1

Подготовка к работе

Путешествие в тысячу миль начинается с одного шага.

Лао-цзы

Итак, вы совершили первый шаг своего хакерского путешествия. В этой главе мы настроим виртуальную лабораторию, среда которой будет состоять из пяти виртуальных машин, таких как:

- **виртуальная машина pfSense** — маршрутизатор/межсетевой экран с открытым исходным кодом для защиты уязвимых виртуальных машин от внешних хакерских атак;
- **виртуальная машина Kali Linux** — машина, содержащая хакерские инструменты, описанные в этой книге;
- **две desktop-версии виртуальной машины Ubuntu Linux** — эти машины будут использоваться для демонстрации атак на среду настольного компьютера и ноутбука;
- **виртуальная машина Metasploitable** — машина, с помощью которой будут продемонстрированы атаки на сервер Linux.

Виртуальная лаборатория

Взлом компьютеров, которыми вы не владеете, является неэтичным и незаконным, поэтому в данной главе мы создадим виртуальную лабораторию, которая послужит средой для занятий этичным хакингом. Обзор этой лабораторной среды представлен на рис. 1.1.

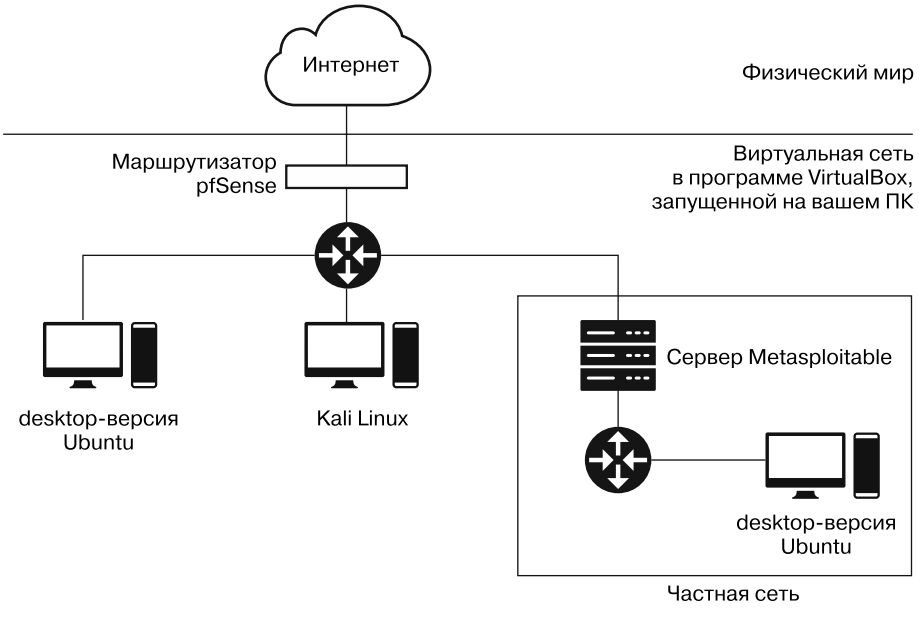

Рис. 1.1. Связи между виртуальными машинами

Нам также предстоит настроить две сети: основную внутреннюю, изолированную от интернета с помощью межсетевого экрана pfSense, и частную, изолированную от основной с помощью сервера Metasploitable. Вторую структуру мы будем использовать для изучения атак, в которых хакерам необходимо взломать одну машину, чтобы атаковать другую, как в случае с межсетевыми экранами. Основную сеть мы настроим в этой главе, а частную — в главе 14.

Не беспокойтесь, если вы пока не вполне понимаете все технические нюансы этих конфигураций; вся инфраструктура будет подробно описана далее в книге. Я рекомендую использовать компьютер под управлением ОС Windows, Linux или macOS с не менее чем 30 Гбайт свободного места на жестком диске и 4 Гбайт оперативной памяти. Вам предстоит одновременно запускать несколько виртуальных машин, поэтому понадобится довольно мощный компьютер.

