2 Создание испытательной лаборатории

В этой главе мы расскажем, как создать и настроить лабораторию для наших тестов на проникновение. Многие тесты сначала необходимо выполнять в ограниченной лабораторной среде, прежде чем делать это в производственной среде. Помните, перед проведением любого этапа испытаний на проникновение в реальной среде вы должны получить письменное разрешение и в процессе соблюдать все местные законы. Было бы неплохо перед тестированием во избежание всевозможных проблем все детали проведения испытаний обсудить с адвокатом. Некоторые страховые компании также предлагают тестерам на проникновение на случай непредвиденных повреждений застраховать все риски.

Чтобы вы могли избежать юридических проблем и ненужных расходов, мы настоятельно рекомендуем создать лабораторную среду для экспериментального тестирования на проникновение. Это можно сделать как на жестком диске обычного компьютера, так и на виртуальной машине. Используя данную лабораторию, вы сможете увидеть результаты тестов, проанализировать их влияние на оборудование, программное обеспечение и быстродействие, так как многие из этих тестов способны нарушить нормальную работу оборудования, что затронет работу организаций.

В этой главе мы подробно рассмотрим следующие темы.

- Настройка среды Windows на виртуальной машине.
- Установка уязвимых серверов.
- Установка дополнительных инструментов в Kali Linux.
- Сетевые службы в Kali Linux.
- Дополнительные лаборатории и ресурсы.

Технические требования

- Минимальные аппаратные требования: 6 Гбайт оперативной памяти, четырехъядерный процессор 2,4 ГГц, 500 Гбайт свободного места на жестком диске.
- VirtualBox: https://www.virtualbox.org/wiki/Downloads.
- Metasploitable 2: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/.

- Упаковщик: https://www.packer.io/downloads.html.
- Vagrant: https://www.vagrantup.com/downloads.html.
- Metasploitable 3: https://github.com/rapid7/metasploitable3.
- Набор уязвимых веб-серверов: https://d396qusza40orc.cloudfront.net/softwaresec/virtual_machine/BadStore_212.iso.

Физическая или виртуальная?

Решение о том, какую лабораторию создавать: физическую, виртуальную или их комбинацию, зависит от вашего бюджета и доступных ресурсов. Тестирование на проникновение в зависимости от используемых инструментов может быть довольно дорогим. Особенно если вы выбираете коммерческие инструменты. Но, учитывая множество доступных в Kali Linux программ с открытым исходным кодом, без коммерческих инструментов можно обойтись. Кроме того, такие инструменты доступны на GitHub и GitLab.

Для профессионального испытания на проникновение мы имеем две физические машины. Одна — ноутбук, используемый в лаборатории, оснащен жестким диском объемом 1 Тбайт, 16 Гбайт оперативной памяти DDR4, процессором i7 и видеокартой NVIDIA GeForce GTX 1050. На нем установлены три виртуальные машины и основная ОС (Kali Linux 2018.2). Вторая машина — это старая рабочая станция Tower с дисками 2 Тбайт, 24 Гбайт оперативной памяти DDR3 и процессором Intel Xeon 3500 со встроенной видеокартой. На ней установлено несколько виртуальных машин, в том числе используемые в моей виртуальной лабораторной среде.

При создании лабораторной среды необходимо для каждой операционной системы, включая основную ОС и все виртуальные машины, соблюсти хотя бы минимальные рекомендуемые требования. Для комфортной работы без ошибок, связанных с недостатком оперативной памяти, было бы правильно иметь запас оперативной памяти больше рекомендуемого. Учитывая, что большинство операционных систем, созданных на базе Linux, требуют всего 2 Гбайт оперативной памяти, выполнить это требование не так уж и тяжело. Но опять же все зависит от вашего бюджета и доступных ресурсов.

Настройка Windows на виртуальной машине

Поскольку Microsoft Windows 10 — это последняя операционная система от компании Microsoft, мы решили установить ее в своей лаборатории по тестированию на проникновение. Эта операционная система сейчас устанавливается на большинстве новых персональных компьютеров и ноутбуков. Чтобы не повредить свою основную ОС, для проведения тестов Windows 10 лучше установить на виртуальную

машину. Мы рекомендуем установить тестовую операционную систему на виртуальную машину и читателям, у которых в качестве основной ОС установлена более старая версия Windows, MAC или Linux. Конечно, количество компьютеров под управлением Windows 7 постоянно уменьшается. Это объясняется тем, что поддержка данной операционной системы закончилась и эти системы становятся более уязвимыми для злоумышленников. Хотя есть пользователи, хранящие верность Windows 7 и установившие запрет на обновление.

Для этой установки мы используем ознакомительную копию Windows 10 Enterprise Edition, доступную для прямой загрузки с сайта Microsoft. Вы можете скачать ознакомительную копию Windows 10 Enterprise со страницы, расположенной по адресу https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise. Учтите, что ознакомительный срок с этой версией операционной системы равен 90 дням. Далее вы должны или приобрести лицензию, или отказаться от дальнейшего использования системы.

На странице загрузки вы найдете две доступные версии: ISO-образ и версию с долгосрочным обслуживанием (LSTB). Выберите образ ISO — Enterprise и нажмите кнопку Continue (Продолжить). Заполните необходимые поля ввода и снова нажмите кнопку Continue (Продолжить). Пожалуйста, запомните введенные вами данные, так как потребуется с помощью телефонного звонка или СМС пройти проверку подлинности.

Выберите разрядность загружаемой операционной системы (32 или 64 бита), язык и нажмите кнопку Download (Загрузить).

Теперь можно приступить к созданию виртуальной машины Windows 10. Нет никакой разницы, какой виртуальной машиной воспользуетесь вы: VirtualBox или VMware. Мы работали с VirtualBox.

Запустите установленную ранее виртуальную машину и нажмите кнопку New (Создать). Эта кнопка находится в левом верхнем углу окна менеджера виртуальных машин. Присвойте виртуальной машине имя и выберите необходимую версию (32 или 64 бита). Выбор версии зависит от разрядности вашего компьютера и от загруженной версии ISO-образа. Для продолжения нажмите кнопку Next (Далее).

Выделите виртуальной машине объем доступной оперативной памяти. Для Windows 10 рекомендуется выделять не менее 2 Гбайт. Учитывая, что на нашей машине установлено 24 Гбайт оперативной памяти, мы для виртуальной машины Windows 10 выделили чуть больше 6 Гбайт (рис. 2.1).

Создайте новый виртуальный жесткий диск. Для этого в окне Hard Disk (Жесткий диск) установите переключатель в положение Create virtual hard disk new (Создать новый виртуальный жесткий диск) и нажмите кнопку Create (Создать).

В следующем окне Specified Type (Укажите тип) оставьте предлагаемый по умолчанию тип создаваемого диска — VDI (VirtualBox Disk Images) и нажмите кнопку Next (Далее). На экране появится окно File location on size (Укажите формат хранения). Установите переключатель в положение Dynamic virtual hard disk (Динамический виртуальный жесткий диск). Выбрав этот параметр, вы сэкономите место на жестком

диске. Выбирая размер динамического виртуального жесткого диска, вы указываете его максимальный размер, который не может быть превышен. На деле же будет использована только необходимая для работы операционной системы часть выделенного пространства. Нажмите кнопку Next (Далее). Появится окно Name and file size (Укажите имя и размер файла).

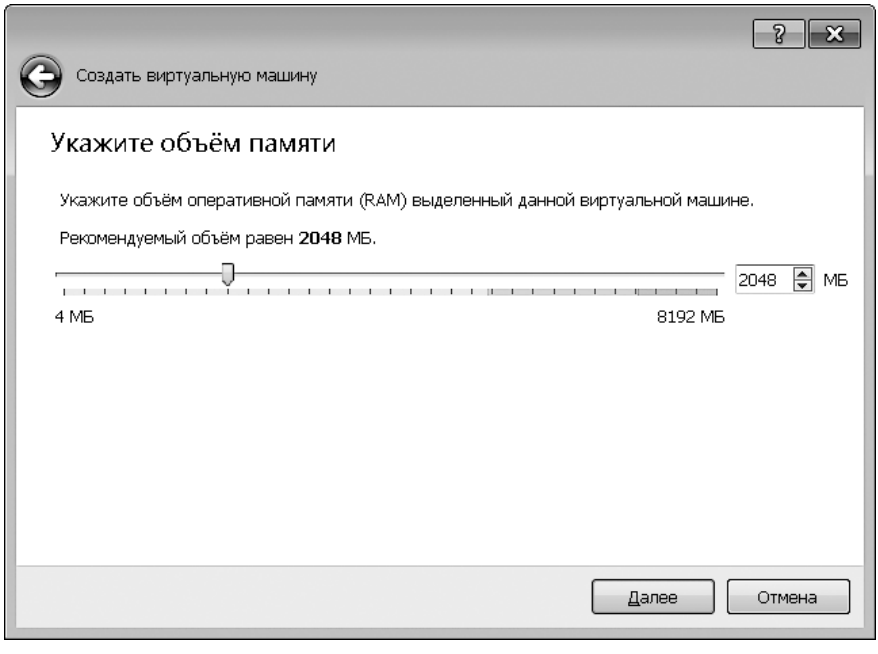

Рис. 2.1. Выделение памяти для виртуальной машины Windows 10

При выборе размера виртуального диска следует учесть, сколько займут сама операционная система и установленные приложения. Нам, например, нужно будет установить Metasploitable. Поэтому для виртуальной машины Windows 10 мы выделили 64 Гбайт. Нажмите кнопку Create (Создать) (рис. 2.2).

