Л314. Анализ беспроводного трафика в Kali Linux. Развертывание Eve-ng.

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, HIDs)*. 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).

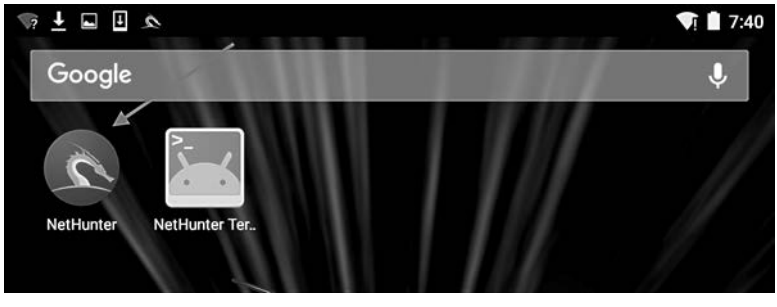

Рис. 12.1. Значок NetHunter на экране мобильного устройства

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).

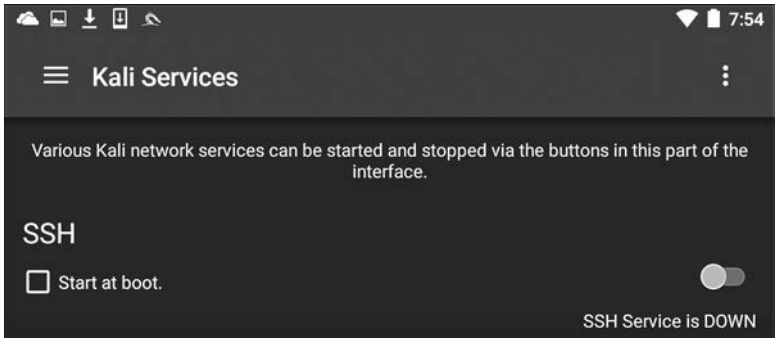

Рис. 12.2. Меню настроек различных служб NetHunter

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).

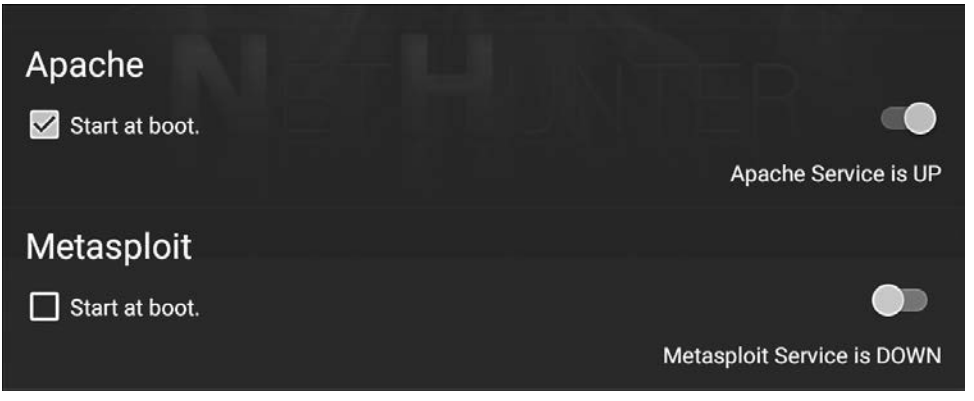

Рис. 12.3. Настройка запуска служб Apache и Metasploit при старте

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).

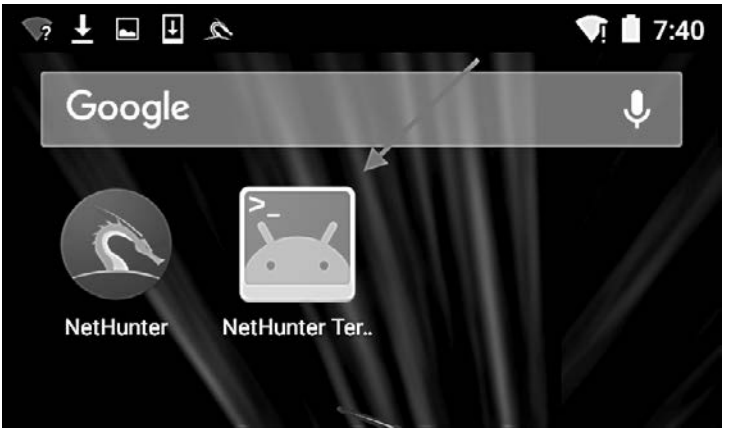

Рис. 12.4. Запуск терминала

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.

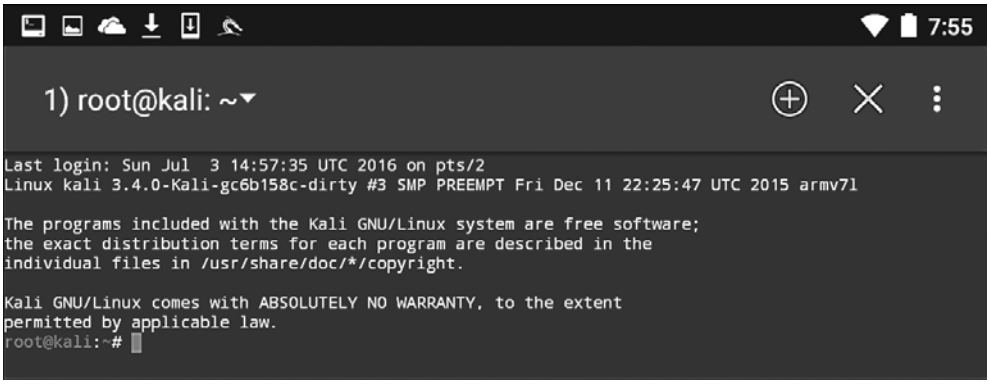

Рис. 12.5. Терминал запущен

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).

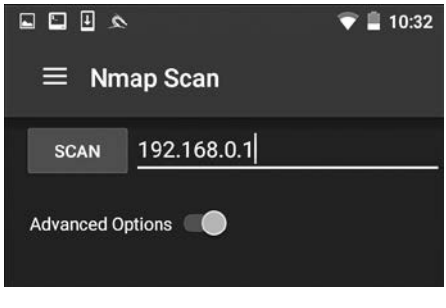

Рис. 12.6. Вводим IP-адрес исследуемого объекта

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).