Настройка VirtualBox

Для настройки сетевой среды необходимо установить программу VirtualBox, которая позволяет создавать виртуальные машины. При использовании VirtualBox мы указываем характеристики виртуальной машины (например, количество процессоров, объем жесткого диска и оперативной памяти), и эта программа собирает виртуальный компьютер, на котором можно запускать программы так же, как на

ноутбуке или настольном компьютере. VirtualBox можно использовать бесплатно на устройствах под управлением операционных систем Linux, Mac и Windows.

Скачайте VirtualBox с сайта https://www.virtualbox.org/wiki/Downloads/, выбрав установочные файлы, соответствующие операционной системе и архитектуре вашего компьютера. Затем выполните установку. Этот процесс будет зависеть от типа вашего компьютера, но, как правило, в его ходе можно использовать параметры, заданные по умолчанию. После завершения установки и запуска VirtualBox вы увидите экран, изображенный на рис. 1.2.

Рис. 1.2. Главный экран VirtualBox

Настройка pfSense

Теперь мы настроим *pfSense*, маршрутизатор/межсетевой экран с открытым исходным кодом, который защитит наши виртуальные машины от внешних атак. В процессе настройки важно тщательно следовать приведенной далее инструкции. Сначала скачайте исходные файлы pfSense с сайта https://www.pfsense.org/download/. В раскрывающемся списке Architecture (Архитектура) выберите вариант AMD64 (64-bit), в списке Installer — DVD Image (ISO) Intaller, а в списке Mirror (Зеркало) — ближайший к вам сервер, после чего нажмите кнопку Download (Скачать) (рис. 1.3).

Рис. 1.3. Выберите указанные параметры, чтобы скачать pfSense

Разархивируйте загруженный файл pfSense `iso.gz`. Если вы используете компьютер под управлением Unix, то можете сделать это, введя в терминале команду **`gunzip`** и имя скачанного файла (например, `gunzip pfSense-`*`имя_файла`*`.iso.gz`). Запустите программу VirtualBox и нажмите кнопку New (Создать), расположенную на верхней панели инструментов (рис. 1.4).

Рис. 1.4. Кнопка New (Создать) оформлена в виде звезды

Далее вам будет предложено ввести кое-какую информацию о своей новой машине. Следующие примеры относятся к программе VirtualBox для macOS, но версии для Linux и Windows практически ничем не отличаются. В поле Name (Имя) введите pfSense, в списке Type (Тип) выберите BSD, а в списке Version (Версия) — FreeBSD (64bit). Задав эти три параметра (рис. 1.5), нажмите кнопку Continue (Продолжить).

Виртуальной машине pfSense не требуется много оперативной памяти, поэтому при указании ее объема задайте значение 1024 MB. При настройке параметров виртуального жесткого диска выберите вариант Create a virtual hard disk now (Создать новый виртуальный жесткий диск). В качестве типа файла укажите VDI (VirtualBox Disk Image). Сделайте свой новый виртуальный жесткий диск динамическим

и ограничьте его размер 5 Гбайт, которых должно быть более чем достаточно для установки pfSense.

