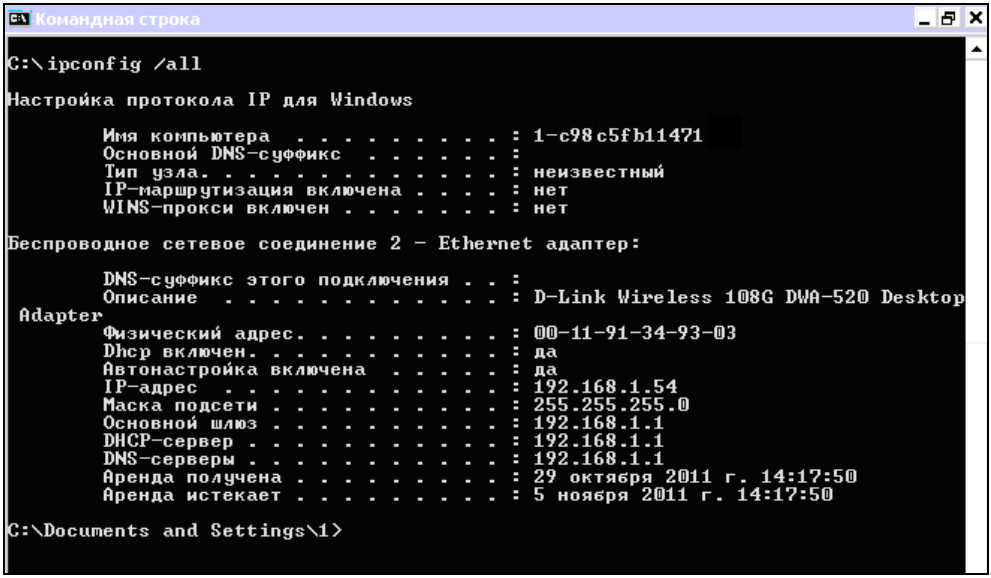
Командная строка
C:\ipconfig /all
Настройка протокола IP для Windows
Имя компьютера . . . . . : 1-c98c5fb11471
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : неизвестный
IP-маршрутизация включена . . . . : нет
WINS-прокси включен . . . . . : нет
Беспроводное сетевое соединение 2 - Ethernet адаптер:
DNS-суффикс этого подключения . . :
Описание . . . . . : D-Link Wireless 108G DWA-520 Desktop Adapter
Физический адрес. . . . . : 00-11-91-34-93-03
Dhcp включен. . . . . : да
Автонастройка включена . . . . . : да
IP-адрес . . . . . : 192.168.1.54
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 192.168.1.1
DHCP-сервер . . . . . : 192.168.1.1
DNS-серверы . . . . . : 192.168.1.1
Аренда получена . . . . . : 29 октября 2011 г. 14:17:50
Аренда истекает . . . . . : 5 ноября 2011 г. 14:17:50
C:\Documents and Settings\1>

Рис. 2.2

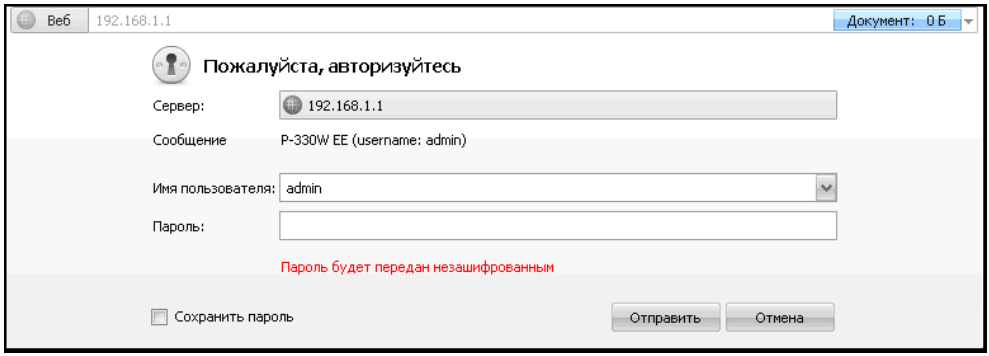
Веб
192.168.1.1
Документ: 0 Б
Пожалуйста, авторизуйтесь
Сервер:
192.168.1.1
Сообщение
P-330W EE (username: admin)
Имя пользователя:
admin
Пароль:
Пароль будет передан незашифрованным
Сохранить пароль
Отправить
Отмена