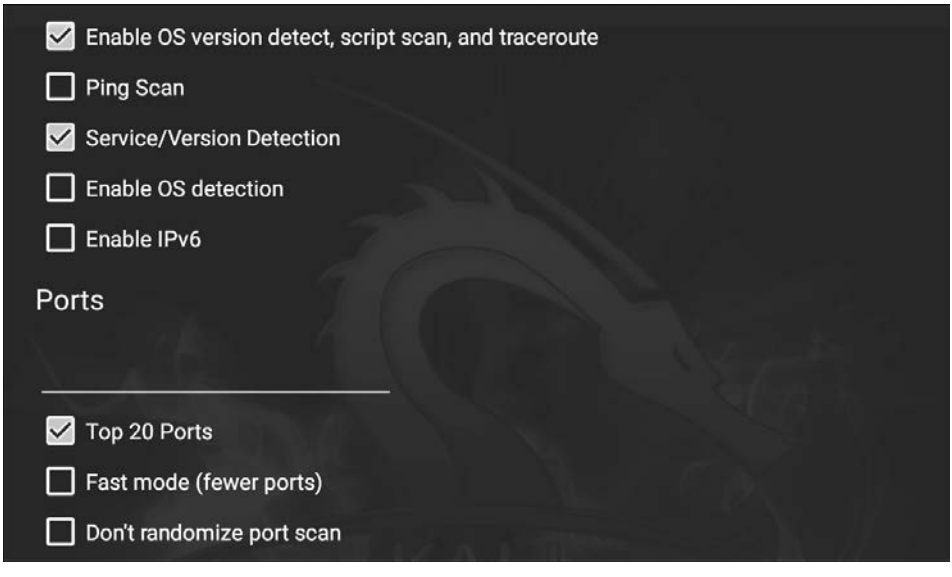

Рис. 12.7. Настройка сканирования

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.

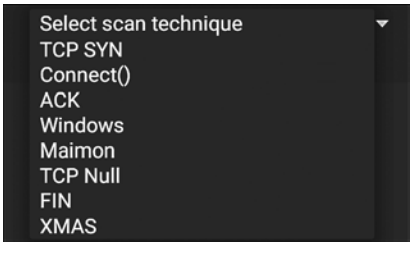

Рис. 12.8. Выбор параметров сканирования

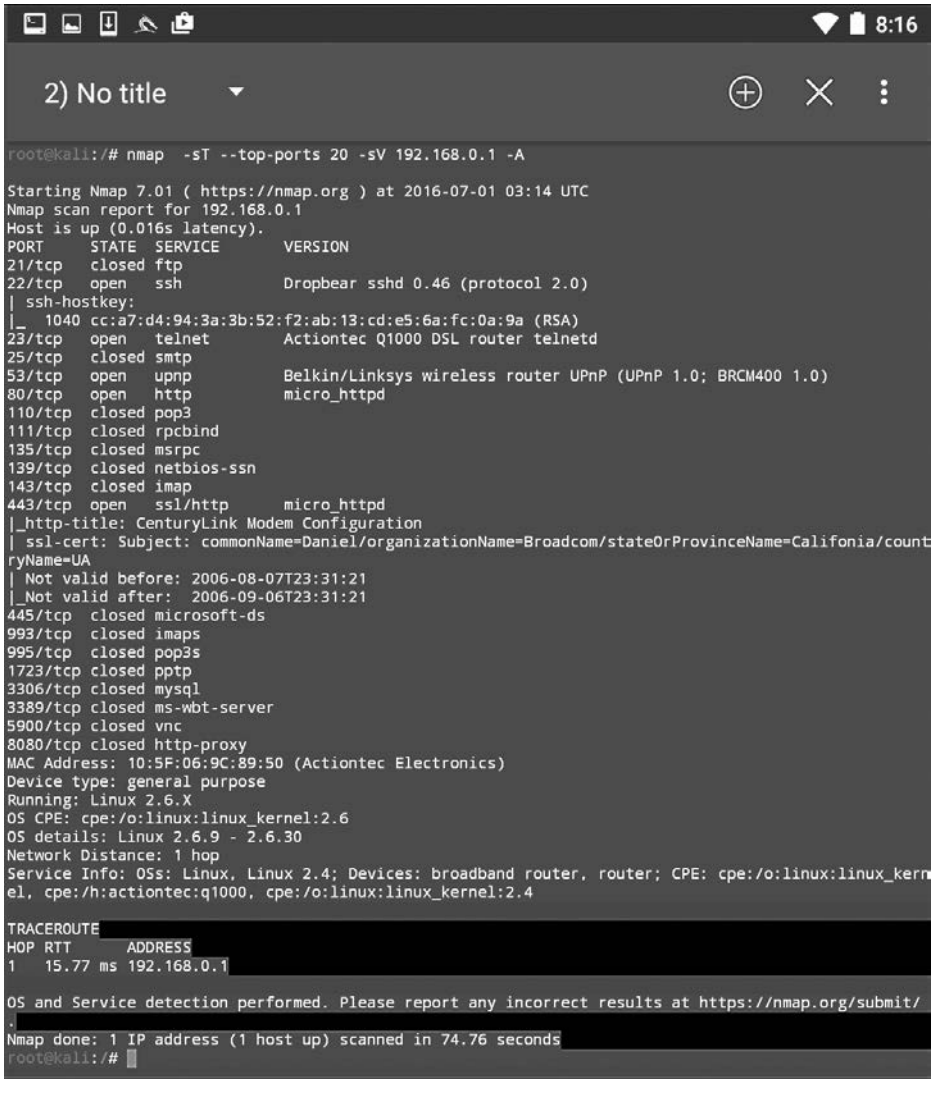

Рис. 12.9. Сканирование запущено

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.