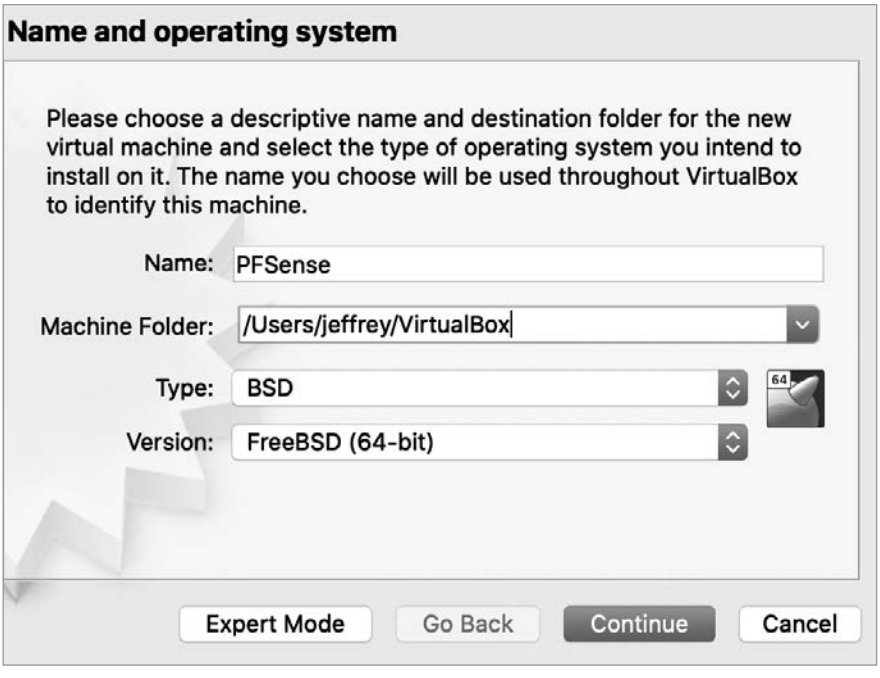

Рис. 1.5. Введите эти параметры при создании виртуальной машины pfSense

Настройка внутренней сети

Межсетевой экран pfSense можно представить в качестве привратника, стоящего между интернетом и вашей внутренней сетью. Он проверяет входящий и исходящий трафик, чтобы убедиться в том, что ваша внутренняя сеть защищена от атак извне. Это позволяет создать безопасное место для добавления уязвимых машин, которые сможете атаковать только вы.

Щелкните правой кнопкой мыши на названии pfSense в списке виртуальных машин и выберите в контекстном меню пункт Settings (Настроить) (рис. 1.6).

Перейдите на вкладку Network (Сеть) и убедитесь в том, что сетевой адаптер на вкладке Adapter 1 (Адаптер 1) включен, в поле Attached to (Тип подключения) выбран вариант Bridged Adapter (Сетевой мост), а содержимое поля Name (Имя) совпадает с именем вашей беспроводной сетевой карты. Включение сетевого моста обеспечивает прямое соединение между виртуальной машиной pfSense и интернетом. Теперь

перейдите на вкладку Adapter 2 (Адаптер 2), убедитесь в том, что сетевой адаптер включен, в поле Attached to (Тип подключения) выбран вариант Internal Network (Внутренняя сеть), которую мы назовем Internal LAN (Внутренняя локальная сеть). Эта сеть позволит соединить pfSense с другими виртуальными машинами. После нажатия кнопки OK внутренняя сеть станет доступна для остальных виртуальных машин.

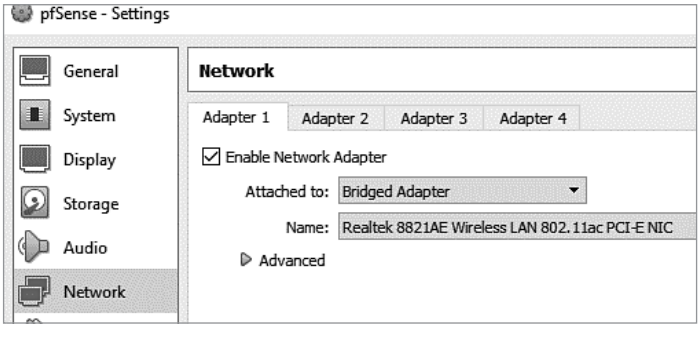

Рис. 1.6. Настройка сетевых адаптеров

Конфигурирование параметров pfSense

Теперь мы можем запустить pfSense и сконфигурировать параметры нашего виртуального маршрутизатора. Некорректная конфигурация этих параметров может препятствовать подключению виртуальных машин к интернету.

Дважды щелкните на пункте pfSense в списке виртуальных машин. На появившемся экране (рис. 1.7) щелкните на значке в виде папки, а затем — на значке Add (Добавить) в левом верхнем углу. Найдите и выберите ISO-образ pfSense, а затем нажмите кнопку Start (Запуск).

Рис. 1.7. Выбор ISO-образа pfSense

Загрузка виртуальной машины pfSense займет некоторое время. По ее завершении вы увидите экран с уведомлением об авторских правах и условиях распространения.

Дважды нажмите клавишу Enter, чтобы принять условия и установить pfSense. Как правило, лучше использовать параметры, заданные по умолчанию.