Рис. 2.3

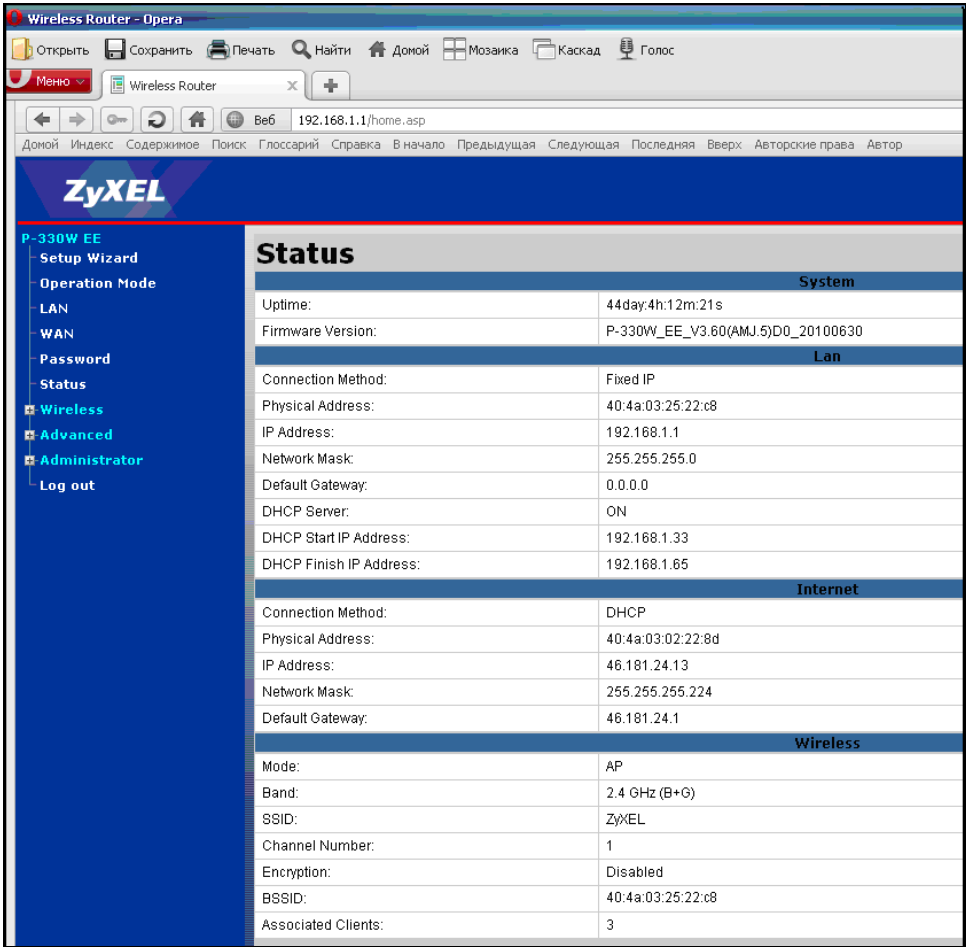
Wireless Router - Opera
Открыть
Сохранить
Печать
Найти
Домой
Мозаика
Каскад
Голос
Меню
Wireless Router
Веб
192.168.1.1/home.asp
Домой Индекс Содержимое Поиск Глоссарий Справка В начало Предыдущая Следующая Последняя Вверх Авторские права Автор
ZyXEL
P-330W EE
Setup Wizard
Operation Mode
LAN
WAN
Password
Status
Wireless
Advanced
Administrator
Log out
Status
System
Uptime: 44day:4h:12m:21s
Firmware Version: P-330W_EE_V3.60(AMJ.5)D0_20100630
Lan
Connection Method: Fixed IP
Physical Address: 40:4a:03:25:22:c8
IP Address: 192.168.1.1
Network Mask: 255.255.255.0
Default Gateway: 0.0.0.0
DHCP Server: ON
DHCP Start IP Address: 192.168.1.33
DHCP Finish IP Address: 192.168.1.65
Internet
Connection Method: DHCP
Physical Address: 40:4a:03:02:22:8d
IP Address: 46.181.24.13
Network Mask: 255.255.255.224
Default Gateway: 46.181.24.1
Wireless
Mode: AP
Band: 2.4 GHz (B+G)
SSID: ZyXEL
Channel Number: 1
Encryption: Disabled
BSSID: 40:4a:03:25:22:c8
Associated Clients: 3