Теперь нам нужно указать, где находится ISO-образ устанавливаемой операционной системы. В левой части менеджера виртуальных машин щелкните на названии только что созданной ВМ и нажмите кнопку Start (Начать). Эта кнопка находится на панели инструментов менеджера виртуальных машин. Машина запустится, и вы увидите диалоговое окно Select start-up disk (Выберите загрузочный диск). Выберите образ загрузочного диска. Для этого нажмите кнопку в виде папки, расположенную справа от поля ввода пути к устанавливаемому ISO-образу, и выберите в появившемся окне ранее загруженный ISO-образ ознакомительной копии Windows 10. Для продолжения установки нажмите кнопку Start (Продолжить) (рис. 2.3).

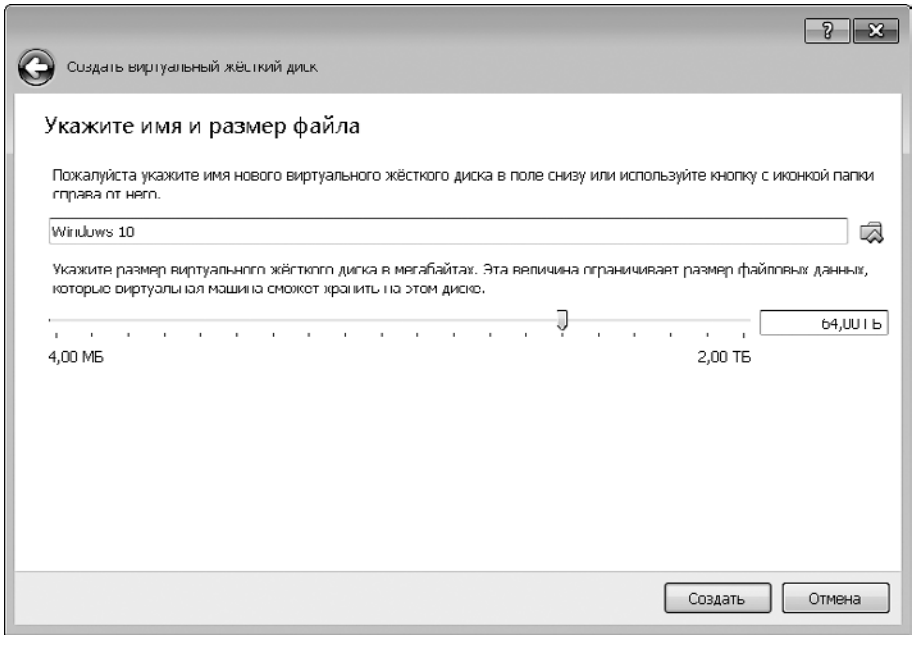

Рис. 2.2. Виртуальная машина подготовлена к установке операционной системы

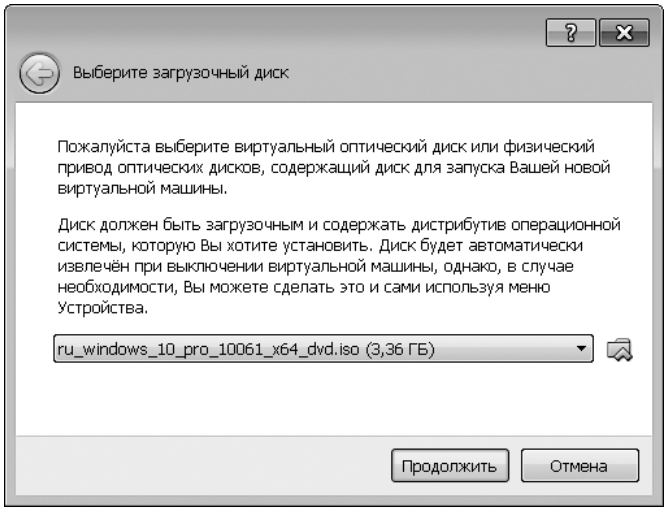

Рис. 2.3. Окно Выберите загрузочный диск

На экране появится заставка программы установки операционной системы Windows 10. Введите необходимую информацию и для продолжения нажмите кнопку Next (Далее).

Чтобы начать процесс установки, нажмите кнопку Install (Установить).

Примите условия лицензии Microsoft и для продолжения нажмите кнопку Next (Далее). Выберите выборочную установку, нажмите кнопку Create (Создать), после чего отформатируйте жесткий диск виртуальной машины (рис. 2.4).

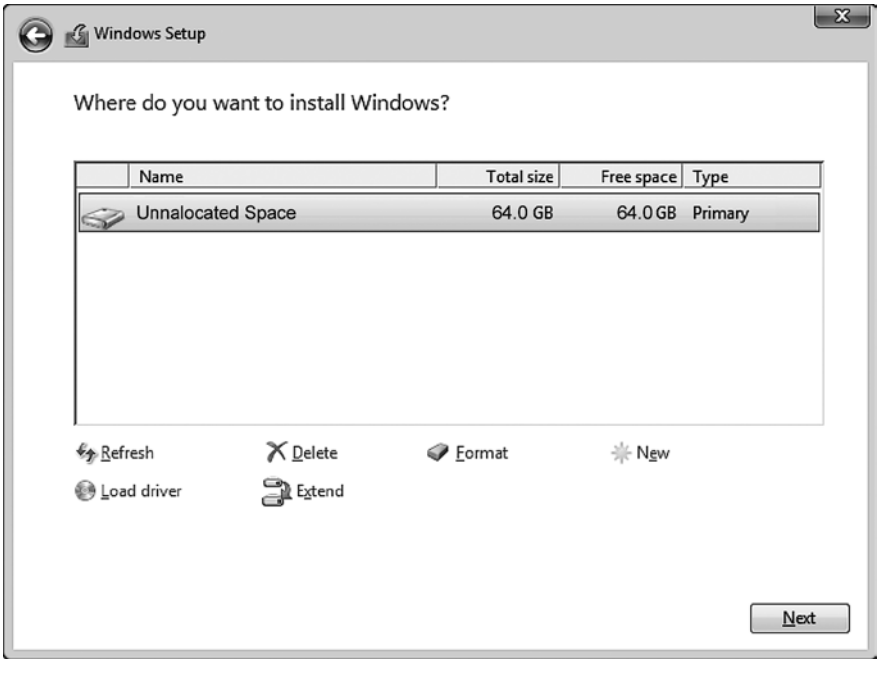

Рис. 2.4. Выберите функцию форматирования виртуального жесткого диска

После форматирования убедитесь, что выбран раздел с указанным ранее размером, и для продолжения нажмите кнопку Next (Далее) (рис. 2.5).

Процесс установки операционной системы займет некоторое время, а вы пока ознакомьтесь со списком других книг по тестированию на проникновение: https://www.packtpub.com/tech/Penetration-Testing.

После того как установка завершится (рис. 2.6), позвольте ОС автоматически перезагрузиться.

После перезагрузки вам сначала будет предложено выбрать язык и раскладку клавиатуры. Далее, перед тем как предложить установить параметры конфиденциальности, система попросит ввести ваш адрес электронной почты. Для настройки безопасного входа нажмите кнопку Set up PIN (Настроить PIN-код). По телефону или путем СМС может потребоваться подтвердить свою личность. После завершения проверки вы сможете установить PIN-код. Обязательно запомните его (это как минимум шесть цифр), так как он потребуется для входа в систему.

