19

Приложение. Настройка лаборатории для пентеста на компьютере с Ubuntu Desktop

В этой главе вы научитесь проектировать и строить виртуализированную лабораторную среду для пентеста на компьютере с Ubuntu Desktop. Это позволит вам снизить затраты: используя технологии виртуализации, вы сможете обойтись без приобретения нескольких физических устройств.

Кроме того, вы узнаете, как развернуть виртуально изолированные сети, чтобы исключить риск случайной атаки на системы, которые вам не принадлежат. Далее вы настроите Kali Linux в качестве машины атакующего и Metasploitable 3 как уязвимую систему-цель. Важно помнить, что при отработке навыков наступательной безопасности (*offensive security*), таких как этичный хакинг и пентест, все действия должны выполняться только в отношении систем и сетей, доступ к которым вам разрешен, поскольку такие проверки безопасности обычно являются инвазивными и могут привести к повреждению систем.

Для завершения построения лаборатории вам придется вернуться к материалам главы 2 «Создание лаборатории пентеста» и главы 3 «Настройка среды для продвинутых методов тестирования на проникновение».

В этой главе мы рассмотрим следующие темы:

- Настройка гипервизора и виртуальных сетей.
- Установка Kali Linux на Ubuntu.
- Установка Metasploitable 3 на Ubuntu.

Приступим!

Технические требования

Чтобы выполнять упражнения этой главы, вам потребуются:

- Oracle VM VirtualBox — https://www.virtualbox.org/wiki/Downloads;
- Oracle VM VirtualBox Extension Pack — https://www.virtualbox.org/wiki/Downloads;
- Kali Linux — https://www.kali.org/get-kali/;
- Vagrant — https://www.vagrantup.com/;
- Metasploitable 3 (Windows and Linux) — https://app.vagrantup.com/rapid7.

Обзор лабораторной среды и технологий

Концепция создания собственной виртуализированной лаборатории для пентеста позволяет максимально эффективно использовать вычислительные ресурсы уже имеющегося у вас компьютера без необходимости приобретать онлайн-доступ к лабораториям у различных провайдеров или покупать дополнительные компьютеры и устройства.

Как преподаватель и практикующий специалист в области кибербезопасности, я заметил, что многие люди, начинающие свой путь в сфере информационных технологий, обычно считают, что для их области обучения необходима физическая лабораторная инфраструктура. В определенной степени это действительно так, однако ввиду развития технологий создание физической лаборатории для отработки навыков имеет множество сопутствующих недостатков.

Перечислю их:

- требуется физическое пространство для размещения серверов и сетевых устройств, которые необходимы для работы;
- энергопотребление каждого устройства приводит к высоким совокупным финансовым затратам;
- стоимость создания или приобретения каждого физического устройства, будь то сетевое оборудование или сервер, является высокой.

Это лишь часть проблем, с которыми сталкиваются студенты и начинающие специалисты в области ИТ. Возможно, у новичка есть лишь один компьютер — настольный или ноутбук. Но технологии виртуализации открывают множество новых возможностей в сфере информационных технологий, чтобы люди и организации эффективнее управляли своими аппаратными ресурсами.

В мире виртуализации гипервизор — это специальное приложение, которое позволяет пользователю виртуализировать операционные системы и применять

аппаратные ресурсы компьютера таким образом, чтобы эти ресурсы могли совместно использоваться другой виртуализированной операционной системой или приложением. Благодаря этому вы можете устанавливать более одной операционной системы поверх уже существующей операционной системы компьютера.

Представьте, что в качестве основной операционной системы (обычно называемой операционной системой хоста) у вас установлена Microsoft Windows 11, но при этом вы хотите на том же компьютере одновременно запускать операционную систему на базе Linux. Сделать это можно с помощью гипервизора. Таким образом, мы будем использовать виртуализацию для построения экономически эффективной лабораторной среды для пентеста.

При проектировании лабораторной среды для тестирования на проникновение нам потребуются следующие компоненты:

- *Гипервизор* — приложение для виртуализации операционных систем и их запуска на любом аппаратном обеспечении. С его помощью можно создавать несколько виртуальных машин, работающих одновременно на одном компьютере. Существует множество гипервизоров, но Oracle VM VirtualBox — предпочтительный вариант, так как он бесплатный и простой.
- *Машина атакующего* — позволяет создавать и запускать различные типы кибератак и угроз с целью выявления и взлома уязвимостей безопасности на целевых системах. В качестве машины атакующего мы будем использовать Kali Linux.
- *Уязвимые машины* — без них лабораторная среда не будет полной. Мы настроим уязвимую систему Metasploitable 2, представляющую собой операционную систему на базе Linux с развернутыми веб-приложениями, и Metasploitable 3 с серверными версиями на базе Windows и Linux. Кроме того, будет развернут Windows Server с двумя клиентскими машинами Windows для изучения уязвимостей безопасности в системах аутентификации Microsoft.
- *Уязвимое веб-приложение* — поможет вам лучше понять, каким образом злоумышленники обнаруживают и взламывают системы защиты в веб-приложениях. Мы настроим веб-приложение OWASP Juice Shop на Kali Linux с контейнером Docker.
- *Доступ в интернет* — настроим на виртуальной машине Kali Linux. Так будет удобнее загружать дополнительные приложения, инструменты и программные пакеты.

На рис. 19.1 показана сетевая топология виртуализированной лабораторной среды для тестирования на проникновение.

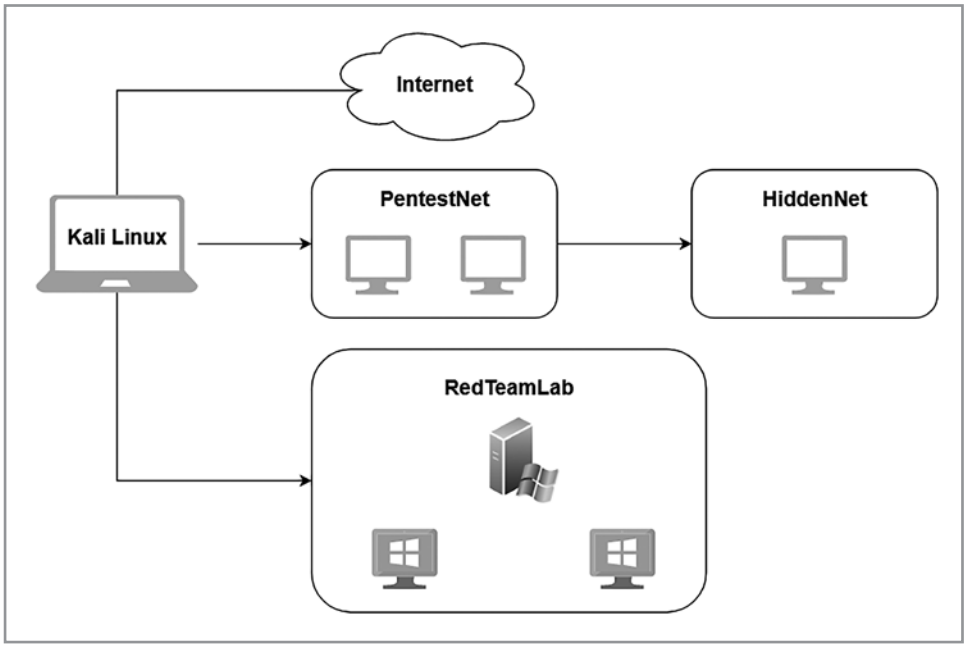

Рис. 19.1. Общая топология сети

Как изображено на схеме, существует четыре сетевые зоны:

- Интернет — используется для доступа к онлайн-ресурсам и напрямую подключен к виртуальной машине Kali Linux.
- Среда `PentestNet` — содержит две уязвимые машины, расположенные в сети `172.30.1.0/24`, и также напрямую подключена к Kali Linux.
- Среда `RedTeamLab` — содержит инфраструктуру *Active Directory (AD)* с сервером Windows и двумя клиентскими машинами, находящимися в сети `192.168.42.0/24`, и напрямую подключена к Kali Linux.
- Среда `HiddenNet` — содержит один уязвимый хост, а именно Metasploitable 3 (на базе Linux) в сети `10.11.12.0/24`, доступ к которому возможен только через сеть `PentestNet`. Следовательно, нам потребуется скомпрометировать один из хостов в среде `PentestNet` и определить, существует ли возможность выполнить латеральное перемещение (pivoting) для дальнейшего развития атаки.