Рис. 2.4

Обратим внимание на то, что адрес автоматически выдается сроком на одну неделю. И для дальнейших исследований запомним, что MAC-адрес нашей карты — 00-11-91-34-93-03.

Подключаемся к роутеру, используя имя по умолчанию `admin` и пароль `1234` (а именно такими они являются в роутерах ZyXEL) (рис. 2.3 и 3.4).

Посмотрим лог-файл устройства, для наглядности установив фильтр на события по HDCP, и убедимся том, что система добросовестно зафиксировала и наш MAC-адрес 00-11-91-34-93-03 (рис. 2.5).

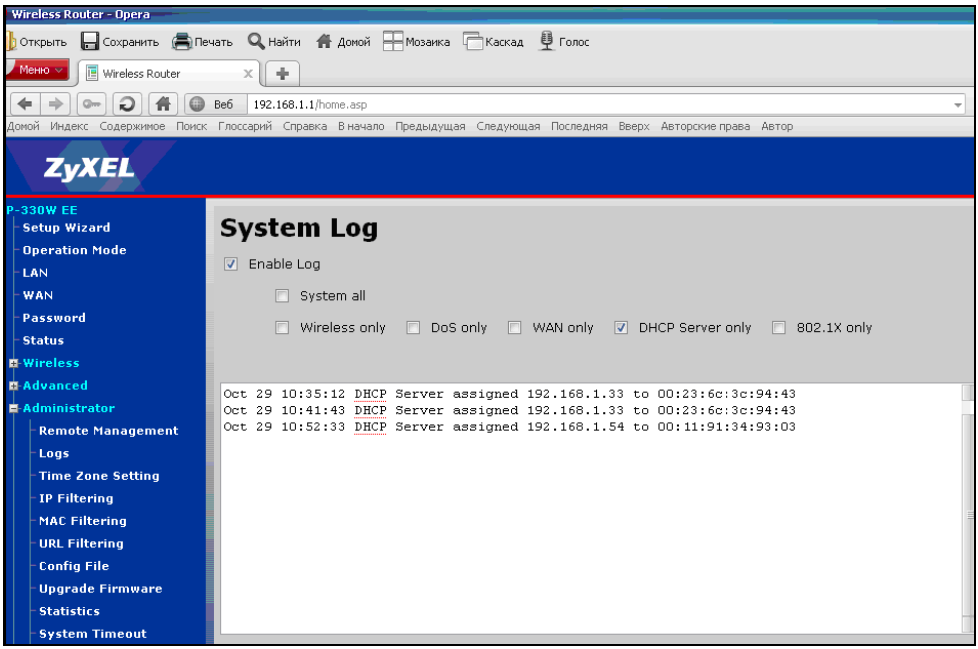

Рис. 2.5

В результате нажатия кнопки **Clear** для аннулирования следов пребывания в системе получаем очищенный лог-файл (рис. 2.6).

Протоколы обнулены, но оказывается, что система все равно сохранила следы нашего пребывания! IP-адрес назначается ею на определенное время (здесь: семь дней). Семь дней, конечно же, еще не истекли. IP-адрес 192.168.1.54 зарезервирован именно для нашего MAC-адреса. И это можно увидеть в таблице DHCP-сервера (рис. 2.7).