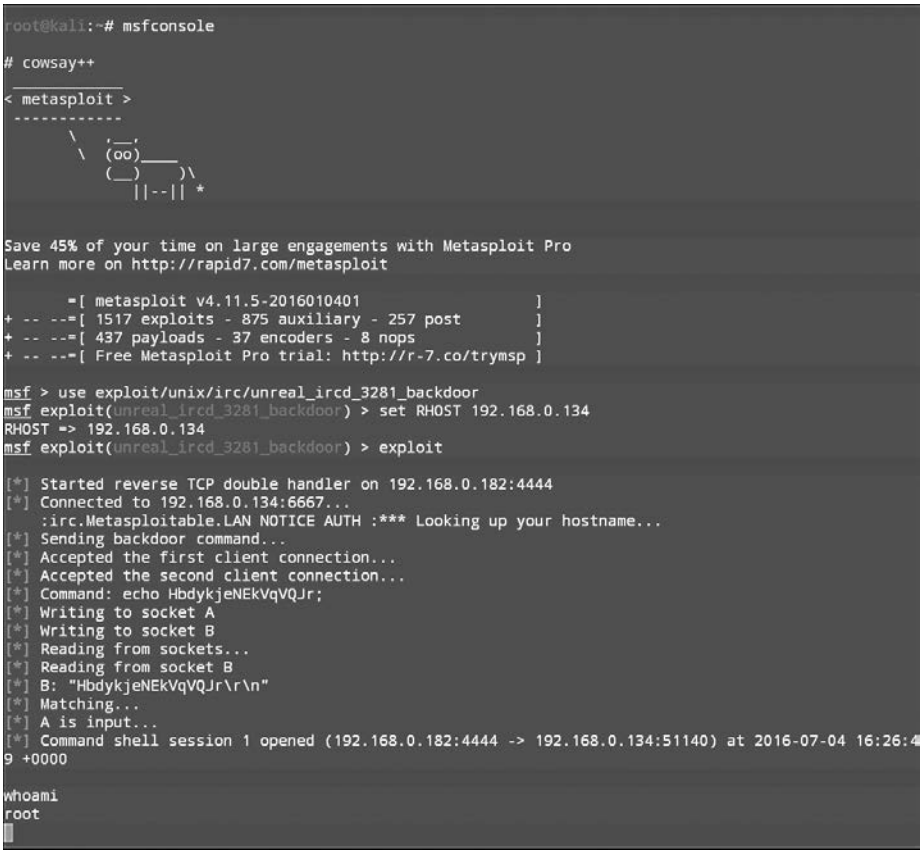

Рис. 12.10. Вывод предыдущих команд

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).

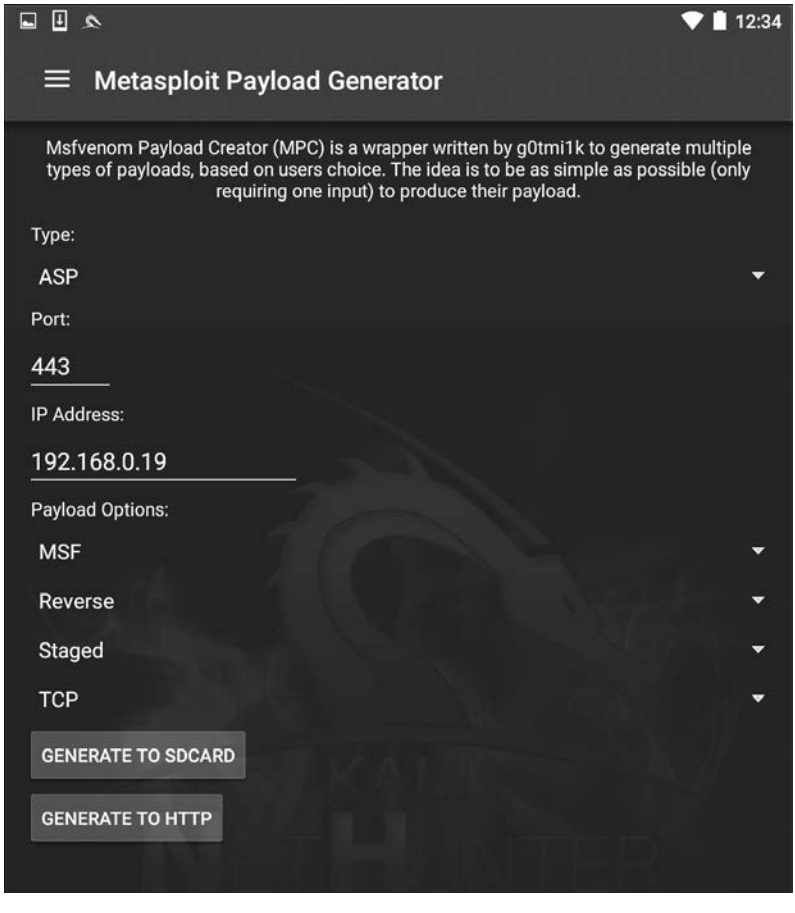

Рис. 12.11. Генератор полезной нагрузки Metasploit

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 эксплойтов, расположенную по адресу https://www.exploit-db.com/, и позволяет искать дополнительные эксплойты, 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).

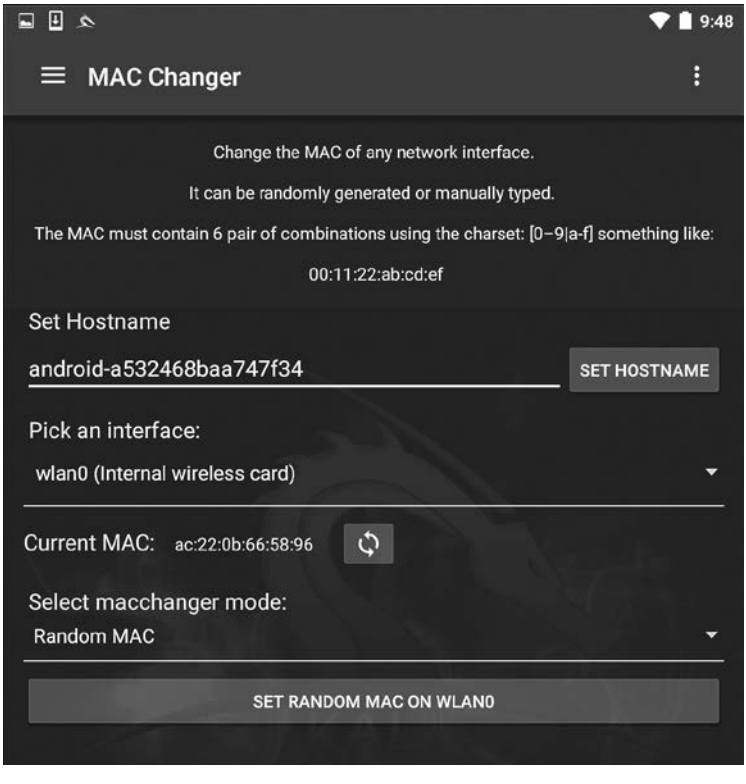

Рис. 12.12. Экран MAC Changer

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).