На рис. 19.2 детально показано, какие IP-сети назначены в нашей лабораторной среде.

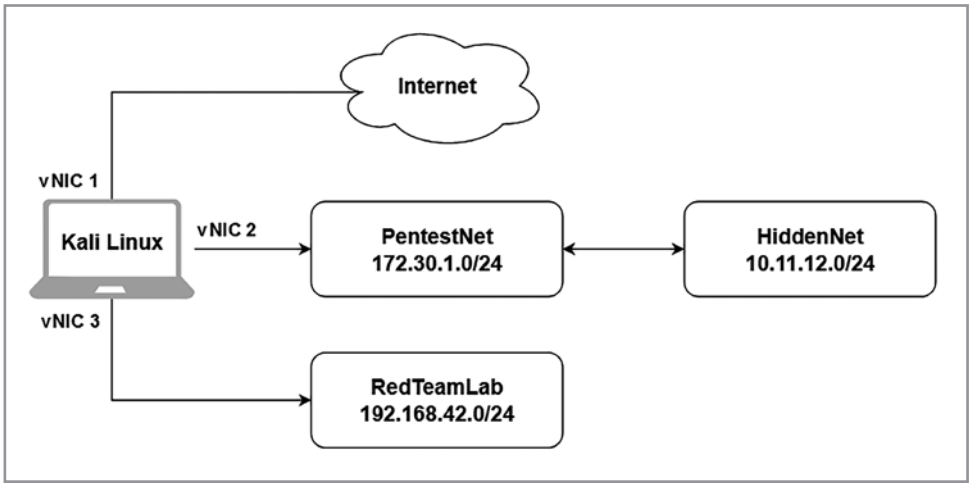

Рис. 19.2. Детальная топология сети

Вы можете видеть, что виртуальной машине Kali Linux будут назначены три сетевых адаптера, которые в гипервизорах обычно называются виртуальными *сетевыми интерфейсными картами (vNIC)*. Эти vNIC позволяют получить доступ:

- к интернету с использованием мостового подключения (bridged connection);
- к среде `PentestNet` в сети `172.30.1.0/24`;
- к среде `RedTeamLab` в сети `192.168.42.0/24`.

Такая архитектура лаборатории идеально подходит для изучения выполнения латерального перемещения между системами, пивотинга (перехода атак с одной сети в другую), а также компрометации среды Active Directory.

Теперь, когда у вас есть представление о виртуальной лабораторной среде, а также о системах и технологиях, с которыми мы работаем на протяжении этой книги, давайте перейдем к настройке гипервизора и виртуальных сетей.

Настройка гипервизора и виртуальных сетей

В ИТ-индустрии существует множество гипервизоров от различных производителей. Oracle VM VirtualBox — это бесплатный и простой в работе гипервизор, который обладает всеми основными функциями, аналогичными коммерческим (платным) продуктам. В этом разделе вы узнаете, как установить Oracle VM VirtualBox и создать виртуальные сети на своем компьютере.

Перед началом работы убедитесь:

- что процессор компьютера поддерживает технологии виртуализации, такие как *VT-x/AMD-V*;
- что функция виртуализации включена в настройках процессора через *BIOS/UEFI*.

ПРИМЕЧАНИЕ

Если вы не уверены, как получить доступ к BIOS/UEFI на вашем компьютере, обратитесь к руководству пользователя устройства или посетите сайт производителя для получения конкретных инструкций.

Чтобы настроить виртуальные сети, следуйте инструкции.

1. Откройте терминал в Ubuntu Desktop и для установки Oracle VirtualBox и пакета расширений (Extension Pack) используйте команды:

```
glen@ubuntu:~$ sudo apt update
glen@ubuntu:~$ sudo apt install virtualbox virtualbox-ext-pack
```

2. Для создания виртуально изолированной сети с помощью VBoxManage из VirtualBox выполните команды:

```
glen@ubuntu:~$ cd /usr/bin/
glen@ubuntu:/usr/bin$ VBoxManage dhcpserver add --netname PentestNet
--ip 172.30.1.1 --netmask 255.255.255.0 --lowerip 172.30.1.20 --upperip
172.30.1.50 --enable
glen@ubuntu:/usr/bin$ VBoxManage dhcpserver add --netname HiddenNet
--ip 10.11.12.1 --netmask 255.255.255.0 --lowerip 10.11.12.20 --upperip
10.11.12.50 --enable
glen@ubuntu:/usr/bin$ VBoxManage dhcpserver add --netname RedTeamLab
--ip  192.168.42.1 --netmask 255.255.255.0 --lowerip 192.168.42.20
--upperip  192.168.42.50 --set-opt=6 192.168.42.40 --enable
```

Рисунок 19.3 показывает выполнение этих команд.

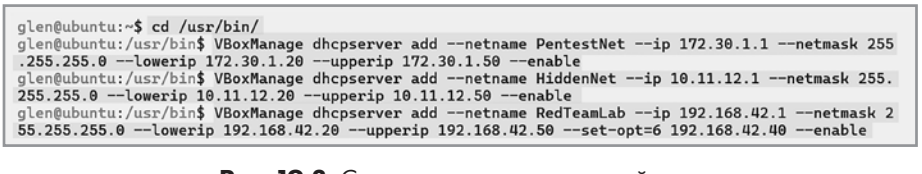

Рис. 19.3. Создание виртуальных сетей

Установка Kali Linux на Ubuntu

1. Откройте веб-браузер в Ubuntu, перейдите по адресу https://www.kali.org/get-kali/ и загрузите версию Kali Linux для VirtualBox. Убедитесь, что загруженный файл сохранен в каталоге Downloads.

2. После завершения загрузки для установки 7-Zip — приложения для распаковки сжатых файлов (Kali Linux) — выполните команду:

```
glen@ubuntu:~$ sudo apt install p7zip-full
```

3. Чтобы перейти в рабочий каталог Downloads и распаковать файл, используйте команды:

```
glen@ubuntu:~$ cd Downloads/
glen@ubuntu:~/Downloads$ 7z x kali-linux-2024.1-virtualbox-amd64.7z
```

Как показано на рис. 19.4, 7-Zip распаковывает файл и извлекает его содержимое.

```
glen@ubuntu:~/Downloads$ 7z x kali-linux-2024.1-virtualbox-amd64.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,16 CPUs AMD Ryzen 9 7900X 12-Core Processor

Scanning the drive for archives:
1 file, 3148943725 bytes (3004 MiB)

Extracting archive: kali-linux-2024.1-virtualbox-amd64.7z
--
Path = kali-linux-2024.1-virtualbox-amd64.7z
Type = 7z
Physical Size = 3148943725
Headers Size = 241
Method = LZMA2:26
Solid = +
Blocks = 1

 10% 2 - kali-linux-2024.1-virtualbox-amd . inux-2024.1-virtualbox-amd64.vdi
```

Рис. 19.4. Извлечение содержимого файла

4. В Ubuntu Desktop откройте меню приложений и нажмите VirtualBox.
5. Когда VirtualBox откроется, нажмите Add (рис. 19.5).