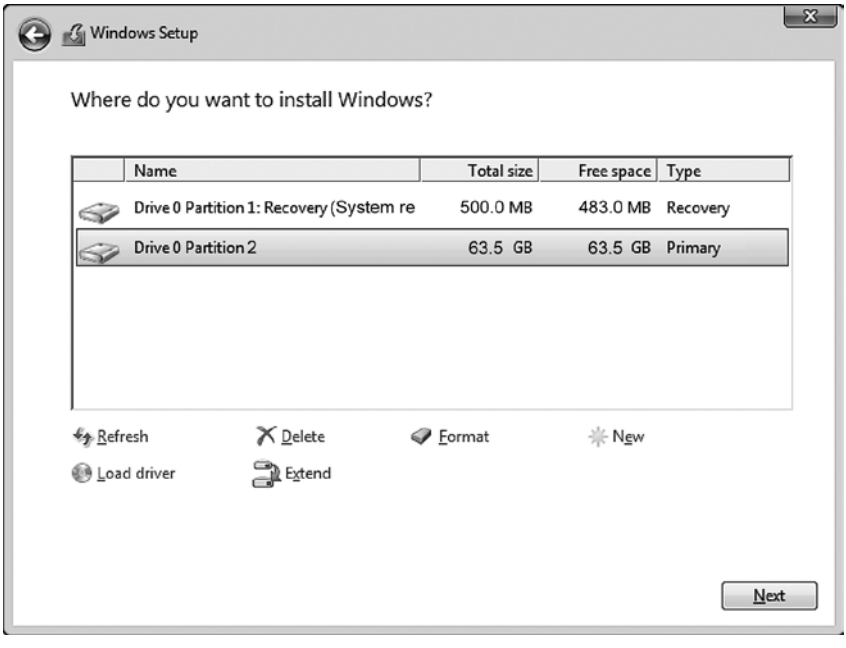

Рис. 2.5. Выбор раздела для установки

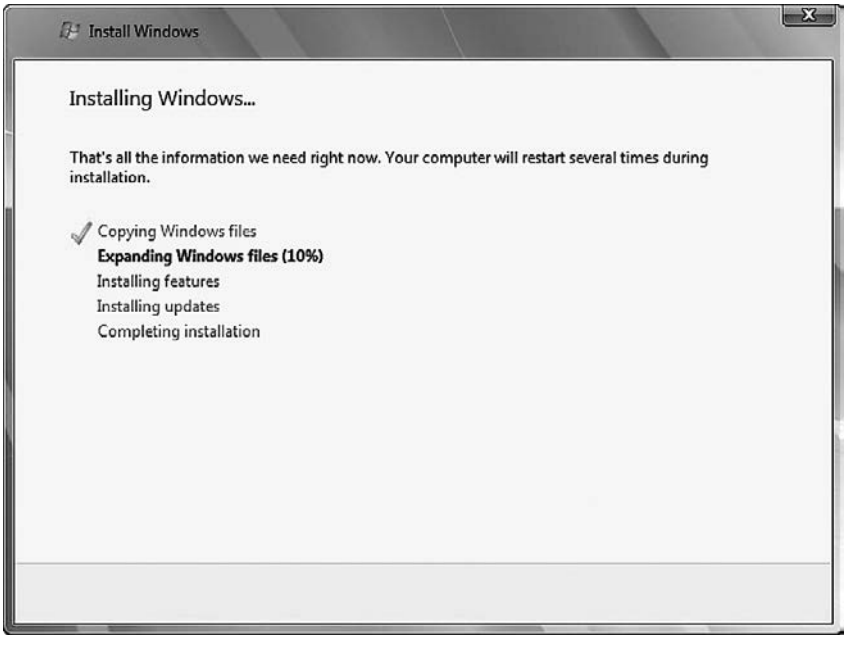

Рис. 2.6. Стадии установки операционной системы Windows 10

После того как установка будет завершена, следует настроить сеть и установить приложения. Подробная информация о вашей ознакомительной копии находится в правом нижнем углу Рабочего стола операционной системы Windows 10 (рис. 2.7).

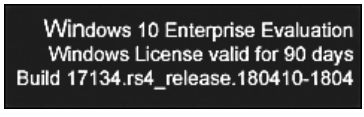

Рис. 2.7. Информация об ознакомительной копии установленной операционной системы

Для быстрого восстановления рабочего состояния виртуальной машины сохраните ее текущее состояние.

Установка уязвимых серверов

В этом разделе в качестве целевой машины мы установим уязвимую виртуальную машину. Она будет использована в нескольких главах книги при рассмотрении конкретных тем. Чтобы вы не нарушали закон, мы решили создать уязвимый сервер на компьютере, а не использовать доступные в Интернете уязвимые серверы. Следует еще раз обратить ваше внимание, что вы никогда не должны без письменного разрешения проникать в другие серверы. Еще одной целью установки виртуальной машины является улучшение ваших навыков контроля. С помощью этих навыков вы легко сможете понять, что происходит в целевой машине, и исправить выявленные проблемы так, чтобы атаки стали неэффективными.

В некоторых странах даже сканирование портов чужой машины считается преступным деянием. Кроме того, мы легко можем восстановить операционную систему, установленную на виртуальной машине.

В следующих разделах в качестве уязвимых серверов мы установим виртуальные машины Metasploitable 2 и Metasploitable 3. Metasploitable 2 — это виртуальная машина ранней версии. Она, в отличие от Metasploitable 3, проще в установке и настройке. Metasploitable 3 — более новая версия, в которой учтены все обновления уязвимостей. Но процедура установки Metasploitable 3 немного отличается от установки предыдущей версии виртуальной машины, и у новичков могут возникнуть некоторые затруднения, поэтому мы расскажем вам, как установить и настроить обе виртуальные машины, и рекомендуем при наличии свободных ресурсов опробовать каждую из них.

Настройка Metasploitable 2 на виртуальной машине

Metasploitable 2 — это уязвимая виртуальная машина, которую мы собираемся использовать. Ее создал знаменитый Х. Д. Мур (H. D. Moore) из Rapid7.

Кроме Metasploitable 2, существуют и другие уязвимые системы, которые можно использовать для обучения тестированию на проникновение. Ознакомьтесь с этими системами по адресу https://www.vulnhub.com.

В Metasploitable 2 предусмотрено множество уязвимостей как на уровне операционной системы, так и на уровне сети и веб-приложений.

Информацию об уязвимостях, содержащихся в Metasploitable 2, можно найти на сайте Rapid7 по адресу https://community.rapid7.com/docs/DOC-1875.

Для установки Metasploitable 2 на виртуальную машину VirtualBox выполните следующие действия.

1. Загрузите файл Metasploitable 2 со страницы по адресу http://sourceforge.net/projects/metasploitable/files/Metasploitable2/.
2. Распакуйте ZIP-файл Metasploitable 2. Когда архив будет распакован, вы увидите пять файлов:
   - `Metasploitable.nvram`;
   - `Metasploitable.vmdk`;
   - `Metasploitable.vmsd`;
   - `Metasploitable.vmx`;
   - `Metasploitable.vmxf`.
3. Создайте в VirtualBox новую виртуальную машину. Назовите ее Metasploitable2, в раскрывающемся списке Type (Тип) выберите операционную систему Linux, а в списке Version (Версия) — Ubuntu.
4. Выделите память объемом 1024 Мбайт.
5. В настройках виртуального жесткого диска установите переключатель в положение Use existing hard disk (Использовать существующий жесткий диск). Выберите ранее извлеченные файлы Metasploitable.
6. Чтобы этот сервер был доступен только из основной операционной системы и с виртуальной машины Kali Linux, измените настройки сети, определив тип подключения как Host-only adapter (Внутренняя связь). Обратите внимание: чтобы Kali Linux была видна только для основной ОС и установленных в ней виртуальных машин, также выберите в сетевых настройках Kali Linux тип подключения Host-only adapter (Внутренняя связь).
7. Запустите виртуальную машину Metasploitable2. Когда процесс загрузки виртуальной машины завершится, войдите в консоль Metasploitable2, используя следующие учетные данные:
   - имя пользователя: msfadmin;
   - пароль: msfadmin.

   Так выглядит консоль Metasploitable 2 после входа в систему (рис. 2.8).

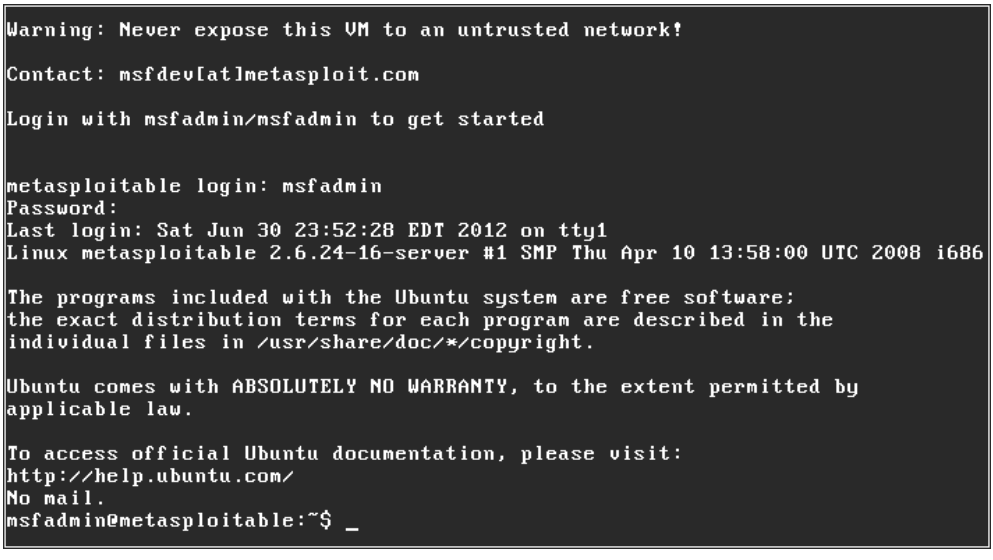

Рис. 2.8. Консоль Metasploitable 2 после входа в систему

Настройка Metasploitable 3 на виртуальной машине

Metasploitable 3, выпущенная Rapid7 в 2016 году, — версия с самыми последними обновлениями. По сравнению с предшествующей версией она имеет больше уязвимостей. Однако версии загружаемой виртуальной машины Metasploitable 3 не существует. Кроме того, Metasploitable 3 нуждается в установке и настройке нескольких дополнительных компонентов. При этом необходимо, чтобы пользователь самостоятельно создал виртуальную машину.