После установки вы увидите диалоговое окно с предложением выполнить перезагрузку. Выберите вариант Reboot (Перезагрузить) и нажмите клавишу Enter. После перезагрузки pfSense вы опять увидите экран с уведомлением об авторских правах, поскольку виртуальная машина pfSense снова загружается с ISO-образа, который мы использовали ранее. Чтобы это исправить, в меню File (Файл) в верхнем левом углу интерфейса pfSense выберите пункт Close (Закрыть). В появившемся диалоговом окне выберите вариант Power off the machine (Выключить машину) и нажмите кнопку OK (рис. 1.8).

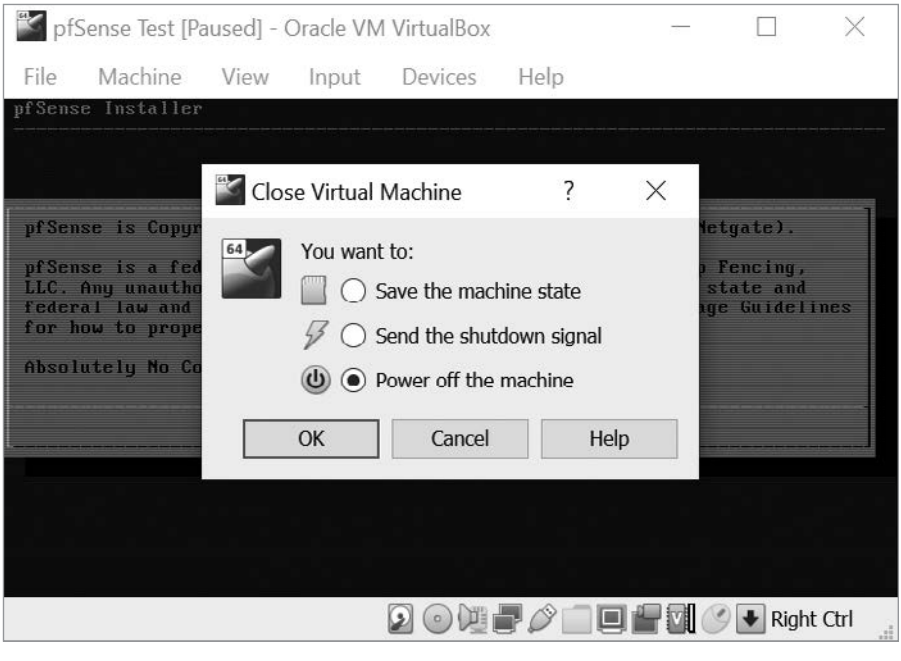

Рис. 1.8. Выключение машины pfSense для удаления ISO-образа

После выключения виртуальной машины pfSense щелкните на ее названии в списке виртуальных машин правой кнопкой мыши и в контекстном меню выберите пункт Settings (Настроить). Перейдите на вкладку Storage (Носители) и щелкните правой кнопкой мыши на ранее выбранном ISO-образе. В контекстном меню выберите пункт Remove Attachment (Удалить прикрепление), как показано на рис. 1.9. Далее вам будет предложено подтвердить удаление оптического привода. Выберите пункт Remove (Удалить), а затем нажмите кнопку OK в правом нижнем углу экрана Settings (Настройки).