Рис. 19.5. VirtualBox

6. Появится окно Select a virtual machine file (Выбор файла виртуальной машины). Перейдите в каталог Downloads, затем в распакованную папку `Kali-Linux-2024.1-VirtualBox-amd64` и выберите файл `Kali-Linux-2024.1-VirtualBox-amd64.vbox`, после чего нажмите Open (рис. 19.6).

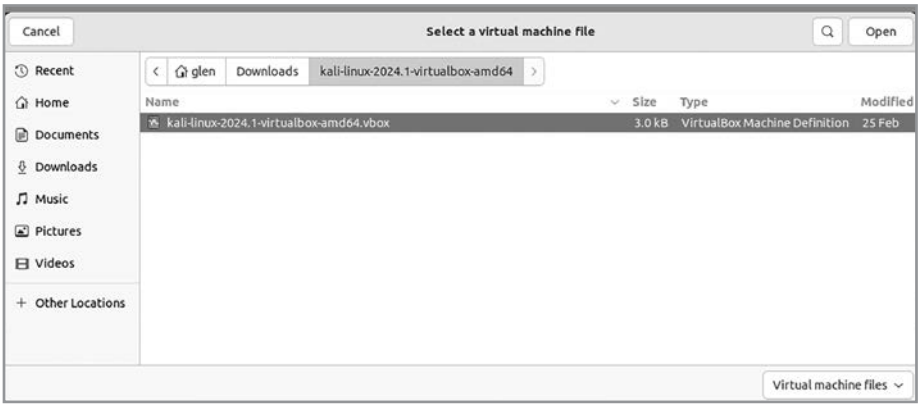

Рис. 19.6. Импорт Kali Linux

7. В VirtualBox выберите только что импортированную виртуальную машину Kali Linux и нажмите Settings (рис. 19.7).

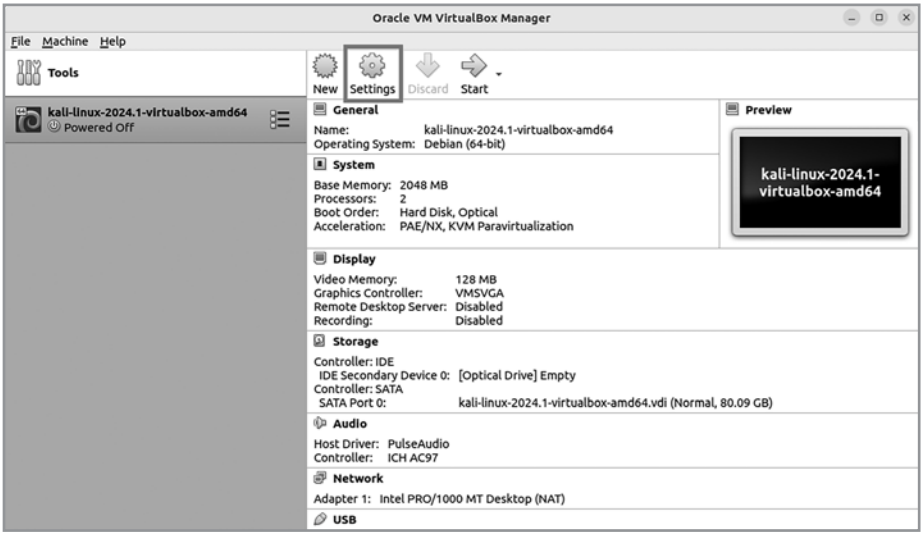

Рис. 19.7. Виртуальная машина Kali Linux

8. В меню Settings виртуальной машины Kali Linux выберите Network ▸ Adapter 1 и задайте следующие параметры:
   - Enable Network Adapter (Сетевой адаптер включен).
   - Attached to: Bridged Adapter.

- Name: с помощью выпадающего списка выберите физический сетевой адаптер, который подключен к вашей физической сети и имеет доступ в интернет.

На рис. 19.8 показано применение к Adapter 1 (vNIC 1) перечисленных выше настроек.

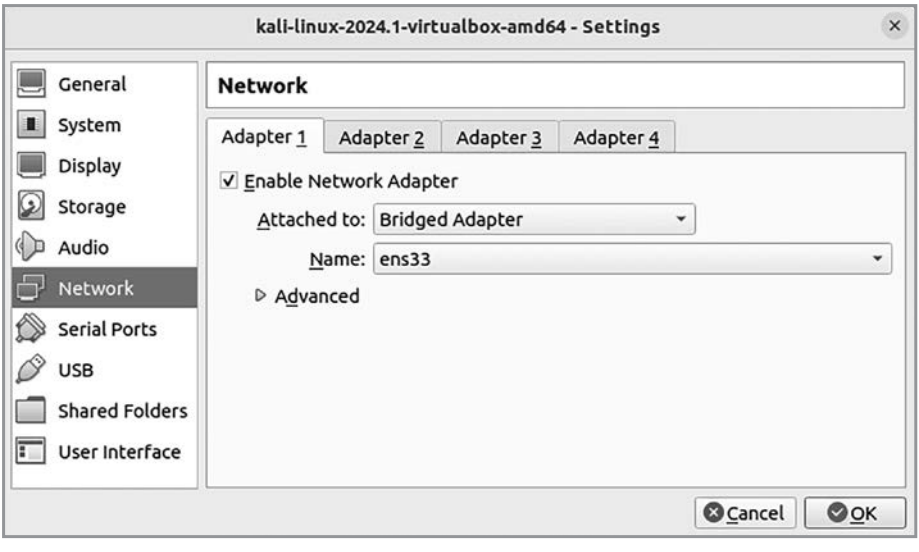

Рис. 19.8. Сетевой адаптер 1

9. Назначим Adapter 2 (vNIC 2) сети `PentestNet`. Выберите вкладку Adapter 2 и задайте следующие параметры:
   - Enable Network Adapter (Сетевой адаптер включен).
   - Attached to: Internal Network.
   - Name: вручную введите `PentestNet` в соответствующем поле.
   - Promiscuous Mode: Allow All.

ПРИМЕЧАНИЕ Включение режима promiscuous на сетевом интерфейсе позволяет машине Kali Linux перехватывать и обрабатывать все пакеты, которые получает данный интерфейс. Это полезно для выполнения захвата и анализа сетевого трафика.

На рис. 19.9 показано применение к Adapter 2 (vNIC 2) перечисленных выше настроек.

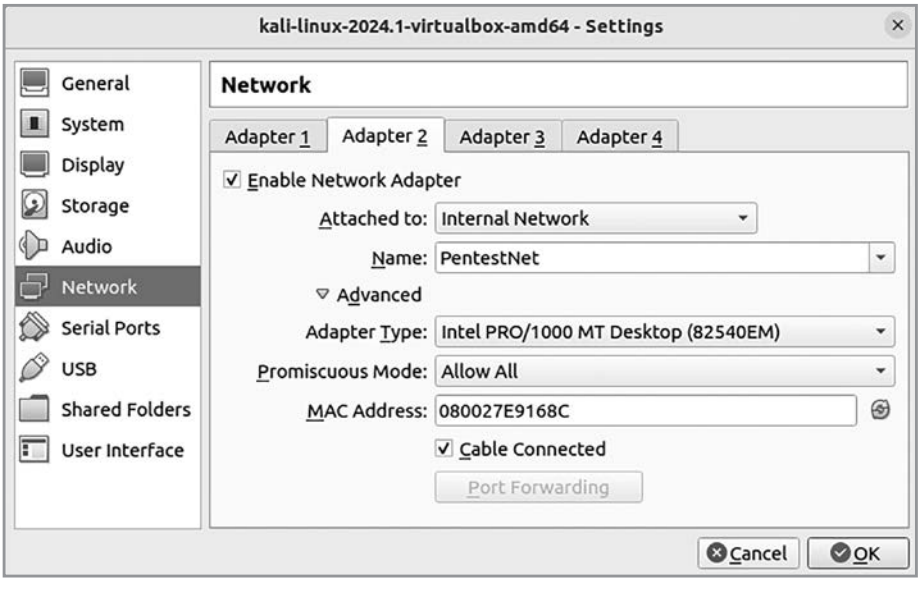

Рис. 19.9. Сетевой адаптер 2

10. Назначим Adapter 3 (vNIC 3) сети `RedTeamLab`. Выберите вкладку Adapter 3 и задайте следующие параметры:
    - Enable Network Adapter (Сетевой адаптер включен).
    - Attached to: Internal Network.
    - Name: вручную введите `RedTeamLab` в соответствующем поле.
    - Promiscuous Mode: Allow All.