В этом примере виртуальная машина Metasploitable 3 будет установлена на компьютере под управлением Windows 10. Но сначала потребуется загрузить следующие компоненты:

- виртуальную машину VirtualBox или VMware. Мы получили сообщения, что при использовании VirtualBox с версией 5.2 могут возникнуть проблемы. Хорошие результаты получаются, если работать с VirtualBox версии 5.1.14;
- Packer;
- Vagrant.

Установка Packer

Packer от Hashicorp позволяет легко создавать автоматизированные образы, такие как Metasploitable 3. Чтобы загрузить версию Packer, соответствующую вашей операционной системе, посетите страницу загрузки: https://www.packer.io/. Разрядность

вашей операционной системы можно посмотреть в диалоговом окне System (Система) (рис. 2.9).

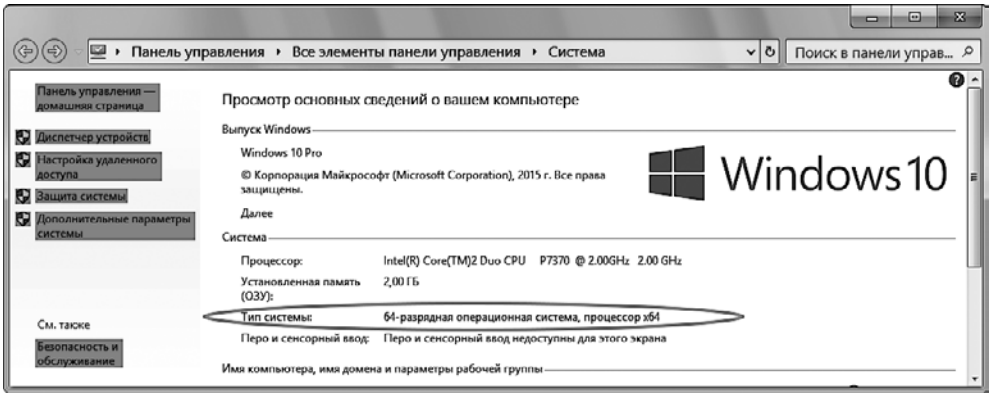

Рис. 2.9. Проверка разрядности вашей операционной системы

По окончании загрузки извлеките файлы из архива. После извлечения вы увидите исполняемый файл `packer.exe`.

Создайте в любом удобном для вас месте папку под именем `packer`. Мы эту папку создали как корневую на диске C (рис. 2.10).

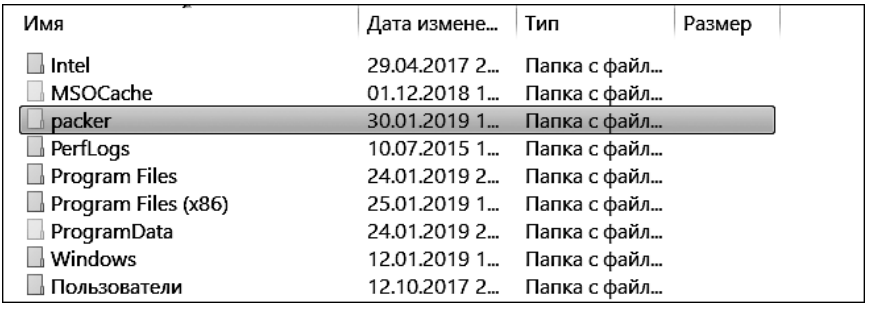

Рис. 2.10. Папка Packer создана

Теперь для запуска этого приложения из командной строки необходимо добавить к созданной папке путь. Для этого выполните следующие действия.

1. Перейдите в Control Panel ▸ System (Панель управления ▸ Система) и щелкните на строке Advanced system setting (Дополнительные параметры системы) (рис. 2.11).
2. В окне System Properties (Свойства системы) щелкните кнопкой мыши на вкладке Advanced (Дополнительно). Далее на открытой вкладке нажмите кнопку Environment Variables (Переменные среды) (рис. 2.12).

   Под пользовательскими переменными вы должны увидеть запись пути для admin.

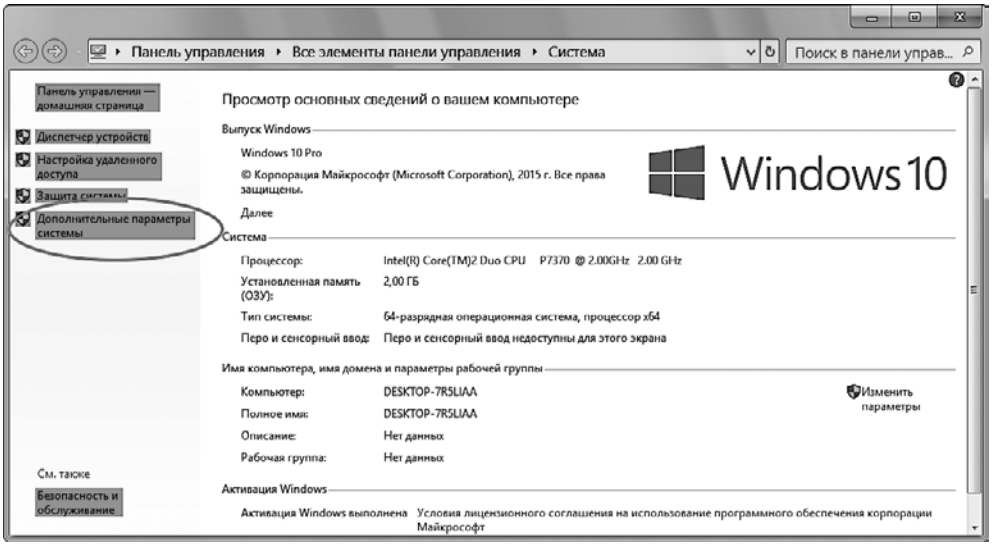

Рис. 2.11. Панель управления

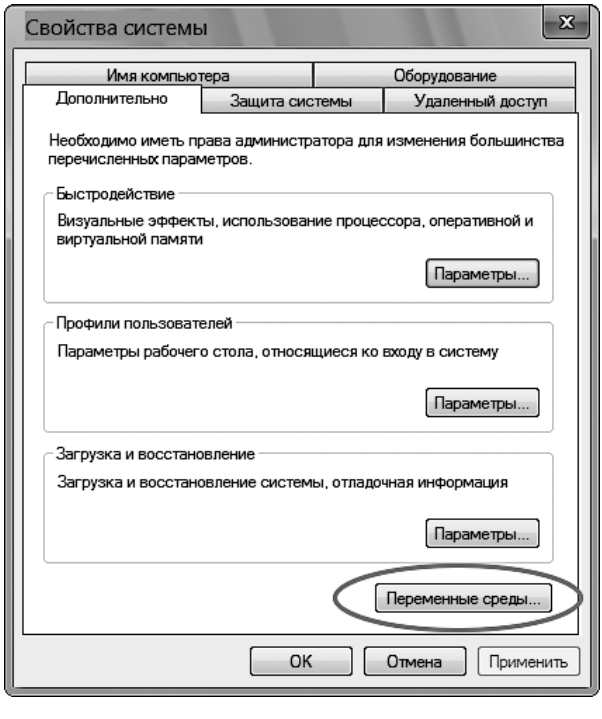

Рис. 2.12. Вкладка Advanced (Дополнительно) окна System Properties (Свойства системы)

3. В поле System variables (Системные переменные) укажите путь к переменной `Path`: `C:\Program Files (x86)\Common Files\Oracle|Java\javapath` (рис. 2.13).