Оставить в системе свой MAC-адрес, тем более если он не поддельный, — это серьезный след. Вот если бы имелась возможность конфигурирования времени действия IP-адреса, назначенного DHCP-сервером, в настройках

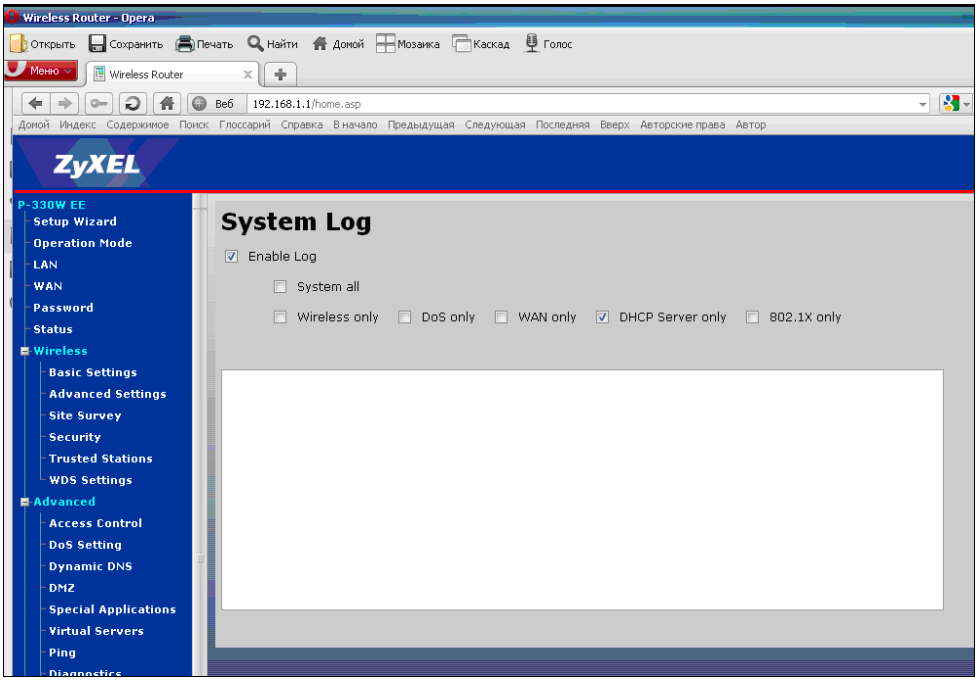
Wireless Router - Opera
Открыть Сохранить Печать Найти Домой Мозаика Каскад Голос
Меню
Wireless Router
Веб
192.168.1.1/home.asp
Домой Индекс Содержимое Поиск Глоссарий Справка В начало Предыдущая Следующая Последняя Вверх Авторские права Автор
ZyXEL
P-330W EE
Setup Wizard
Operation Mode
LAN
WAN
Password
Status
Wireless
Basic Settings
Advanced Settings
Site Survey
Security
Trusted Stations
WDS Settings
Advanced
Access Control
DoS Setting
Dynamic DNS
DMZ
Special Applications
Virtual Servers
Ping
Diagnostics
System Log
Enable Log
System all
Wireless only
DoS only
WAN only
DHCP Server only
802.1X only