На рис. 19.10 показано применение к Adapter 3 (vNIC 3) перечисленных выше настроек.

После настройки сетевых параметров Adapter 3 отключите его, сняв флажок Enable Network Adapter, и нажмите OK, чтобы сохранить настройки виртуальной машины Kali Linux. Мы снова включим Adapter 3, когда он понадобится.

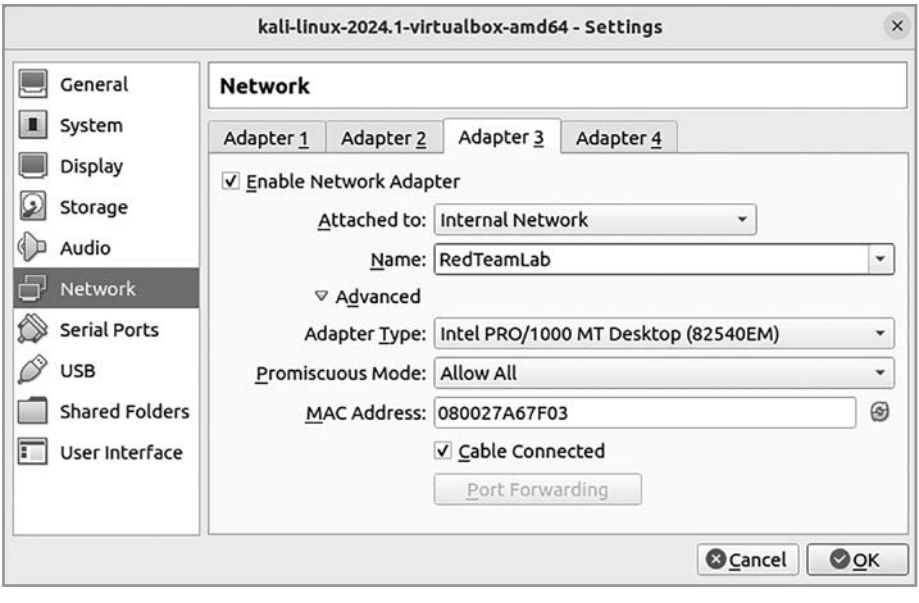

Рис. 19.10. Сетевой адаптер 3

Установка Metasploitable 3 на Ubuntu

В этом разделе вы узнаете, как собрать и развернуть Metasploitable 3 (как версию Windows Server, так и версию Linux Server) на Ubuntu Desktop. Сервер под управлением Windows будет иметь два сетевых интерфейса: один подключен к сети `PentestNet` (`172.30.1.0/24`), а второй — к сети `HiddenNet` (`10.11.12.0/24`). Такая конфигурация позволит нам выполнять пивотинг и латеральное перемещение (lateral movement) между различными сетями. Версия Linux Server будет подключена только к сети `HiddenNet` (`10.11.12.0/24`).

Рисунок 19.11 демонстрирует логические связи между системами и сетями.

Схема показывает, каким образом виртуальные машины связаны между собой в нашей виртуальной лабораторной среде. Например, чтобы получить доступ к Metasploitable 3 — версии Linux, нам сначала потребуется скомпрометировать Metasploitable 3 (на базе Windows) через сеть `PentestNet`, а затем выполнить пивотинг и перенести атаку в сеть `HiddenNet`.

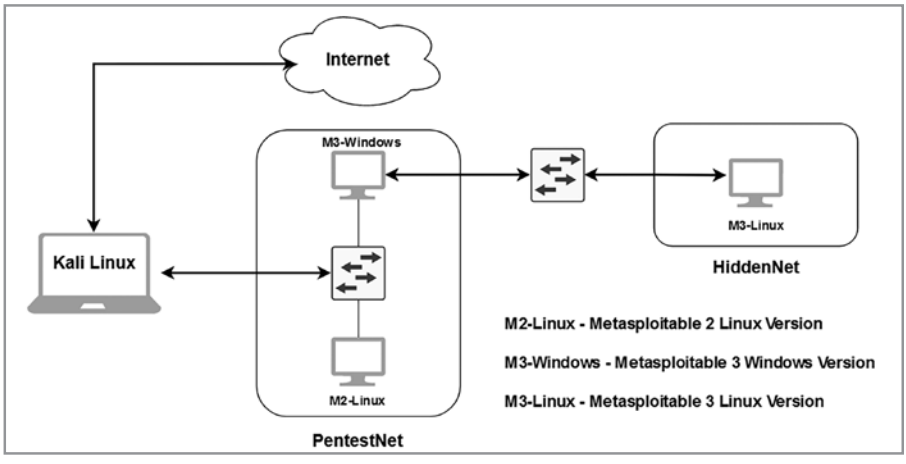

Рис. 19.11. Детальная схема

Часть 1. Сборка версии Windows Server

Чтобы собрать и развернуть Metasploitable 3 (на базе Windows), следуйте инструкции.

1. Откройте терминал в Ubuntu Desktop и для установки и настройки Vagrant используйте команды:

```
glen@ubuntu:~$ cd Downloads/
glen@ubuntu:~/Downloads$ wget -O- https://apt.releases.hashicorp.com/gpg
| sudo gpg --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
glen@ubuntu:~/Downloads$ echo "deb [signed-by=/usr/share/keyrings/
hashicorp-archive-keyring.gpg] https://apt.releases.hashicorp.com $(lsb_
release -cs) main" | sudo tee /etc/apt/sources.list.d/hashicorp.list
glen@ubuntu:~/Downloads$ sudo apt update && sudo apt install vagrant
```

2. Для перезагрузки и установки дополнительных плагинов для Vagrant выполните команды:

```
glen@ubuntu:~/Downloads$ vagrant plugin install vagrant-reload
glen@ubuntu:~/Downloads$ vagrant plugin install vagrant-vbguest
```

Рисунок 19.12 показывает выполнение этих команд.

```
glen@ubuntu:~/Downloads$ vagrant plugin install vagrant-reload
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Fetching vagrant-reload-0.0.1.gem
Installed the plugin 'vagrant-reload (0.0.1)'!
glen@ubuntu:~/Downloads$ vagrant plugin install vagrant-vbguest
Installing the 'vagrant-vbguest' plugin. This can take a few minutes...
Fetching micromachine-3.0.0.gem
Fetching vagrant-vbguest-0.32.0.gem
Installed the plugin 'vagrant-vbguest (0.32.0)'!
```

Рис. 19.12. Перезагрузка плагинов Vagrant

3. Чтобы загрузить Metasploitable 3 — версию Windows Server на ваш компьютер с Ubuntu с помощью Vagrant, используйте команду:

```
glen@ubuntu:~/Downloads$ vagrant box add rapid7/Metasploitable3-win2k8
```

4. Кликните на опции 1, чтобы выбрать VirtualBox в качестве предпочтительного гипервизора (рис. 19.13).

```
glen@ubuntu:~/Downloads$ vagrant box add rapid7/metasploitable3-win2k8
==> box: Loading metadata for box 'rapid7/metasploitable3-win2k8'
    box: URL: https://vagrantcloud.com/api/v2/vagrant/rapid7/metasploitable3-win2k8
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
==> box: Adding box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-win2k8/versions/0.1.0-
weekly/providers/virtualbox/unknown/vagrant.box

==> box: Successfully added box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for 'virtualbox'!
```