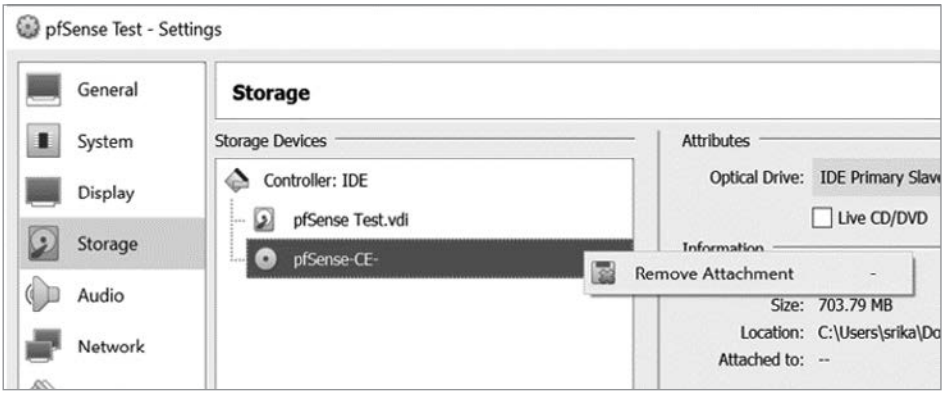

Рис. 1.9. Удаление ISO-образа pfSense

После удаления ISO-образа дважды щелкните на названии pfSense в списке виртуальных машин. Загрузка pfSense займет некоторое время. После этого вы увидите экран со следующим содержимым:

```
Welcome to pfSense               (amd64) on pfSense

WAN (wan)       -> em0       -> v4/DHCP4: 192.1689.1.100/24
LAN (lan)       -> em1       -> v4: 192.168.100.1/24

0) Logout (SSH only)                  9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address       11) Restart webConfigurator
3) Reset webConfigurator password    12) PHP shell + pfSense tools
4) Reset to factory defaults         13) Update from console
5) Reboot system                     14) Disable Secure Shell (sshd)
6) Halt system                       15) Restore recent configuration
7) Ping host                         16) Restart PHP-FPM
8) Shell
```

Настройка Metasploitable

Виртуальная машина Metasploitable представляет собой сервер Linux, намеренно сделанный уязвимым. Это машина, которую мы будем взламывать на протяжении всей книги. Но прежде нам нужно ограничить доступ к ней другим людям. Для этого мы подключим данную машину к внутренней сети, защищенной межсетевым экраном pfSense. Далее описан процесс скачивания и установки этой виртуальной машины.

Скачайте дистрибутив Metasploitable с сайта https://sourceforge.net/projects/metasploitable/. Несмотря на существование более новых версий Metasploitable, мы будем использовать версию 2, поскольку ее проще настроить.

Разархивируйте скачанный ZIP-файл Metasploitable, запустите программу VirtualBox и нажмите кнопку New (Создать). В поле Name (Имя) введите Metasploitable, в списке Type (Тип) выберите вариант Linux, а в списке Version (Версия) — Ubuntu (64bit), после чего нажмите кнопку Continue (Продолжить). При указании объема оперативной памяти задайте рекомендуемое значение. При настройке параметров виртуального жесткого диска выберите вариант Use an existing virtual hard disk file (Использовать существующий виртуальный жесткий диск), щелкните на значке в виде папки и перейдите к разархивированному дистрибутиву Metasploitable. Выберите файл с расширением `.vmdk` и нажмите кнопку Create (Создать). Чтобы настроить параметры сети для машины Metasploitable, щелкните правой кнопкой мыши на ее названии в списке слева и выберите пункт Settings (Настроить) в контекстном меню. Перейдите на вкладку Network (Сеть). В разделе Adapter 1 (Адаптер 1) установите флажок Enable Network Adapter (Включить сетевой адаптер) и выберите созданную ранее внутреннюю сеть (Internal LAN) в раскрывающемся меню Attached to (Тип подключения), как показано на рис. 1.10.

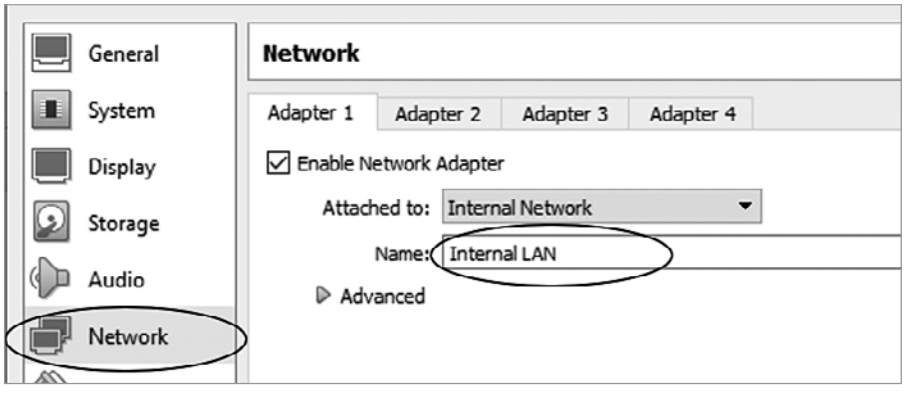

Рис. 1.10. Настройка внутренней сети машины Metasploitable

Откройте виртуальную машину Metasploitable в программе VirtualBox и дождитесь завершения загрузки терминала. На экране должен отобразиться логотип Metasploitable, показанный на рис. 1.11.