Рис. 2.6

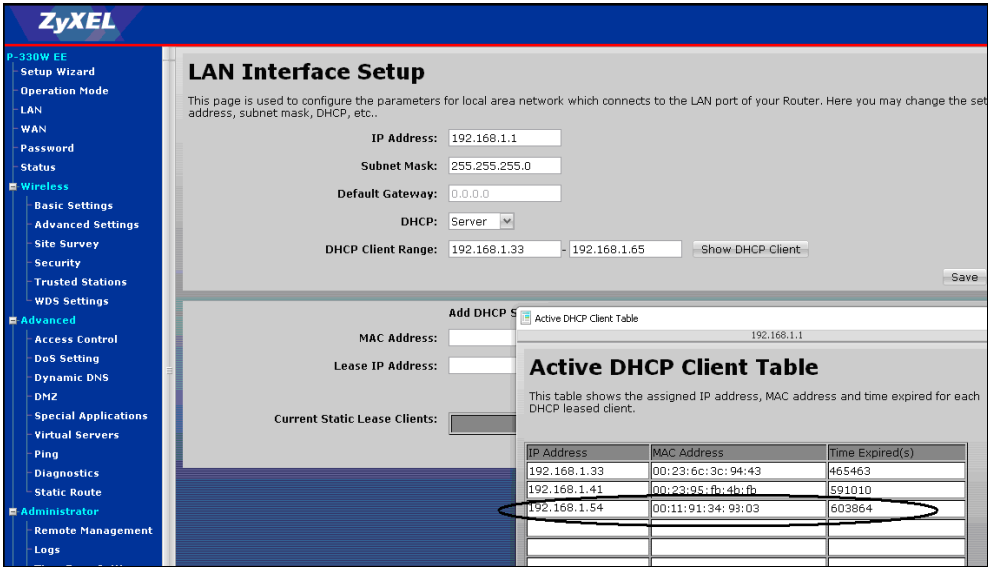
ZyXEL
P-330W EE
Setup Wizard
Operation Mode
LAN
WAN
Password
Status
Wireless
Basic Settings
Advanced Settings
Site Survey
Security
Trusted Stations
WDS Settings
Advanced
Access Control
DoS Setting
Dynamic DNS
DMZ
Special Applications
Virtual Servers
Ping
Diagnostics
Static Route
Administrator
Remote Management
Logs
LAN Interface Setup
This page is used to configure the parameters for local area network which connects to the LAN port of your Router. Here you may change the set
address, subnet mask, DHCP, etc..
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0
DHCP: Server
DHCP Client Range: 192.168.1.33 - 192.168.1.65 Show DHCP Client
Save
Add DHCP S
MAC Address:
Lease IP Address:
Current Static Lease Clients:
Active DHCP Client Table
192.168.1.1
Active DHCP Client Table
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.
IP Address
MAC Address
Time Expired(s)
192.168.1.33
00:23:6c:3c:94:43
465463
192.168.1.41
00:23:95:fb:4b:fb
591010
192.168.1.54
00:11:91:34:93:03
603864

Рис. 2.7

атакуемого устройства, то в дополнение к очистке журналов злоумышленник мог бы выставить этот период в минимально разумное значение. Например, один день. Тогда следы его пребывания в системе пропали бы через сутки.

Попутно необходимо заметить, что если в такой ситуации злоумышленник установит себе статический адрес, то, конечно же, следа в этой таблице он бы не оставил.

В приведенном примере следы остаются не по недосмотру атакующего, а по техническим причинам. Рассмотрим пример, наглядно показывающий, как можно организовать атаку, практически не оставляя следов.

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 об 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. 2.8).

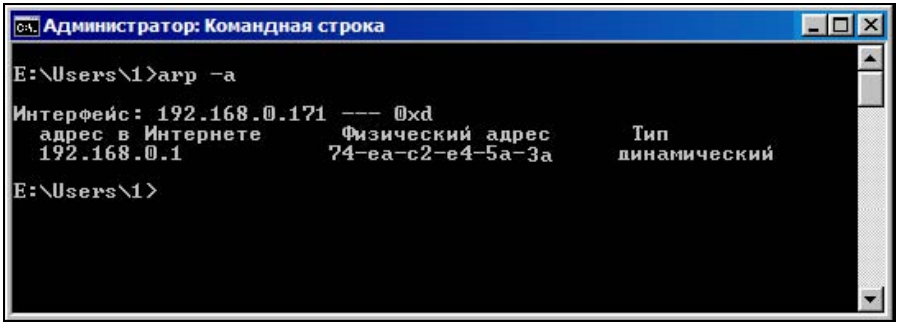

Рис. 2.8

Проимитируем атаку, используя уже известные нам недостатки протокола ARP. С этой целью применим программу, о которой вскользь уже упоминалось 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. 2.9).