A

B

Рис. 19.13. Перезагрузка плагинов Vagrant

5. После завершения процесса загрузки, чтобы переименовать каталог `rapid7-VAGRANTSLASH-Metasploitable3-win2k8`, выполните команды:

```
glen@ubuntu:~/Downloads$ cd ~/.vagrant.d/boxes
glen@ubuntu:~/.vagrant.d/boxes$ mv rapid7-VAGRANTSLASH-Metasploitable3-
win2k8 Metasploitable3-win2k8
```

Рисунок 19.14 показывает успешное выполнение этих команд.

```
glen@ubuntu:~/Downloads$ cd ~/.vagrant.d/boxes
glen@ubuntu:~/.vagrant.d/boxes$ ls -l
total 4
drwxrwxr-x 3 glen glen 4096 Apr 21 10:43 rapid7-VAGRANTSLASH-metasploitable3-win2k8
glen@ubuntu:~/.vagrant.d/boxes$ mv rapid7-VAGRANTSLASH-metasploitable3-win2k8 metasploitable3-win2
k8
glen@ubuntu:~/.vagrant.d/boxes$ ls -l
total 4
drwxrwxr-x 3 glen glen 4096 Apr 21 10:43 metasploitable3-win2k8
```

Рис. 19.14. Инициализация образа Metasploitable 3

6. Чтобы запустить процесс сборки этой виртуальной машины, используйте команды:

```
glen@ubuntu:~/.vagrant.d/boxes$ vagrant init Metasploitable3-win2k8
glen@ubuntu:~/.vagrant.d/boxes$ vagrant up
```

На рис. 19.15 — выполнение этих команд.

```
glen@ubuntu:~/.vagrant.d/boxes$ vagrant init metasploitable3-win2k8   A
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.
glen@ubuntu:~/.vagrant.d/boxes$ vagrant up                            B
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Importing base box 'metasploitable3-win2k8'...
==> default: Matching MAC address for NAT networking...
==> default: Checking if box 'metasploitable3-win2k8' version '0.1.0-weekly' is up to date...
==> default: Setting the name of the VM: boxes_default_1713711081673_83717
==> default: Clearing any previously set network interfaces...
==> default: Preparing network interfaces based on configuration...
    default: Adapter 1: nat
==> default: Forwarding ports...
    default: 3389 (guest) => 3389 (host) (adapter 1)
    default: 22 (guest) => 2222 (host) (adapter 1)
    default: 5985 (guest) => 55985 (host) (adapter 1)
    default: 5986 (guest) => 55986 (host) (adapter 1)
==> default: Running 'pre-boot' VM customizations...
```

Рис. 19.15. Сборка виртуальной машины Metasploitable 3

Сборка обычно занимает несколько минут.

7. После завершения процесса откройте VirtualBox. Вы увидите только что созданную и запущенную виртуальную машину (рис. 19.16).

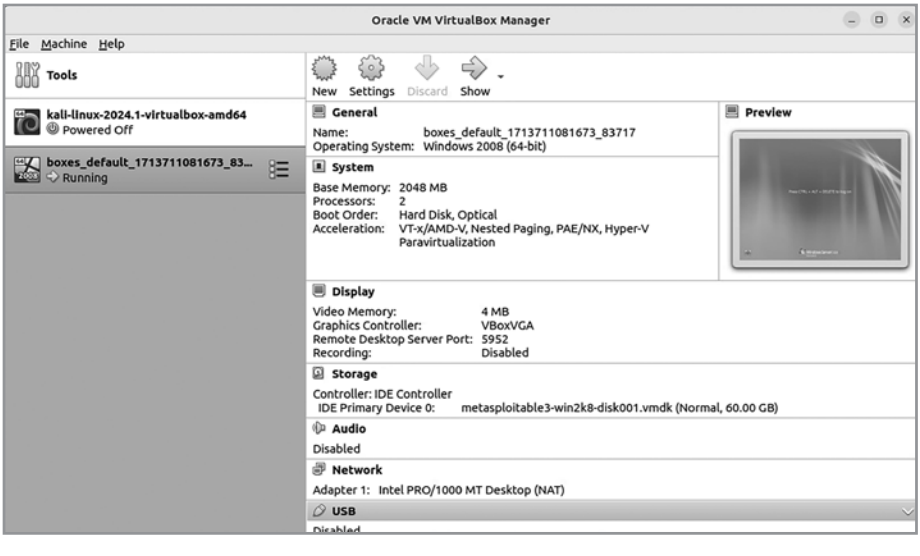

Рис. 19.16. VirtualBox с виртуальной машиной Metasploitable 3

8. Выберите виртуальную машину Metasploitable 3 (на базе Windows) и нажмите Show, чтобы открыть ее из VirtualBox Manager.
9. После запуска виртуальной машины в строке меню виртуальной машины выберите Input ▸ Keyboard ▸ Insert Ctrl-Alt-Del (рис. 19.17).

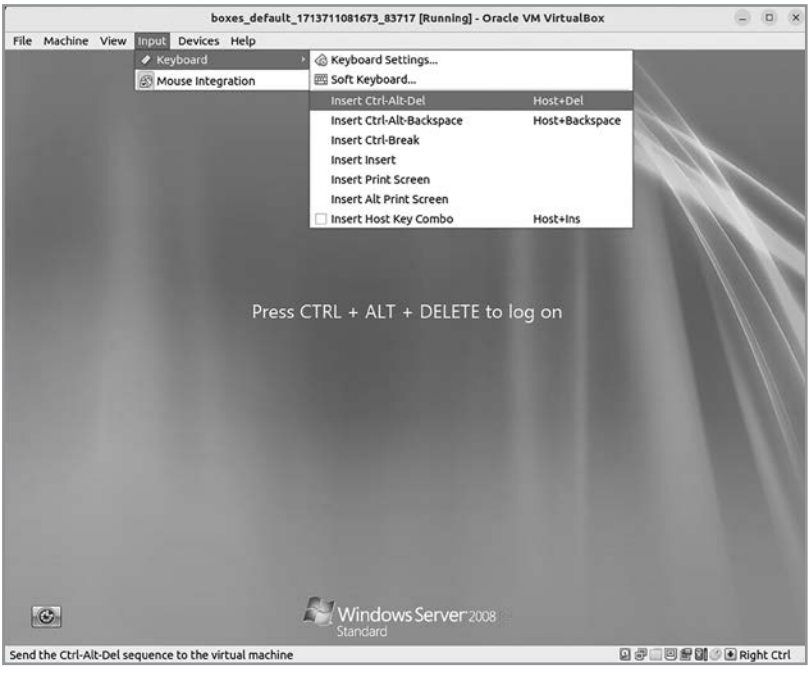

Рис. 19.17. Меню Input в VirtualBox

10. Выберите учетную запись `Administrator` и используйте пароль по умолчанию `vagrant` для входа в систему (рис. 19.18).

Рис. 19.18. Экран входа в систему

11. Войдите на сервер и завершите его работу (выключите систему).
12. После того как виртуальная машина Metasploitable 3 (на базе Windows) будет выключена, выберите эту виртуальную машину и нажмите Settings (рис. 19.19).