Войдите в систему, используя имя пользователя msfadmin и пароль msfadmin.

ПРИМЕЧАНИЕ

Исчезновение указателя мыши говорит о ее захвате виртуальной машиной. Чтобы освободить мышь, нажмите правую клавишу Ctrl (в ОС Windows и Linux) или сочетание клавиш Ctrl+Alt (в macOS).

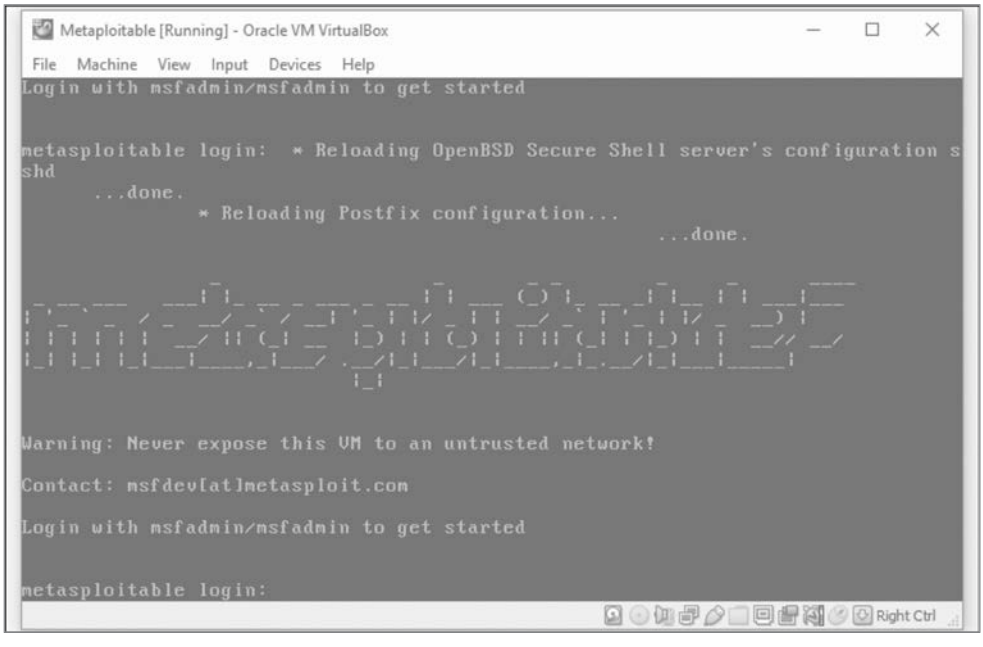

Рис. 1.11. Виртуальная машина Metasploitable после запуска

Настройка Kali Linux

Kali Linux — это дистрибутив Linux, содержащий набор инструментов для тестирования на проникновение. Мы будем использовать виртуальную машину Kali для взлома других машин в нашей виртуальной сети. Скачайте образ Kali Linux для VirtualBox с сайта https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/. Убедитесь, что перечисленные файлы являются образами Kali Linux для VirtualBox, а не для VMWare, и выберите версию образа для VirtualBox, соответствующую версии вашей системы (64- или 32-битную). Добавьте машину Kali в VirtualBox, щелкнув правой кнопкой мыши на скачанном файле OVA и открыв его с помощью VirtualBox. После этого должен появиться экран, содержащий уже сконфигурированные настройки машины. Найдите значок в виде папки в левой части страницы, щелкните на нем и выберите скачанный файл OVA.

ПРИМЕЧАНИЕ

Перед настройкой параметров сети убедитесь в том, что ваша виртуальная машина выключена.