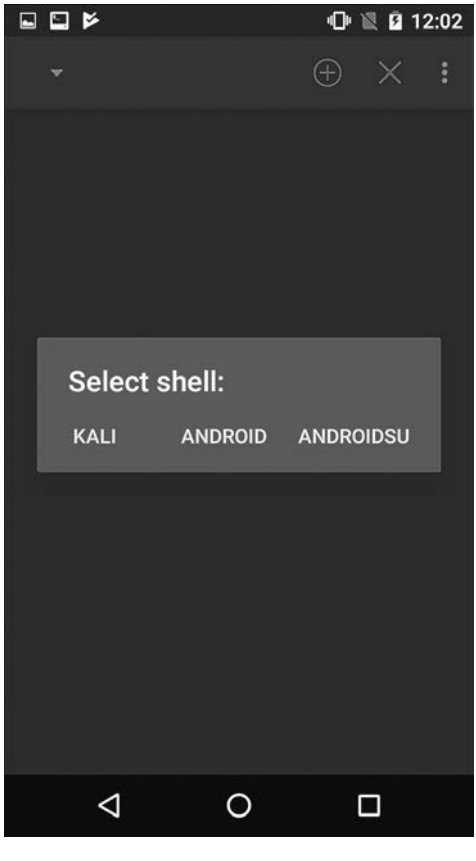

Рис. 12.13. Выбор терминала

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).

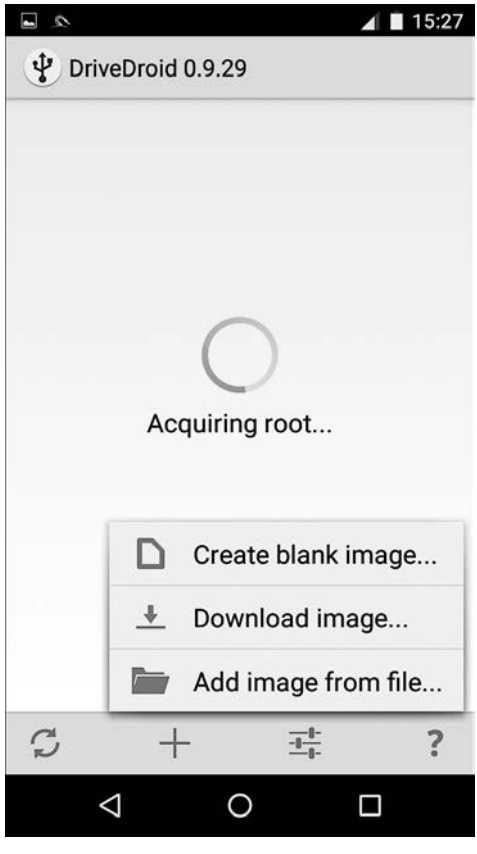

Рис. 12.14. Загрузка DriveDroid

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).

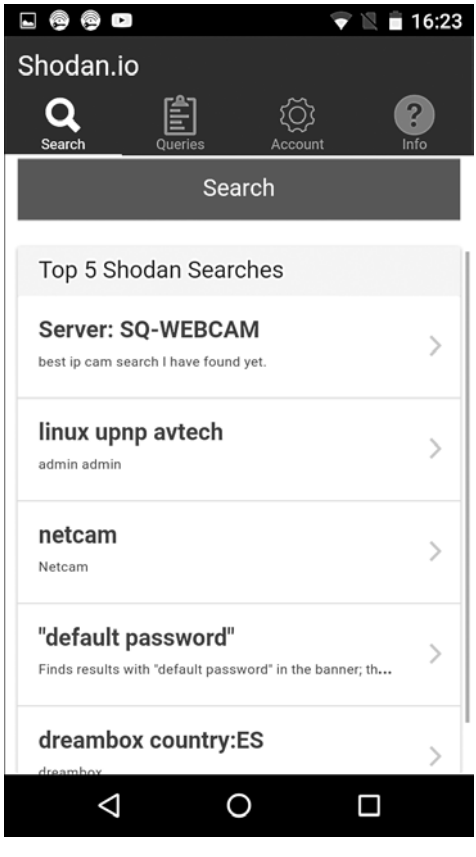

Рис. 12.15. Приложение Shodan

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).

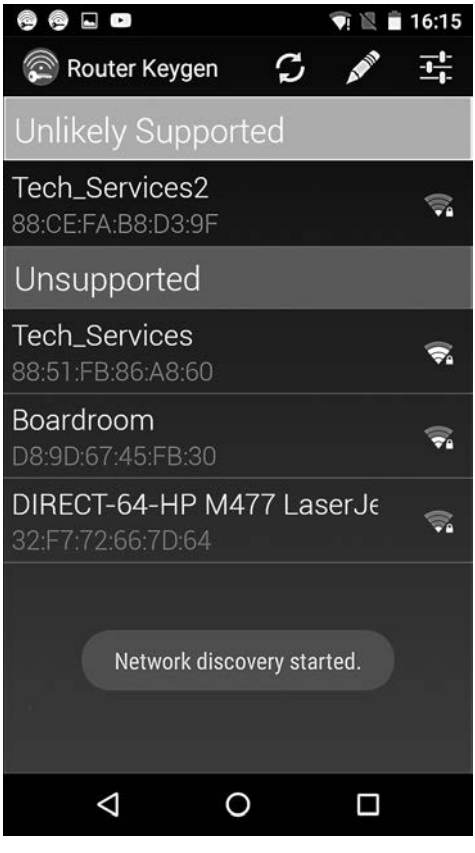

Рис. 12.16. Сканирование Wi-Fi-сетей приложением Router Keygen

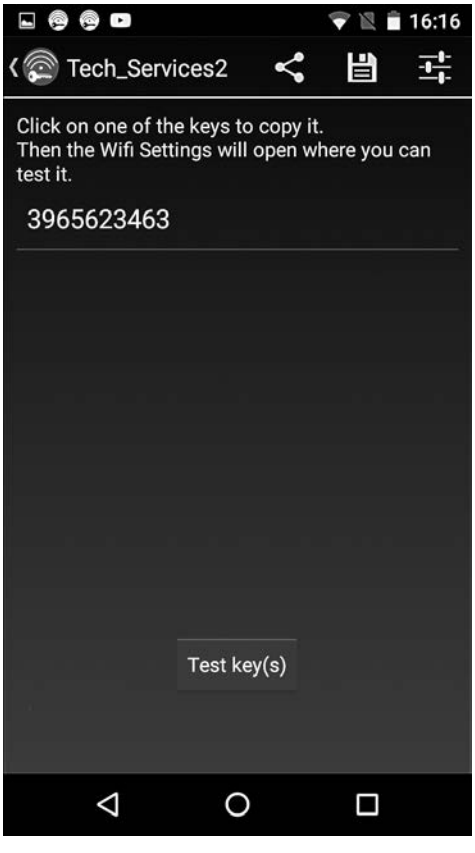

Рис. 12.17. Создание ключей

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.