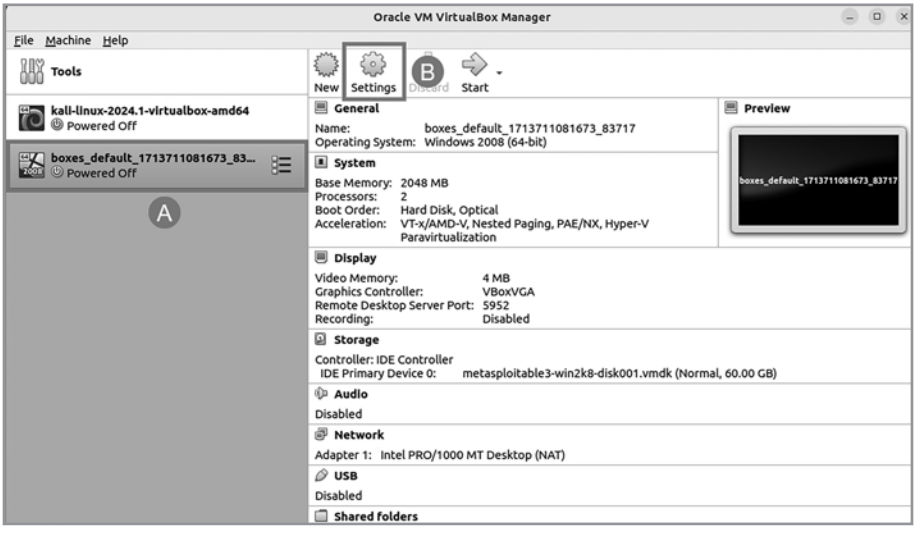

Рис. 19.19. VirtualBox Manager

13. В разделе General ▸ Basic (Общие ▸ Основные) измените имя виртуальной машины по умолчанию (рис. 19.20).

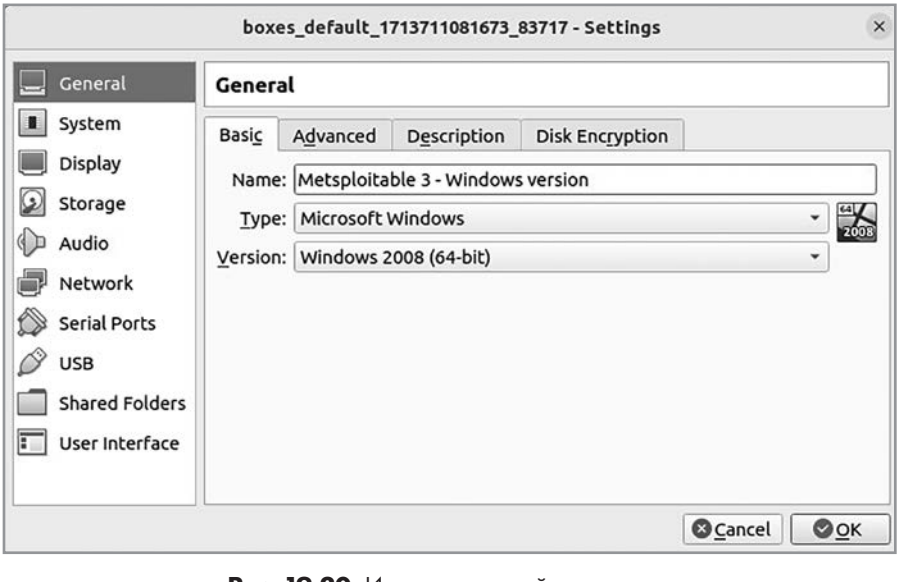

Рис. 19.20. Имя виртуальной машины

14. Выберите Network ▸ Adapter 1 и задайте следующие параметры:
    - Enable Network Adapter (Сетевой адаптер включен).
    - Attached to: Internal Network.
    - Name: вручную введите `PentestNet` в соответствующем поле.
    - Promiscuous Mode: Allow All.

    На рис. 19.21 показаны перечисленные настройки, примененные к Adapter 1.

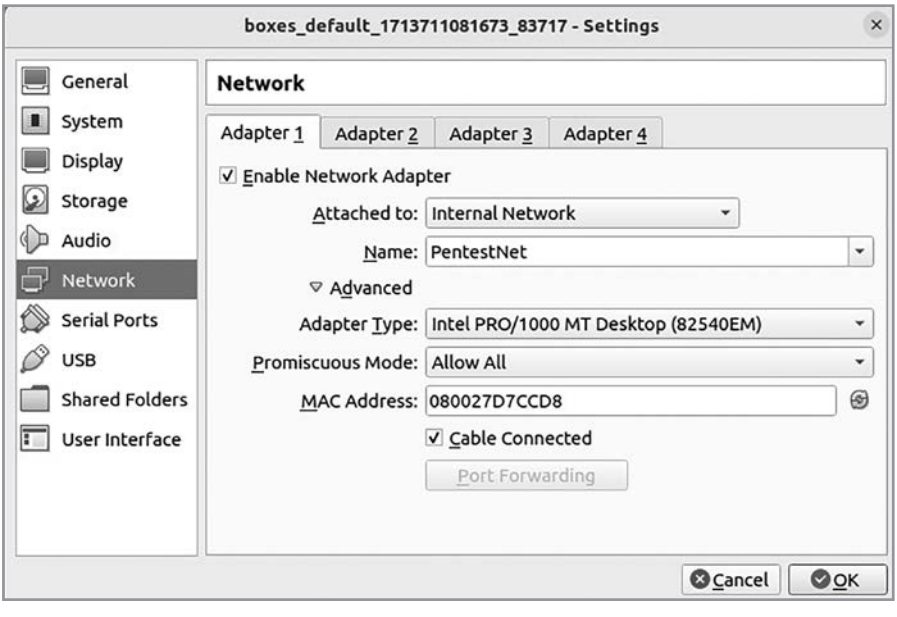

Рис. 19.21. Сетевой адаптер 1

15. Выберите Network ▸ Adapter 2, задайте параметры и нажмите Save (Сохранить):
    - Enable Network Adapter (Сетевой адаптер включен).
    - Attached to: Internal Network.
    - Name: вручную введите `HiddenNet` в соответствующем поле.
    - Promiscuous Mode: Allow All.

На рис. 19.22 показаны перечисленные настройки, примененные к Adapter 2.

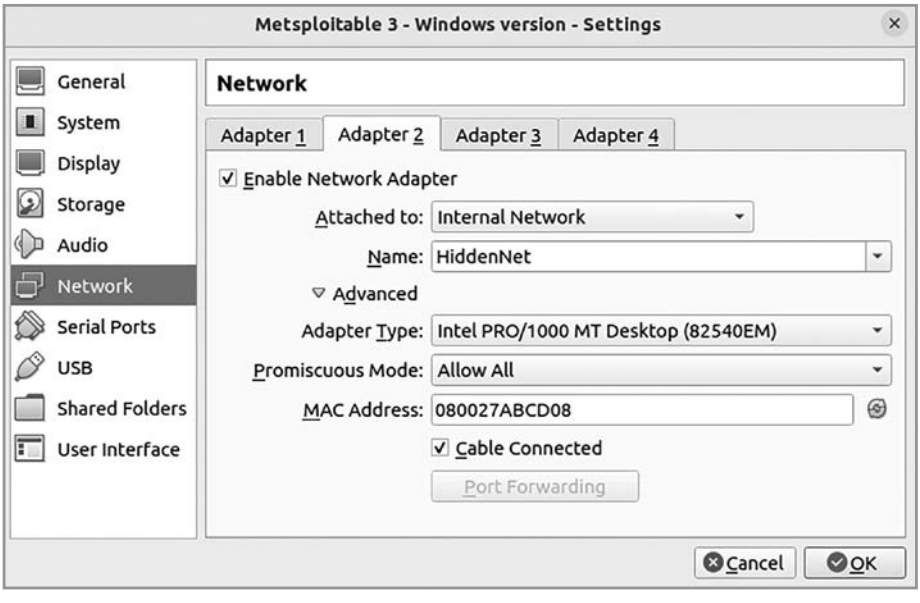

Рис. 19.22. Сетевой адаптер 2

16. Включите виртуальную машину Metasploitable 3 (на базе Windows) и войдите в систему под учетной записью `Administrator`. После входа откройте командную строку Windows и выполните команду `ipconfig`, чтобы убедиться, что виртуальная машина получает IP-адреса из диапазона сетей `172.30.1.0/24` и `10.11.12.0/24` (рис. 19.23).