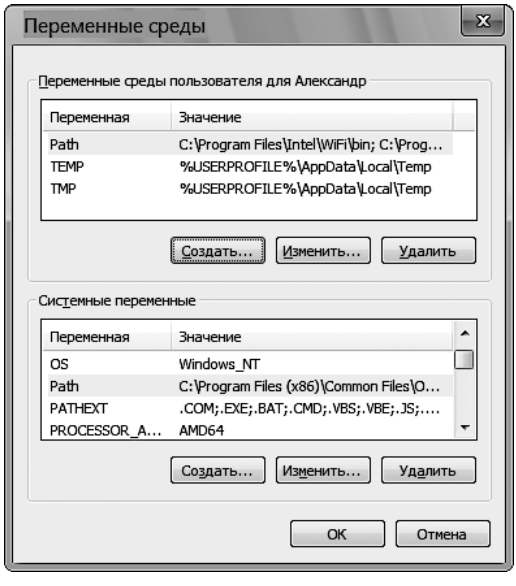

Рис. 2.13. Редактирование пути системной переменной

4. Для продолжения нажмите кнопку Edit (Редактировать). Нажмите в появившемся окне расположенную в правом верхнем углу кнопку New (Создать), выберите из списка `C:\packer` и нажмите кнопку OK.

Чтобы проверить, правильно ли был отредактирован путь, запустите командную строку и введите `packer`. Если все было сделано правильно, в окне терминала вы увидите все доступные команды и аргументы (рис. 2.14).

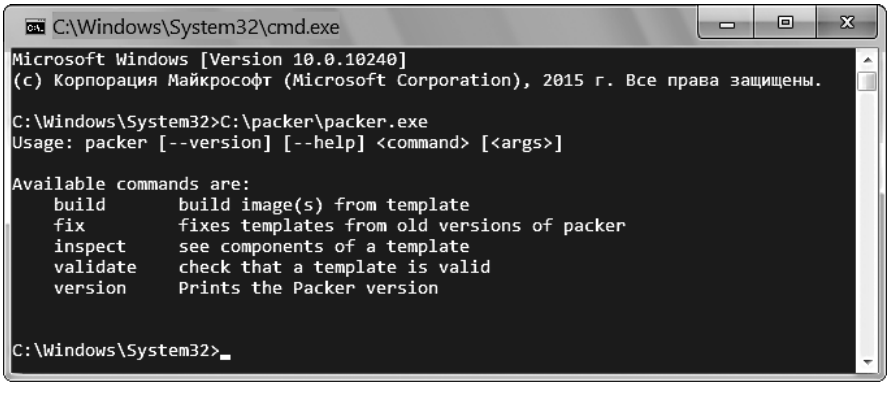

Рис. 2.14. Приложение packer запущено

Установка Vagrant

Vagrant, как и Hashicorp, — приложение с открытым исходным кодом, которое используется для упрощения рабочих процессов и конфигураций в виртуальных средах. Для загрузки подходящей вашей ОС Windows версии программы посетите страницу https://www.vagrantup.com/downloads.html.

После установки соответствующего загрузчика (в данном случае Windows) установите Vagrant.

Мы предполагаем, что VirtualBox у вас уже установлен. Загрузите исходные файлы Metasploitable 3 (рис. 2.15) из репозитория GitHub, который расположен по адресу https://github.com/rapid7/metasploitable3.

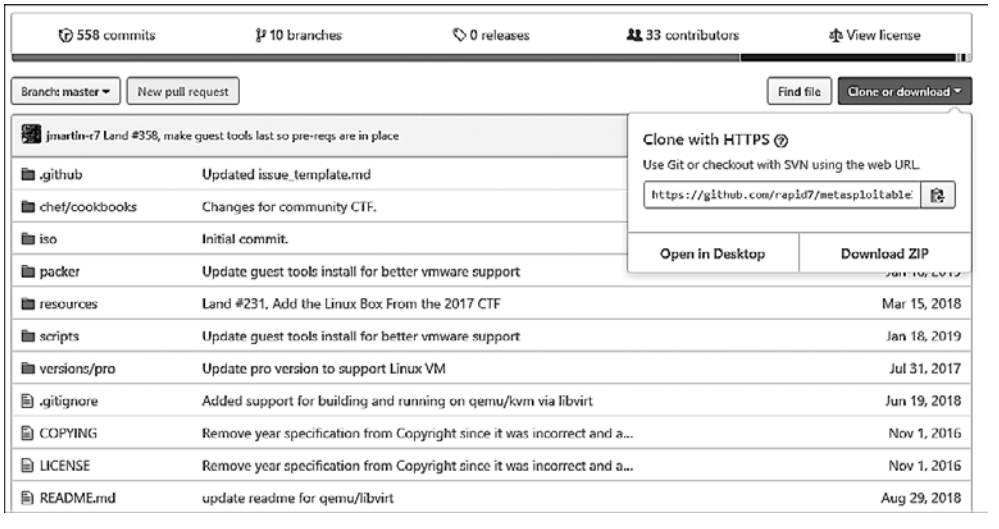

Рис. 2.15. Загрузка исходных файлов Metasploitable 3

Распакуйте загруженный архив в удобную для вас папку. Запустите PowerShell в Windows 10 и, перебирая каталоги, выберите папку с распакованными исходными файлами Metasploitable 3. Далее введите команду `/build_win2008`. Начнется сборка вашего сервера Metasploit 3. Учтите, что она может занять некоторое время. Хоть для начинающих это сложно, но все же попробуйте.

Предварительная настройка Metasploitable 3

Если со сборкой сервера Metasploit 3 возникли сложности, загрузите предварительно собранную версию, которую можно найти на странице GitHub: https://github.com/brimstone/metasploitable3/releases.

Эта версия Metasploitable 3 была создана компанией Brimstone и доступна для скачивания. Размер `.ova`-файла (`Metasploitable3-0.1.4.ova`) всего 211 Мбайт. После загрузки его можно открыть в VirtualBox. Для этого в виртуальной машине

его нужно выбрать и импортировать. По возможности увеличьте предустановленный в 1 Гбайт объем ОЗУ.

Хотя процесс установки и занимает некоторое время, установщик все выполнит автоматически. И в конце вы получите полную версию Metasploitable 3 с Windows Server 2008 (рис. 2.16).

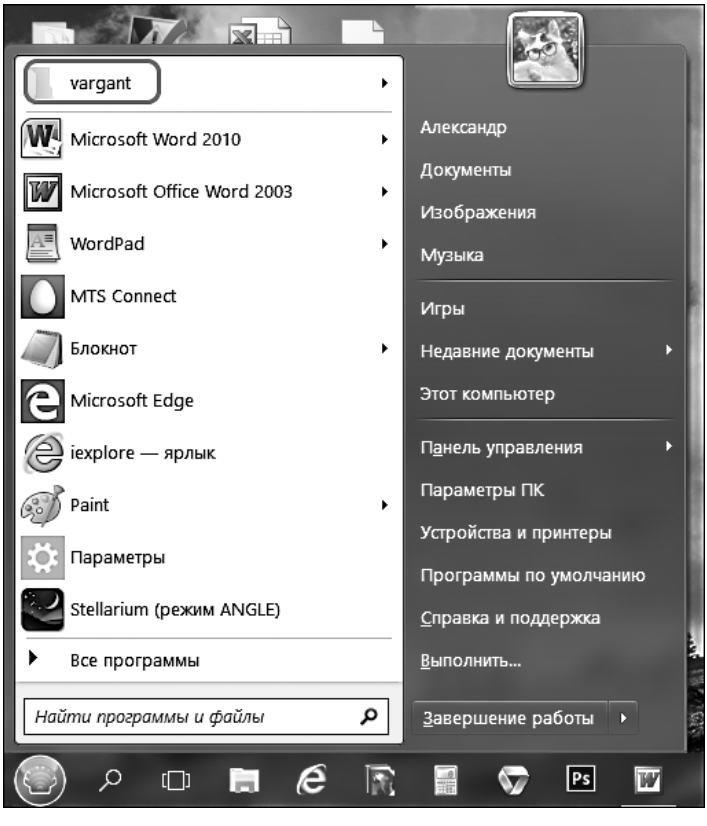

Рис. 2.16. Metasploitable 3 установлена

Установка и настройка BadStore на виртуальной машине

Badstore ISO, по сравнению новыми технологиями, устарел. Однако, в отличие от Metasploitable 3, он невероятно прост в установке и использовании.

Поскольку этот ISO-образ содержит хорошо известные эксплойты, а его размер не превышает 15 Мбайт, начинающие пользователи или читатели с ограниченными ресурсами могут задействовать приложение BadStore для начала проведения тестов на проникновение.

На момент написания этой книги в официальном магазине образ ISO BadStore больше не доступен. Но есть несколько надежных ссылок, по которым его еще

можно скачать. Эти ссылки доступны в статье GitHub по адресу https://github.com/jivoi/junk/blob/master/coursera_software-security/w3/project-2/info.