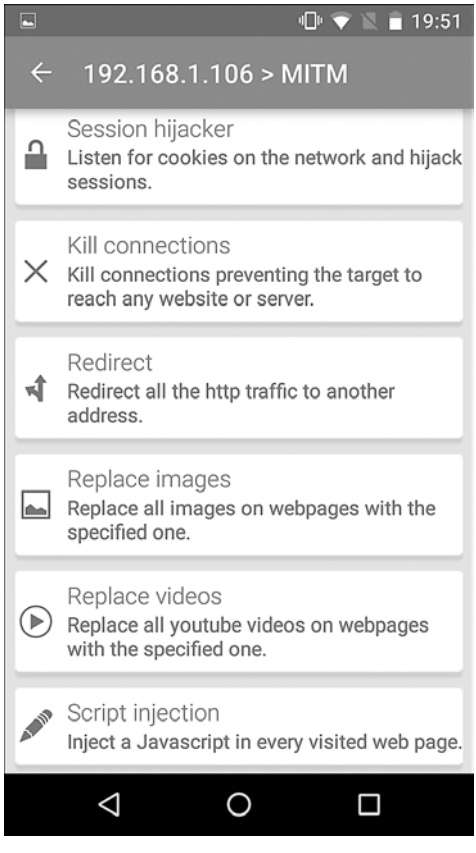

Рис. 12.18. Модули на выбор

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 возможность 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).

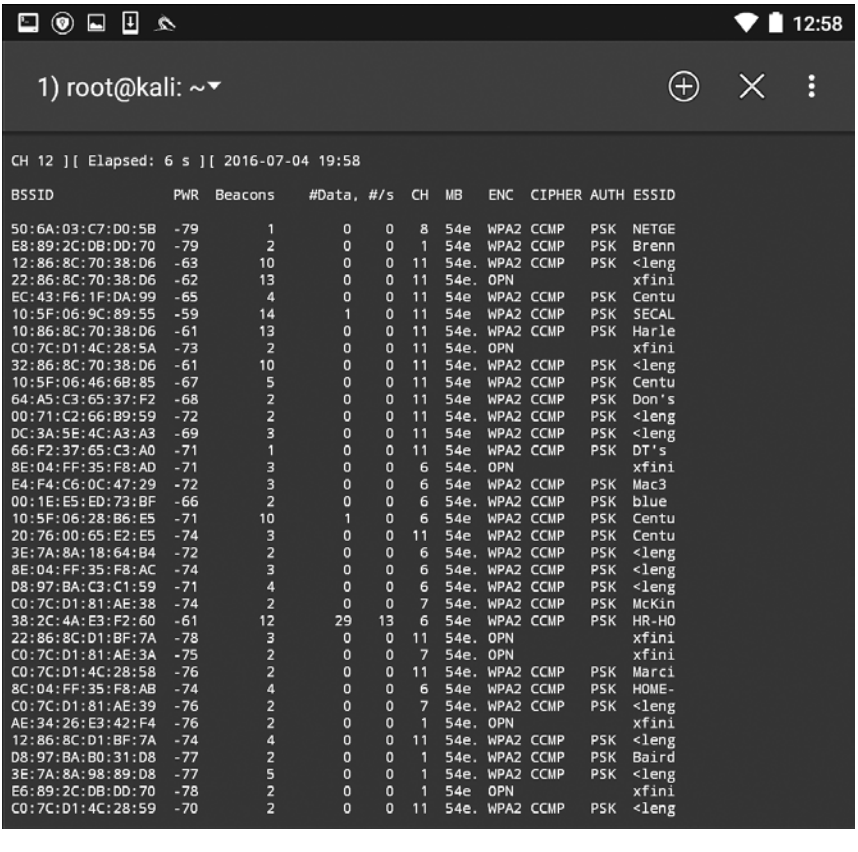

Рис. 12.19. Идентификация потенциальных целевых сетей

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`.

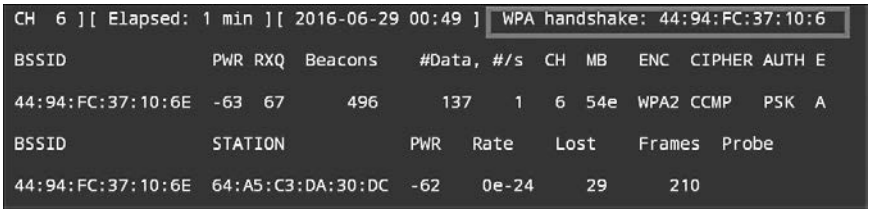

Рис. 12.20. Вывод команды airodump-ng

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).

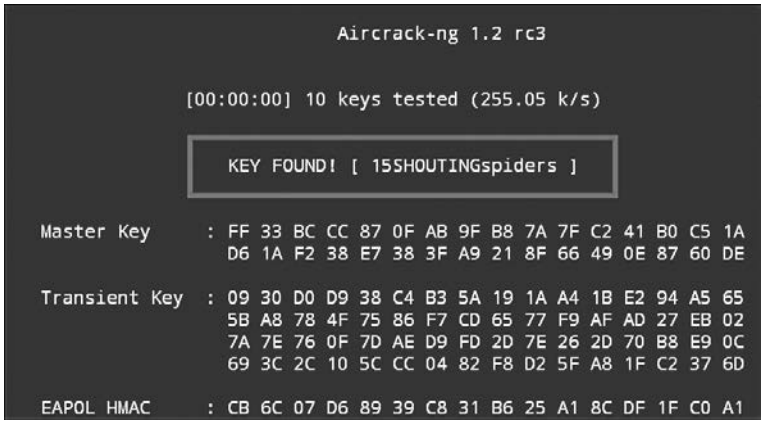

Рис. 12.21. Вывод команды aircrack-ng

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).