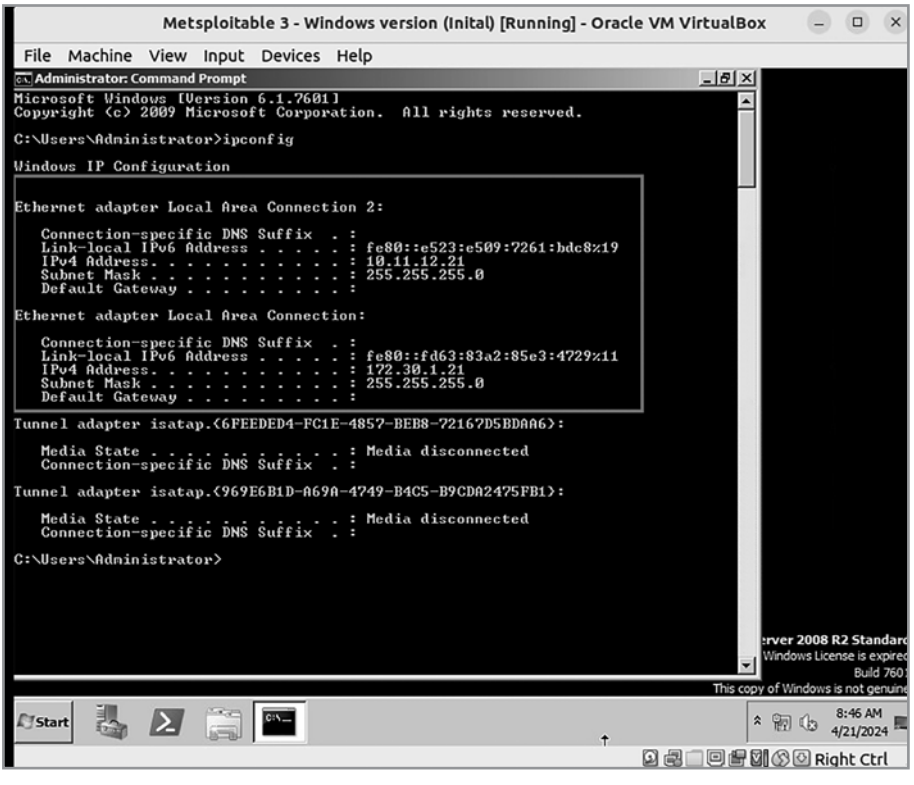

Рис. 19.23. Сетевые адаптеры

17. Закончите упражнение, выключив виртуальную машину.

Часть 2. Сборка версии Linux Server

Чтобы собрать и развернуть Metasploitable 3 версии Linux, следуйте инструкции.

1. В Ubuntu откройте терминал и для загрузки образа Vagrant для Metasploitable 3 версии Linux используйте команды:

```
glen@ubuntu:~$ cd ~/.vagrant.d/boxes
glen@ubuntu:~/.vagrant.d/boxes$ vagrant box add rapid7/Metasploitable3-
ub1404
```

2. Когда появится запрос на выбор провайдера, выберите опцию 1 (рис. 19.24).

```
glen@ubuntu:~/.vagrant.d/boxes$ vagrant box add rapid7/metasploitable3-ub1404
==> box: Loading metadata for box 'rapid7/metasploitable3-ub1404'
    box: URL: https://vagrantcloud.com/api/v2/vagrant/rapid7/metasploitable3-ub1404
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice:
Invalid choice. Try again: 1
==> box: Adding box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for provider: virtualbox
    box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ub1404/versions/0.1.12-weekl
y/providers/virtualbox/unknown/vagrant.box

==> box: Successfully added box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for 'virtualbox'!
```

A

B

Рис. 19.24. Загрузка версии Linux

3. Удалите файл Vagrant с помощью команды:

```
glen@ubuntu:~/.vagrant.d/boxes$ rm Vagrantfile
```

На рис. 19.25 показано выполнение команды.

```
glen@ubuntu:~/.vagrant.d/boxes$ rm Vagrantfile
glen@ubuntu:~/.vagrant.d/boxes$ ls -l
total 8
drwxrwxr-x 3 glen glen 4096 Apr 21 10:43 metasploitable3-win2k8
drwxrwxr-x 3 glen glen 4096 Apr 21 11:21 rapid7-VAGRANTSLASH-metasploitable3-ub1404
```

Рис. 19.25. Удаление файла Vagrant

4. Переименуйте каталог `rapid7-VAGRANTSLASH-Metasploitable3-ub1404` в `Metasploitable3-ub1404` и запустите процесс инициализации для создания виртуальной машины:

```
glen@ubuntu:~/.vagrant.d/boxes$ mv rapid7-VAGRANTSLASH-Metasploitable3-
ub1404 Metasploitable3-ub1404
glen@ubuntu:~/.vagrant.d/boxes$ vagrant init Metasploitable3-ub1404
```

Рисунок 19.26 показывает успешное выполнение этих команд.

```
glen@ubuntu:~/.vagrant.d/boxes$ mv rapid7-VAGRANTSLASH-metasploitable3-ub1404 metasploitable3-ub1404
glen@ubuntu:~/.vagrant.d/boxes$ vagrant init metasploitable3-ub1404
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.
glen@ubuntu:~/.vagrant.d/boxes$
```

Рис. 19.26. Запуск процесса инициализации

5. Откройте File Explorer в Ubuntu Desktop и перейдите в каталог `/home/<username>/.vagrant.d/boxes/Metasploitable3-ub1404/0.1.12-weekly/`

`virtualbox`, затем щелкните правой кнопкой мыши по файлу `box.ovf` и выберите Open With Other Application (Открыть с помощью другого приложения) (рис. 19.27).

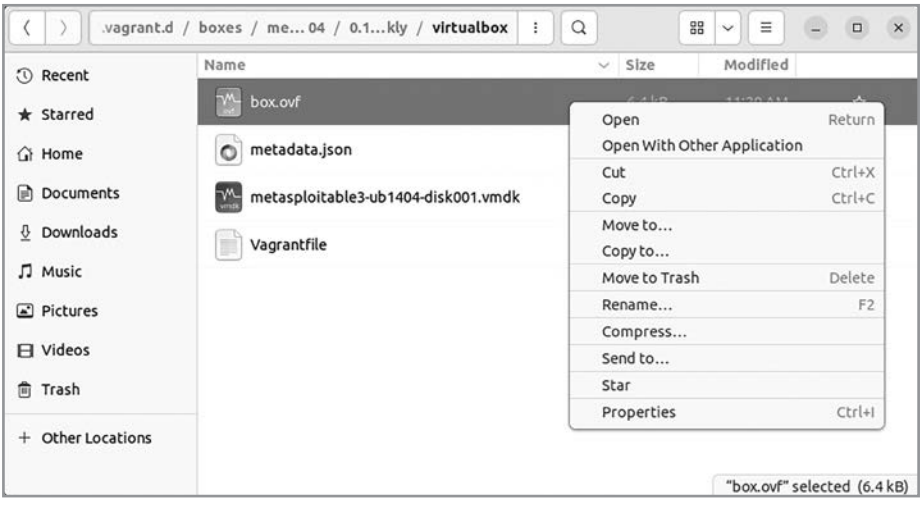

Рис. 19.27. Файлы виртуальной машины

6. В окне Select Application (Выбор приложения) нажмите View All Applications (Показать все приложения) и выберите VirtualBox. После этого появится окно импорта. Нажмите Import (Импортировать) (рис. 19.28).