Кроме того, ISO-образ BadStore можно скачать здесь: https://d396qusza40orc.cloudfront.net/softwaresec/virtual_machine/BadStore_212.iso. Загрузите также руководство для BadStore ISO, так как там содержится важная информация о подключении IP и уязвимостях в ОС.

После того как файл загрузится, запустите VirtualBox и выберите команду меню File ▸ New (Файл ▸ Создать). Введите данные, как показано на рис. 2.17. Для продолжения нажмите кнопку Next (Далее).

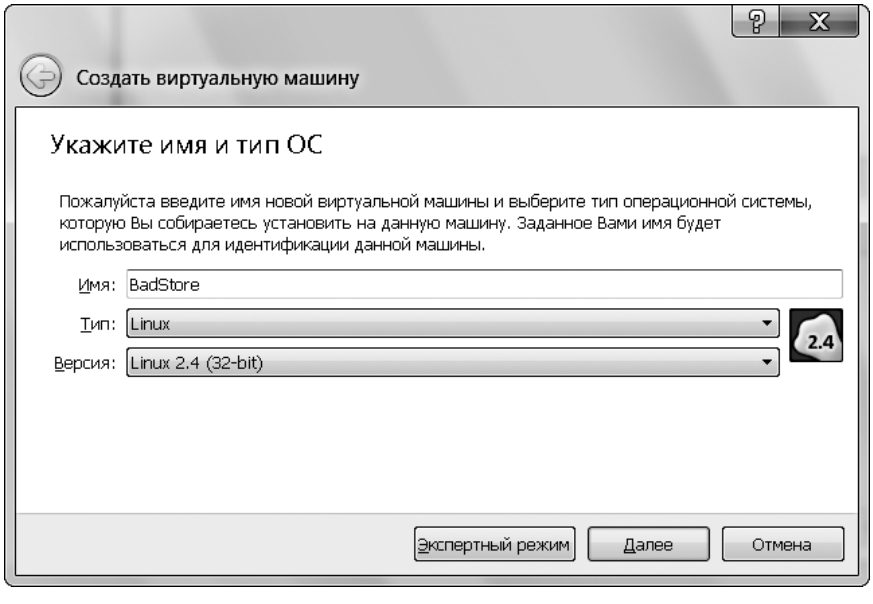

Рис. 2.17. Создание виртуальной машины для BadStore

Для работы BadStore требуется очень мало оперативной памяти. Вы можете использовать объем, предлагаемый по умолчанию. Мы же выделили 640 Мбайт. Чтобы продолжить, нажмите кнопку Next (Далее) (рис. 2.18).

Для завершения установки выполните следующие действия.

- Установите переключатель в положение Create a virtual hard disk now (Создать виртуальный жесткий диск), а затем нажмите кнопку Create (Создать).
- Выберите VirtualBox Disk Image (VDI) в качестве типа файла жесткого диска и нажмите кнопку Next (Далее).
- Установите переключатель в положение Dynamic virtual hard disk (Динамический виртуальный жесткий диск) и нажмите кнопку Next (Далее).
- Поскольку BadStore не требует большого объема жесткого диска, оставьте предлагаемый по умолчанию размер 4 Гбайт.

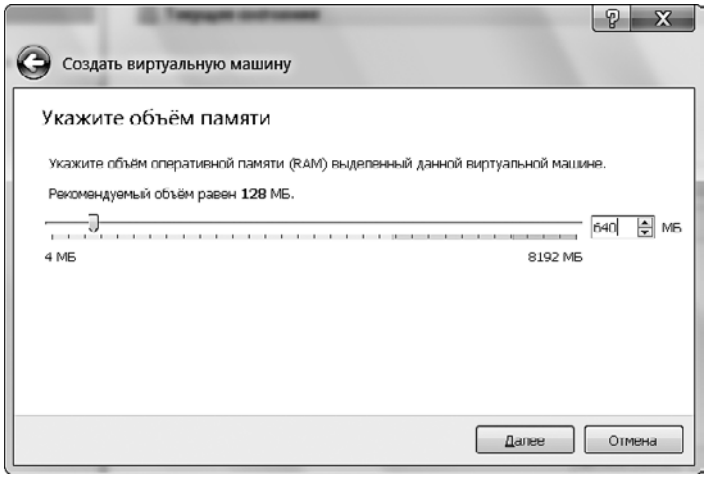

Рис. 2.18. Выделение оперативной памяти для BadStore

Перед запуском виртуальной машины BadStore следует изменить некоторые настройки. В менеджере виртуальных машин щелкните на названии вновь установленной машины и нажмите кнопку Setting (Параметры). Откройте вкладку Network (Сеть), выберите тип подключения Bridged Adapter (Сетевой мост) и нажмите кнопку OK.

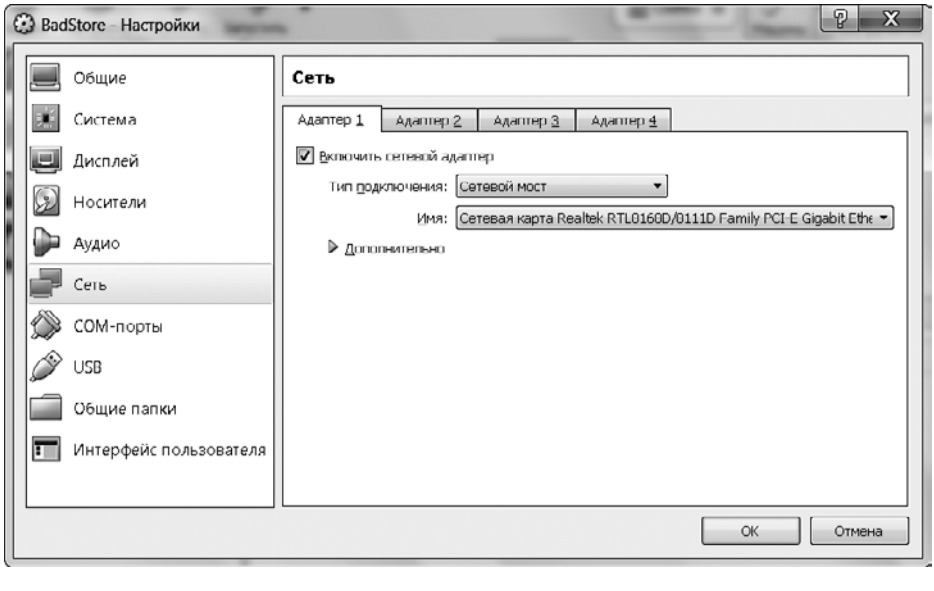

Рис. 2.19. Выбор типа сетевого адаптера для виртуальной машины BadStore

В менеджере виртуальных машин щелкните на названии машины BadStore и нажмите кнопку Start (Начать) (рис. 2.20).

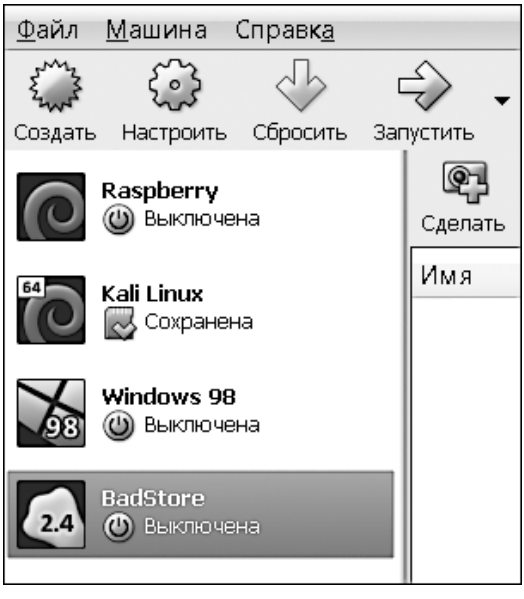

Рис. 2.20. Запуск виртуальной машины BadStore

После запуска виртуальной машины и появления диалогового окна с просьбой выбрать загрузочный диск нажмите кнопку с изображением папки и выберите ранее загруженный файл `BadStore.iso`. Для запуска виртуальной машины нажмите кнопку Start (Начать).

После того как BadStore будет загружена, для запуска консоли нажмите клавишу Enter (рис. 2.21).

После нажатия клавиши Enter для просмотра конфигураций интерфейса введите команду `ifconfig` и снова нажмите Enter.

Конфигурация интерфейса показана на рис. 2.22. Здесь активен интерфейс eth0 с IP-адресом 192.168.3.136. На вашей машине значение IP-адреса должно быть другим. Запомните IP-адрес, который увидите в консоли вашей машины. К виртуальной машине BadStore будете подключаться через браузер именно по этому IP-адресу.