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

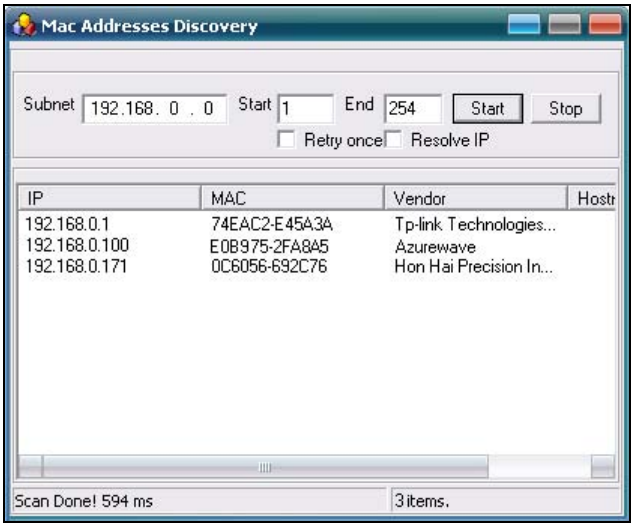

Рис. 2.9

Используя программу IP Tools, разошлем по сети ложные ARP-пакеты, сообщая всем ложный, 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. 2.10).

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. 2.11).

Нормальная работа сети восстановится, спустя несколько секунд после прекращения рассылки ложных 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. Помнится, одно время один наш местный провайдер даже рассылал по этому поводу инструкции, как пользователям можно бороться с такой ситуацией.

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.