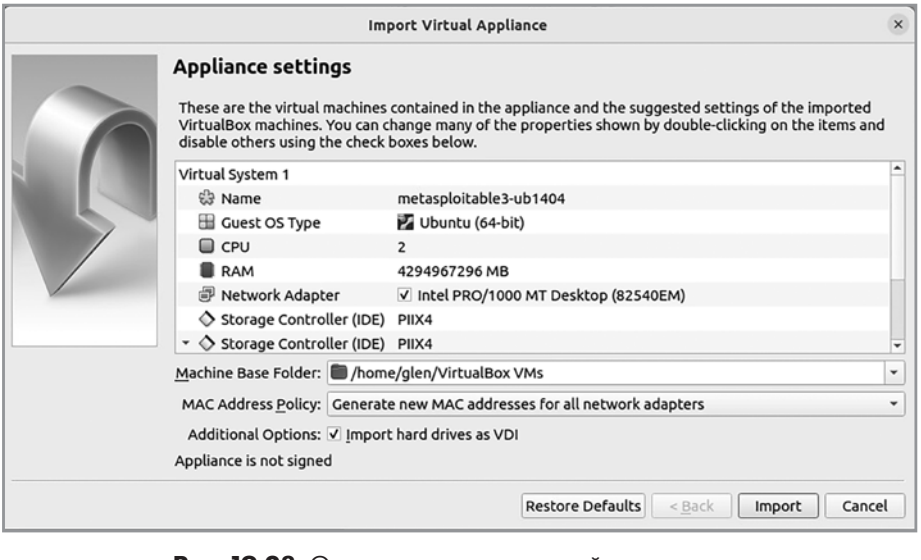

Рис. 19.28. Окно импорта виртуальной машины

7. После завершения процесса импорта виртуальная машина Metasploitable 3 — Linux появится в VirtualBox Manager. Выберите ее и нажмите Settings (рис. 19.29).

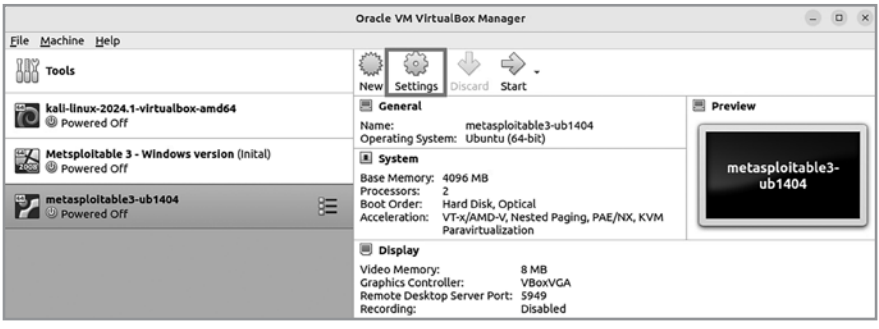

Рис. 19.29. Интерфейс VirtualBox

8. Выберите Network ▸ Adapter 1 и задайте параметры:
   - Enable Network Adapter (Сетевой адаптер включен).
   - Attached to: Internal Network.
   - Name: вручную введите `HiddenNet` в соответствующем поле.
   - Promiscuous Mode: Allow All.

   На рис. 19.30 показаны перечисленные настройки, примененные к Adapter 1.

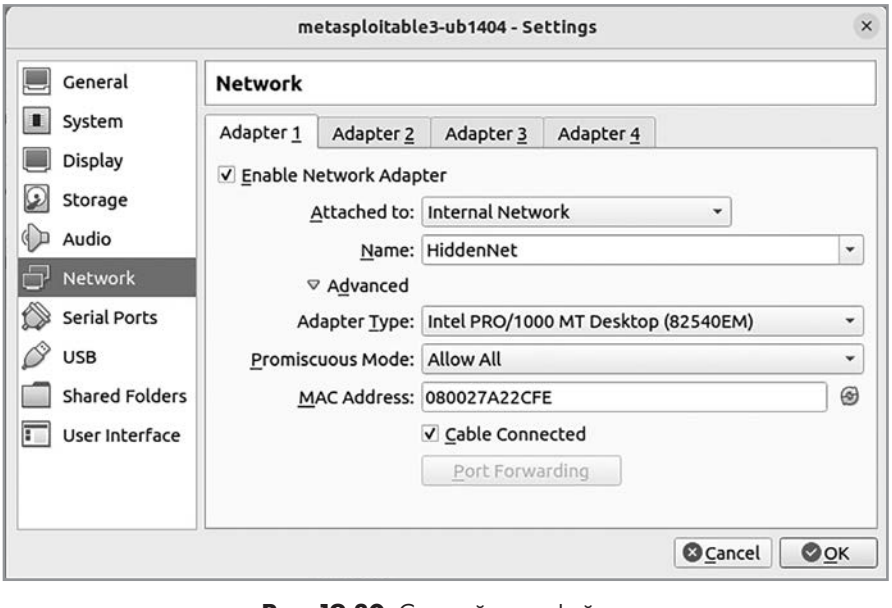

Рис. 19.30. Сетевой интерфейс

9. Нажмите OK, чтобы сохранить настройки.
10. Включите виртуальную машину Metasploitable 3 — Linux и войдите в систему, введя имя пользователя `vagrant` и пароль `vagrant` (рис. 19.31).

Рис. 19.31. Интерфейс Metasploitable 3

11. Выполните команду `ip address`, чтобы убедиться, что виртуальная машина получает IP-адрес в сети `10.11.12.0/24` (рис. 19.32).

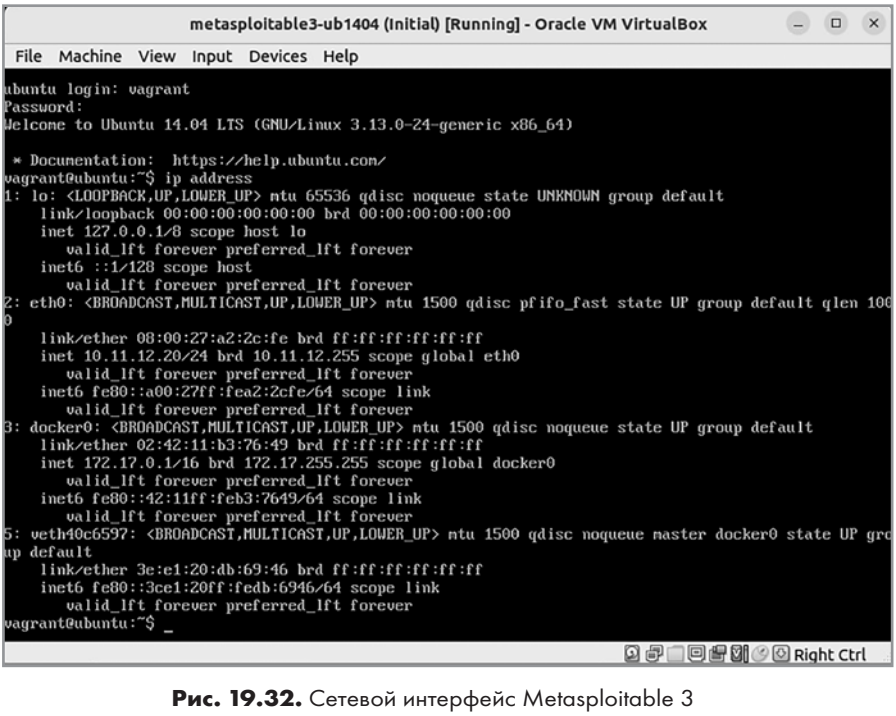

Рис. 19.32. Сетевой интерфейс Metasploitable 3

12. В завершение вы можете использовать команду `sudo halt`, чтобы выключить виртуальную машину.

Краткое содержание

В этой главе было рассмотрено, как настроить гипервизор, создать виртуальные сети и развернуть Kali Linux и Metasploitable 3 в лабораторной среде.

Для завершения построения лаборатории вам следует вернуться к материалам главы 2 «Создание лаборатории пентеста» и главы 3 «Настройка среды для продвинутых методов тестирования на проникновение».