Откройте любой браузер и введите в адресной строке IP-адрес виртуальной машины BadStore: `cgi-bin/badstore.cgi`.

В консоли на нашей машине IP-адрес интерфейса eth0 был 192.168.3.180, поэтому мы для доступа к виртуальной машине BadStore ввели в адресную строку браузера следующий URL-адрес: http://192.168.3.136/cgi-bin/badstore.cgi.

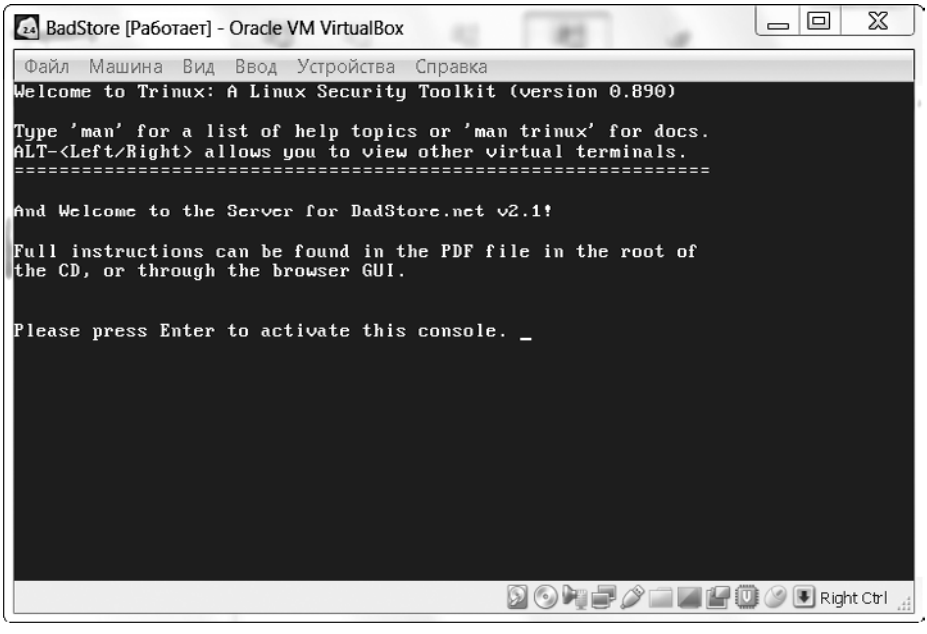

Рис. 2.21. Запуск консоли BadStore

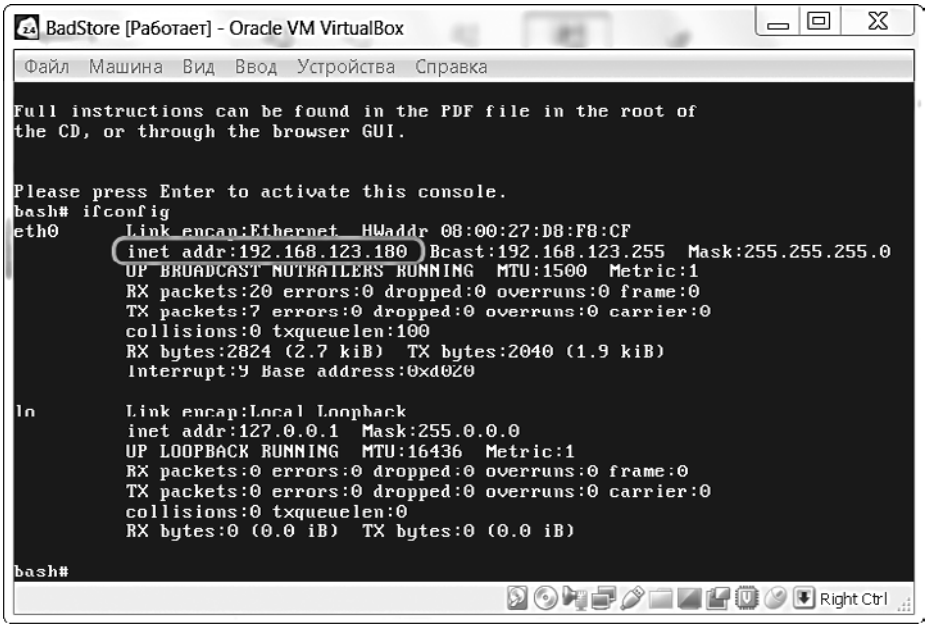

Рис. 2.22. Конфигурация интерфейса eth0

После того как вы введете URL с IP-адресом вашей виртуальной машины BadStore, нажмите клавишу Enter. В окне браузера вы увидите интерфейс BadStore (рис. 2.23).

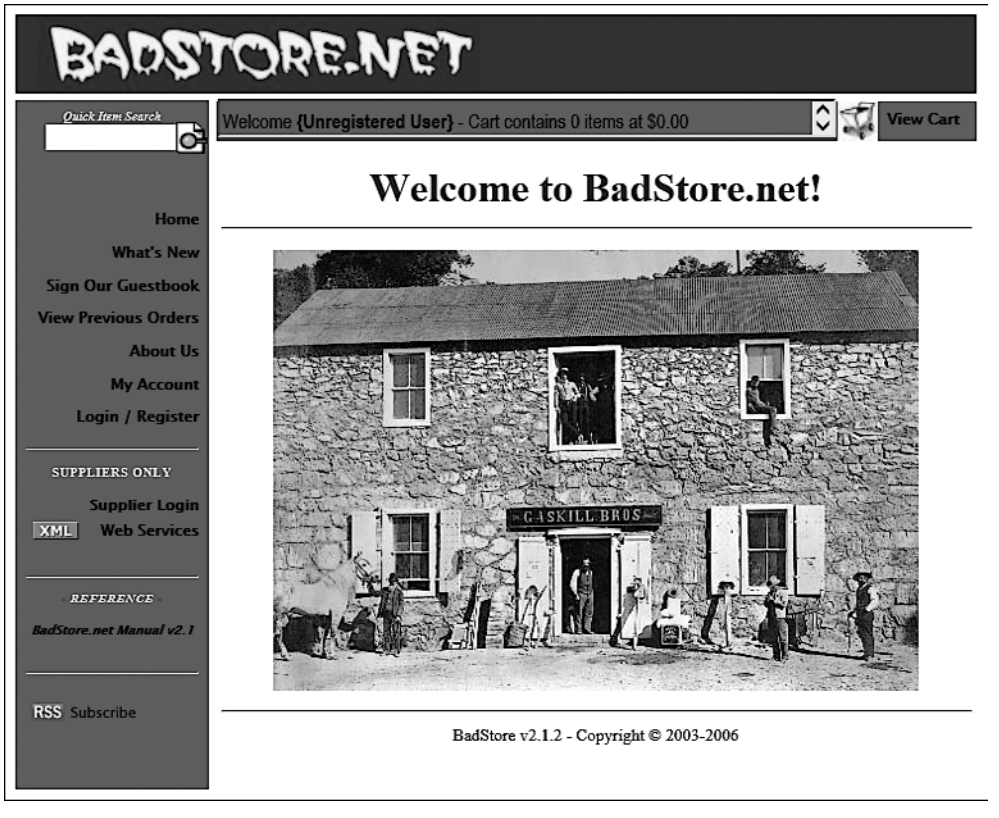

Рис. 2.23. Интерфейс виртуальной машины BadStore

Как уже упоминалось, BadStore устарела. Это видно даже по дизайну интерфейса. Однако для начинающих BadStore очень полезна, так как содержит много распространенных уязвимостей, которые можно легко обнаружить и устранить с помощью инструментов Kali Linux. Подробнее об этом вы прочитаете в следующих главах.

Есть еще одна очень простая в настройке и использовании операционная система, которую можно установить на виртуальную машину, — это очень уязвимая операционная система, сохраненная в ISO-образ Linux (DVL). Его можно загрузить по адресу https://sourceforge.net/projects/virtualhacking/files/os/dvl/DVL_1.5_Infectious_Disease.iso/download.

Установка дополнительных инструментов в Kali Linux

До или во время теста на проникновение может потребоваться включить инструменты, которые при обычной установке в Kali Linux недоступны. Есть большое количество специалистов по тестированию на проникновение, которые постоянно создают новые инструменты. Эти инструменты становятся доступными, и вы их тоже можете использовать. Только потребуется установка этих приложений в операционной системе Kali Linux. Поэтому перед началом тестирования на проникновение следует убедиться, что ваши инструменты обновлены.

При включении дополнительных инструментов тестирования на проникновение сначала рекомендуется заглянуть в репозиторий Kali Linux. Если нужный пакет в репозитории доступен, его можно установить с помощью команд, о которых мы расскажем далее. Если же инструмент в репозитории отсутствует, его можно загрузить или с сайта создателя, или с сайта совместного использования программного обеспечения и агрегирования: https://github.com.