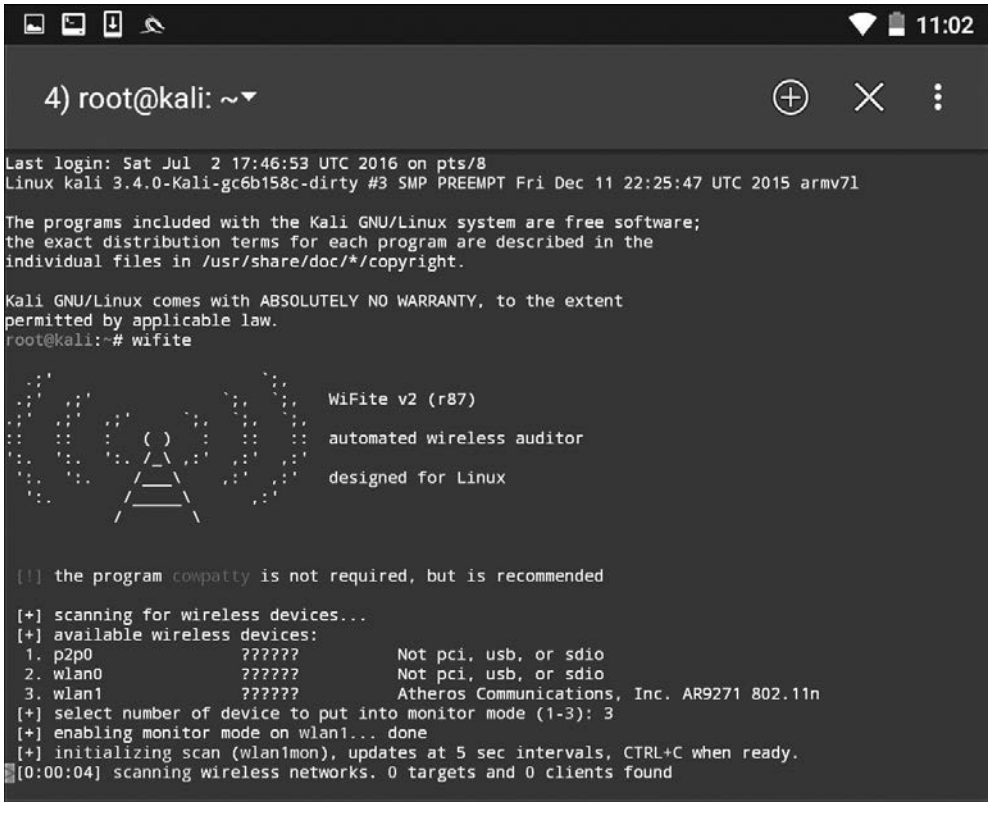

Рис. 12.22. Результат выполнения команды wifite

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).

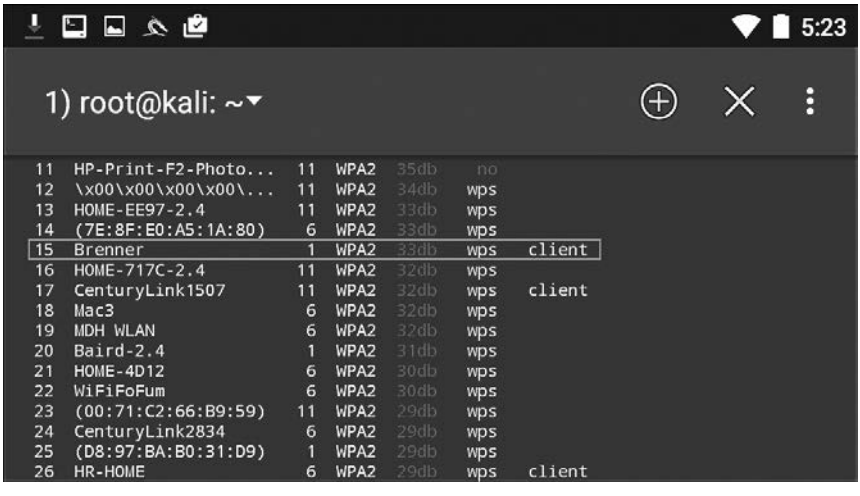

Рис. 12.23. Интерфейс WLAN1 переведен в режим мониторинга

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).

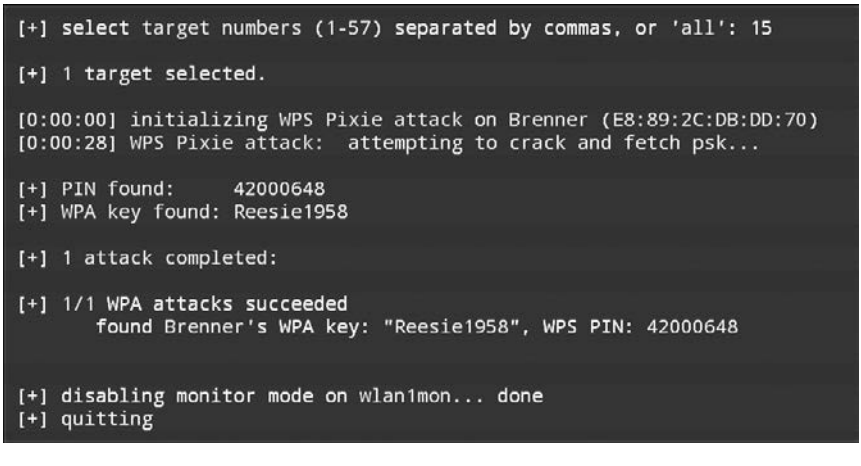

Рис. 12.24. Атака запущена

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

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.

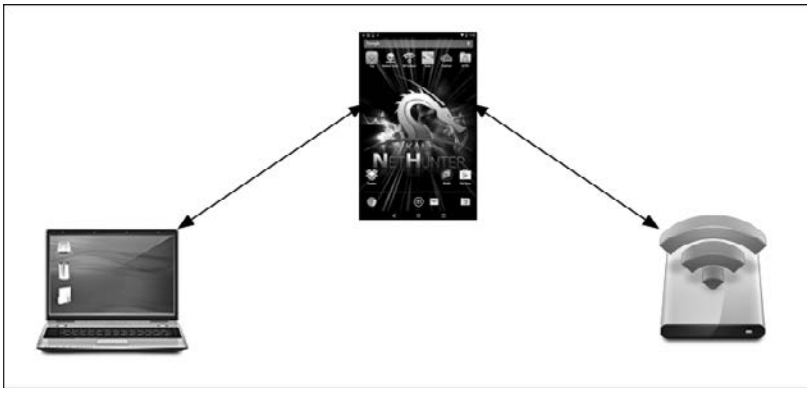

Рис. 12.25. Схема передачи трафика от цели к законной точке доступа через NetHunter

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).