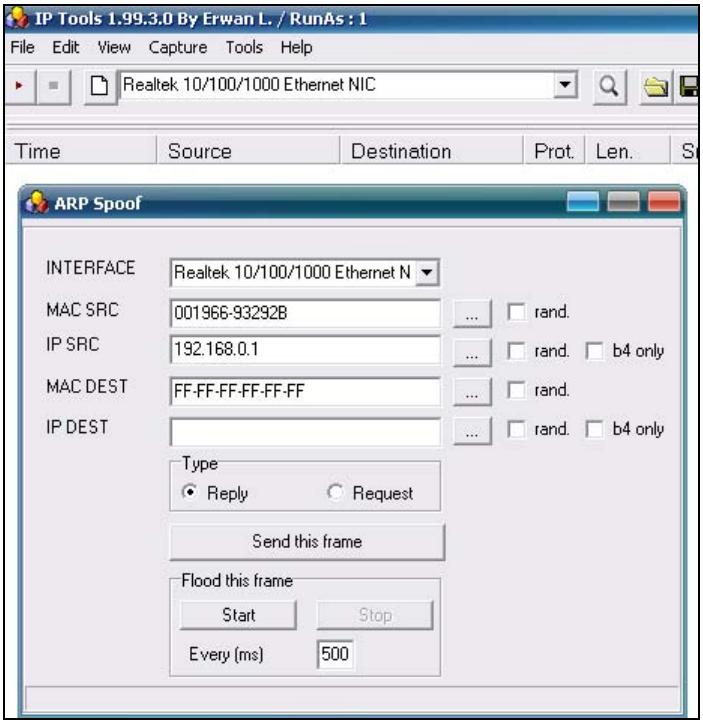

Рис. 2.10

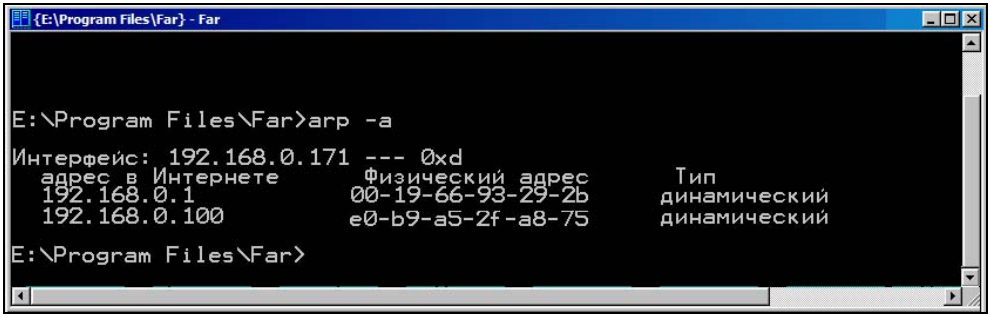

Рис. 2.11

При проведении подобной атаки ленивому хакеру для заметания следов даже не требуется сменять MAC-адрес на своем компьютере, с которого осуществляется 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 снифер для захвата пакетов и посмотрев их содержимое (рис. 2.12).

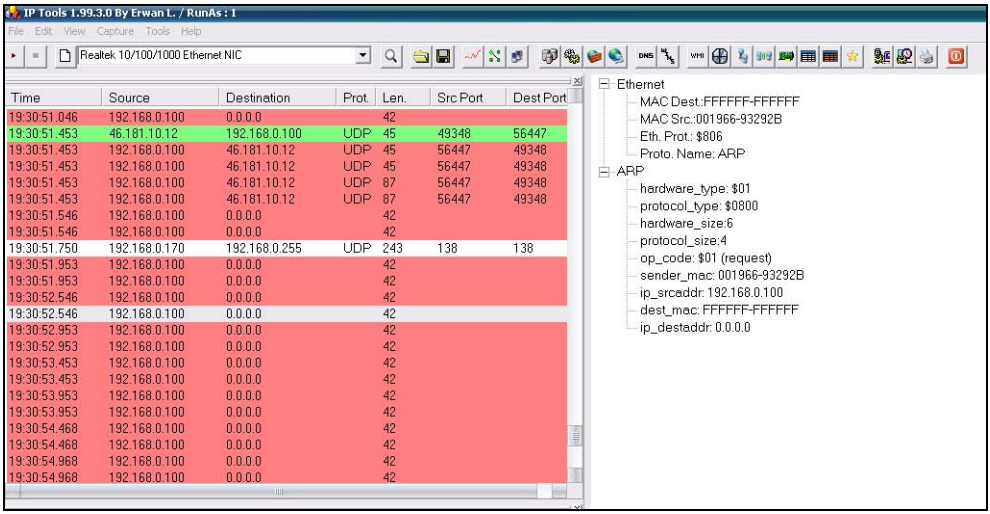

Рис. 2.12

В заключение темы скажем еще о том, что указанная программа имеет необычайное множество полезных возможностей и практически незаменима в качестве набора инструмента при работе с сетями и в том числе при отработке вопросов, связанных с их безопасностью. Здесь же пока мы упомянули совсем немного и только о некоторых ее возможностях: в частности, о некоторых особенностях при работе с протоколом ARP, а также о снифере (как и многие программы такого рода, в нашем случае использовался внешний сниффер WINPCAP, устанавливаемый дополнительно).

ГЛАВА 3

Взлом хэш-функции пароля *enable* маршрутизатора Cisco

Мы не можем не вернуться к разговору о паролях, в силу важности этой темы. Тем более, что это поможет нам в понимании методологии формирования кейса хакера.

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

Например, для операционной системы Windows можно применить метод, когда используя загрузочный, установочный диск, путем несложных манипуляций выгружается реестр системы. Затем в этот реестр вписывается трансформированный куст ветви HKLM\Setup. Изменения эти таковы, что операционная система воспринимает положение вещей так, как будто бы процесс ее инсталляции еще не завершен. После обратной загрузки уже подправленного реестра Windows при перезагрузке попросит внести уже новый пароль администратора. Упоминаем здесь именно об этом способе исключительно из-за оригинальности самой идеи.

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). В UNIX-системах это может быть файл типа etc/shadow.

Но все 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 на старом пароле, то это