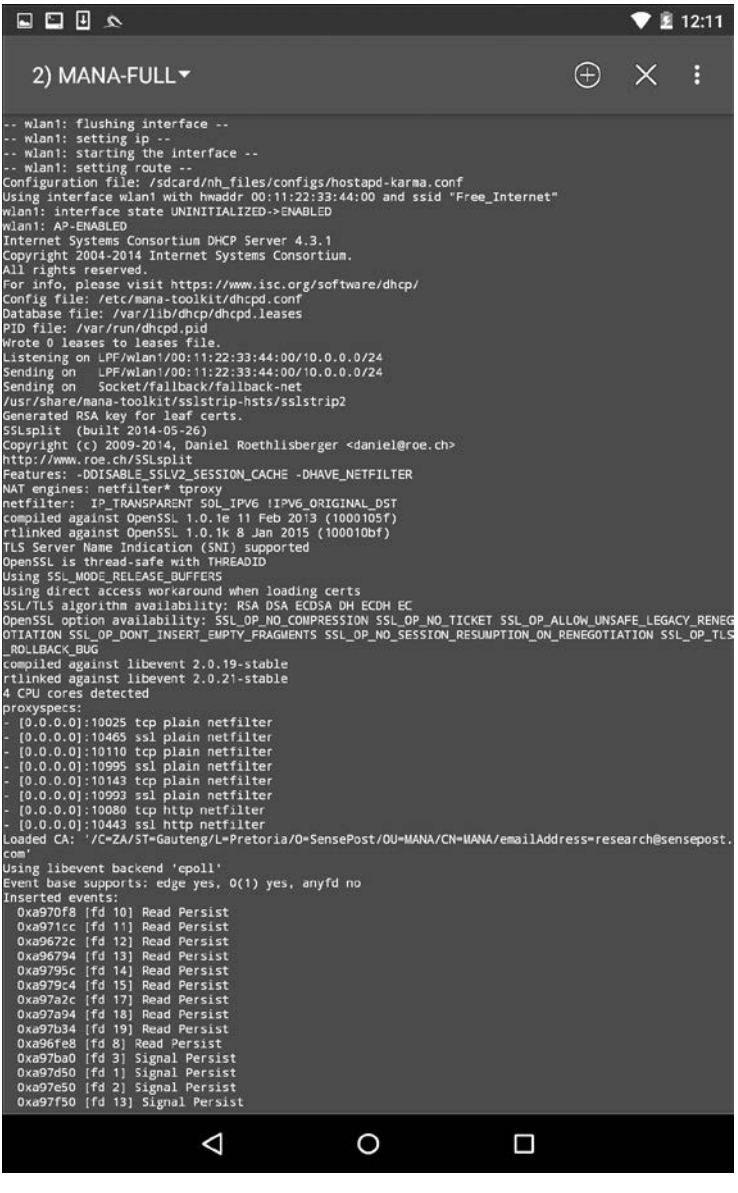

Рис. 12.27. Фальшивая точка доступа создана

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).

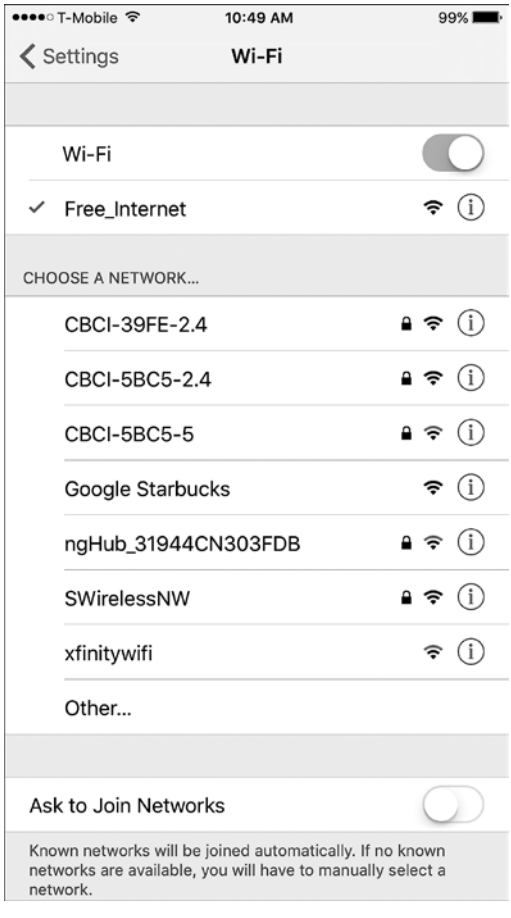

Рис. 12.28. Подключение к точке доступа без аутентификации

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.

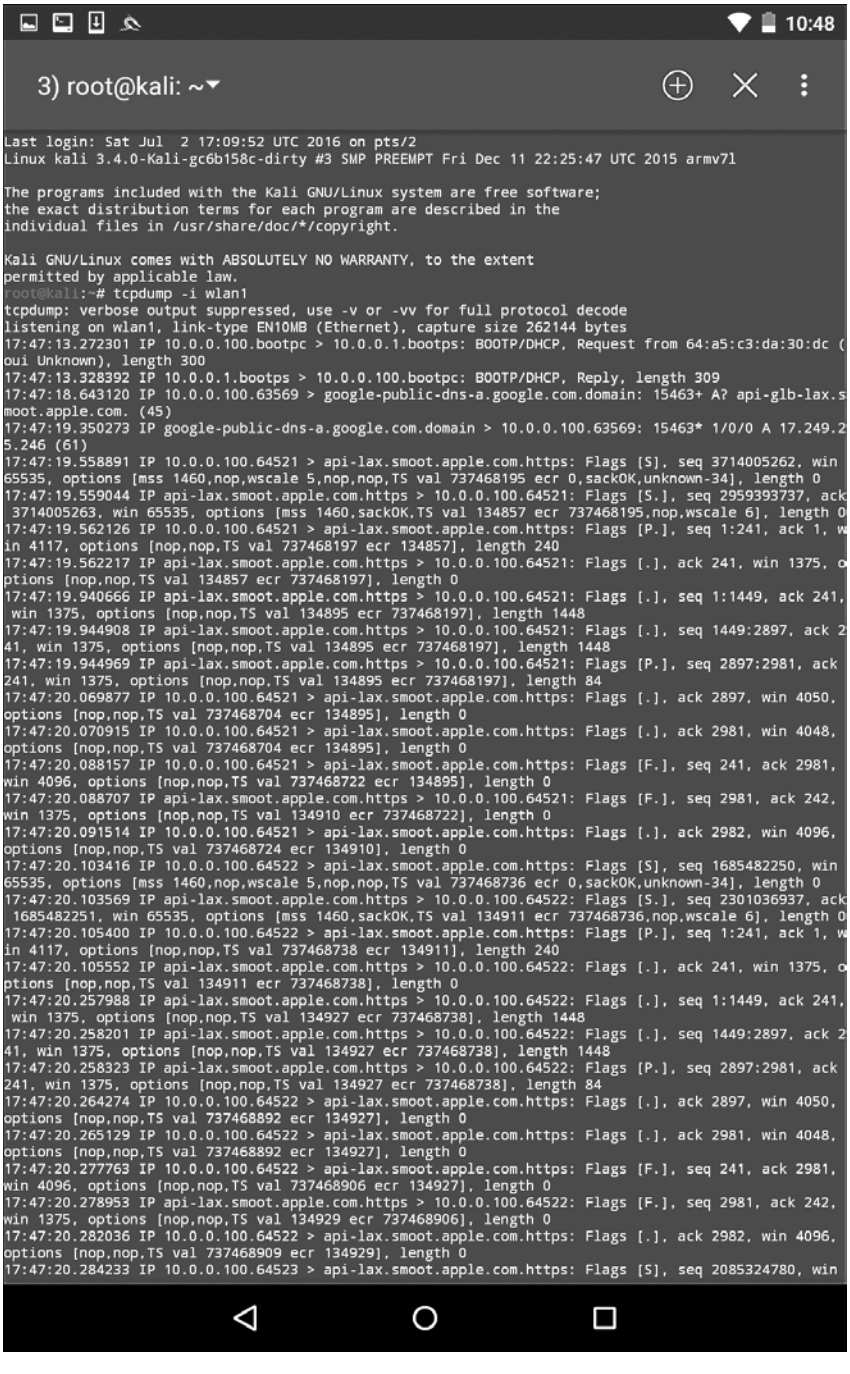

Рис. 12.29. Вывод команды tcpdump

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 Mana 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.

HID-атаки

В NetHunter есть несколько встроенных инструментов, которые позволяют настроить атаку HID. В одном из них используется стандартная командная строка для выполнения нескольких команд подряд. Чтобы получить доступ к меню HID-атаки, щелкните на значке NetHunter, а затем на HID Attacks (HID-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 HID-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 настроить обход для ОС Windows (рис. 12.31).

Поскольку мы пытаемся выполнить HID-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

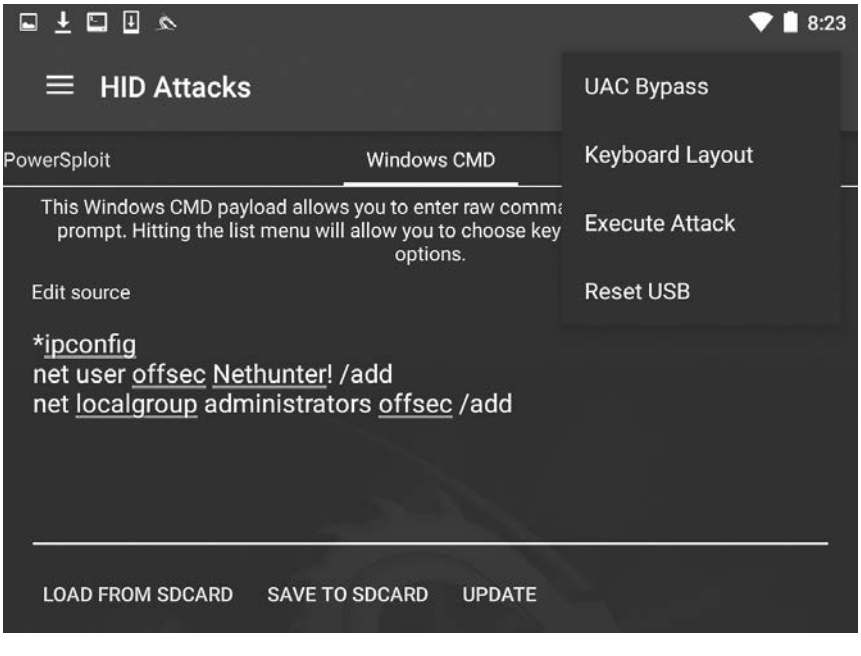

Рис. 12.31. Настройка UAC Bypass для Windows

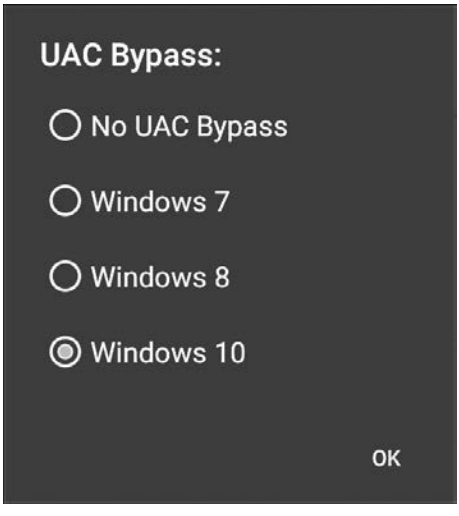

Рис. 12.32. Выбор версии операционной системы Windows

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
   Link-local IPv6 Address . . . . . : fe80::a410:d0b0:d3f8:df17%8
   IPv4 Address. . . . . . . . . . . : 192.168.0.14
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

Рис. 12.33. Команда ipconfig запущена

```
C:\Windows\system32>net user offsec Nethunter! /add
The command completed successfully.


C:\Windows\system32>net localgroup administrators offsec /add
The command completed successfully.
```

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 Keygen?
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/.