Однако есть ряд инструментов, отсутствующих в репозитории, но которые легко можно добавить в инструментарий Kali Linux. В большинстве случаев такие пакеты добавлять не рекомендуется, так как они могут негативно повлиять на работу операционной системы. Кроме того, многие такие пакеты зависят от другого программного обеспечения и могут вызывать проблемы со стабильностью системы.

В операционной системе Kali Linux предусмотрено несколько инструментов для управления пакетами: dpkg, apt и aptitude. Первые два в Kali Linux установлены по умолчанию.

О командах apt и dpkg вы можете узнать больше, перейдя по следующим ссылкам: https://help.ubuntu.com/community/AptGet/Howto/ и http://www.debian.org/doc/manuals/debian-reference/ch02.en.html.

В этом разделе мы кратко рассмотрим команду `apt`, установив пакет с программным обеспечением.

Для поиска в репозитории названия нужного пакета используйте следующую команду:

```
apt-cache search <имя_пакета>
```

Эта команда отобразит весь пакет программного обеспечения с именем *имя_пакета*.

Если вы хотите получить более подробную информацию о найденном пакете, введите следующую команду:

```
apt-cache show <имя_пакета>
```

Чтобы установить новый пакет или обновить уже существующий, введите команду `apt-get`:

```
apt-get install <имя_пакета>
```

Если пакет в репозитории недоступен, его можно найти и загрузить с сайта разработчика этого программного обеспечения или через www.github.com. Программное обеспечение необходимо загружать только из надежных источников. Если требуется формат пакета Debian (пакет будет иметь расширение файла `.deb`), следует использовать команду `dpkg`. Многие пакеты сжаты с помощью таких программ, как 7-Zip. О том, что пакет сжат, говорит расширение `.zip` или `.tar`.

Сетевые сервисы в Kali Linux

В Kali Linux доступно несколько сетевых сервисов. В этом разделе мы расскажем о трех: HTTP, MySQL и SSH. Остальные находятся в Kali Linux ▸ System Services.

HTTP

При тестировании на проникновение нам, например, для обслуживания вредоносных сценариев веб-приложений потребуется веб-сервер. В Kali Linux по умолчанию уже установлен *веб-сервер Apache*. Нам осталось его только запустить.

Далее перечислены шаги, необходимые для запуска в Kali Linux HTTP-сервера.

1. Для запуска сервиса Apache HTTP откройте терминал с командной строкой и введите следующую команду:

   ```
   service apache2 start
   ```

2. Запустите браузер, введите в адресную строку браузера IP-адрес `127.0.0.1` и нажмите клавишу Enter. Если сервис Apache HTTP запущен, в верхней части открытой страницы вы увидите сообщение It works! (рис. 2.24).

Для остановки Apache HTTP выполните следующие действия.

1. Откройте терминал с командной строкой и введите следующую команду:

   ```
   service apache2 stop
   ```

Помните, что после загрузки операционной системы нужно повторить ввод команды service apache2 start. Но процесс запуска сервисов мы можем автоматизировать. Чтобы после загрузки Kali Linux сервис Apache HTTP запустился автоматически, используйте команду update-rc.d apache2 defaults.

2. Добавьте команду для автоматического запуска сервиса `apache2` после каждой загрузки операционной системы.

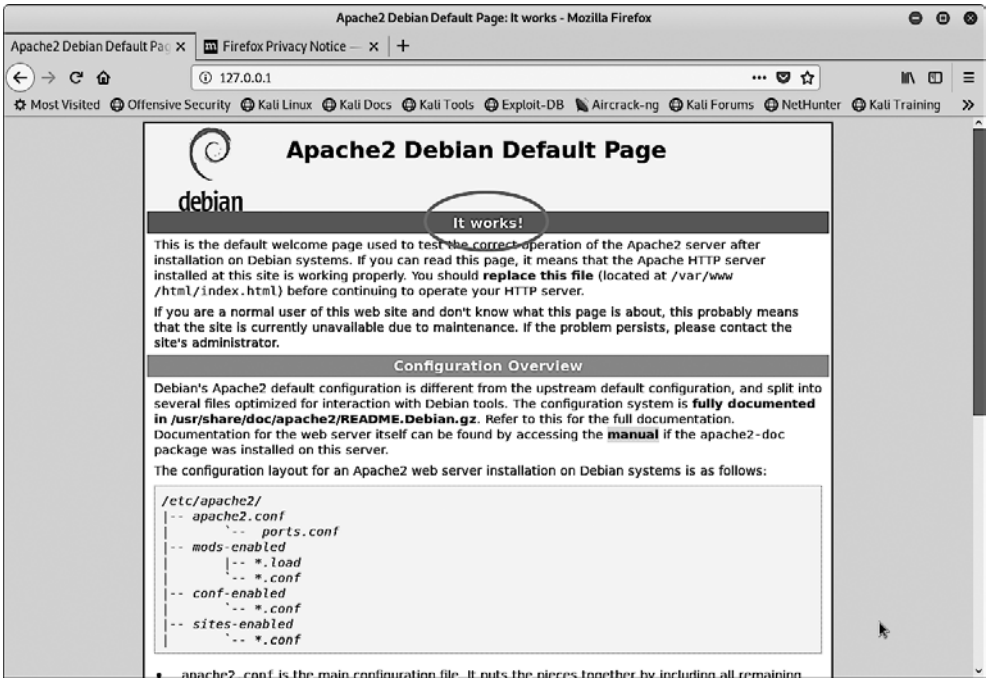

Рис. 2.24. Сервис Apache HTTP запущен

MySQL

Второй сервис, о котором мы поговорим, — *MySQL*. Это реляционная система баз данных. MySQL чаще всего используется совместно с языком программирования PHP и веб-сервером Apache для создания динамических веб-приложений. Этот сервис можно применять и для сбора результатов тестирования, например для хранения информации об уязвимости и результата сопоставления сети.

Чтобы в Kali Linux запустить сервис MySQL, выполните следующие действия.

❑ 1. Введите в окне терминала такую команду:

```
service mysql start
```

2. Чтобы проверить, запущен ли ваш MySQL, используйте клиент MySQL для подключения к серверу. При запуске клиента мы считаем, что для входа на сервер MySQL были указаны имя пользователя и пароль root:

```
mysql -u root
```

В ответ система выдаст следующее сообщение:

```
Enter password:
Welcome to the MySQL monitor. Commands end with ; or g.
```

```
Your MySQL connection id is 39
Server version: 5.5.44-1 (Debian)
Copyright (c) 2000, 2015, Oracle and/or its affiliates.
All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or
itsaffiliates. Other names may be trademarks of their respective owners.
Type ''help;'' or ''h'' for help. Type ''c'' to clear the current input
statement.
mysql>
```

3. После этого приглашения MySQL можно предоставить любые команды SQL. Чтобы выйти из MySQL, введите команду `quit`.

По умолчанию исходя из соображений безопасности в Kali Linux доступ к сервису MySQL можно получить только с локального компьютера. Чтобы эту конфигурацию изменить, отредактируйте в файле конфигурации MySQL раздел bind-address, который находится в каталоге /etc/mysql/my.cnf. Мы не рекомендуем изменять данную конфигурацию, если вы не хотите, чтобы ваш MySQL был доступен для других.

Для остановки сервиса MySQL выполните следующие действия.

1. Введите в окно терминала команду:

```
service mysql stop
```

2. Для автоматического запуска MySQL после загрузки Kali Linux введите такую команду:

```
update-rc.d mysql defaults
```

Эта команда заставит сервис MySQL запуститься после загрузки.

SSH

Следующий сервис, который мы рассмотрим, — *Secure Shell (SSH)*. SSH может использоваться для безопасного входа на удаленную машину. Кроме того, существует несколько других применений SSH, например таких, как безопасная передача файла между машинами, выполнение команд на удаленной машине и пересылка сеанса X11.

Для управления в Kali Linux сервисом SSH выполните следующие действия.

1. Чтобы запустить SSHD, введите в терминале такую команду:

```
service ssh start
```

2. Для тестирования SSH можно войти на сервер Kali Linux с другого сервера с помощью SSH-клиента. Если вы используете операционную систему Windows,

задействуйте, например, SSH-клиент Putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/).

3. Для остановки SSHD введите такую команду:

```
service ssh stop
```

4. Чтобы после загрузки Kali Linux запустить SSH автоматически, введите следующую команду:

```
update-rc.d ssh defaults
```

Эта команда заставит SSH запуститься после загрузки.

Дополнительные лаборатории и ресурсы

Несмотря на то что основное внимание мы уделили Windows 10, Metasploitable 2 и Metasploitable 3, существует еще несколько проектов для изучения уязвимостей и тренировки ваших навыков. Опытные эксперты по безопасности и тестеры на проникновение помнят маленький и очень уязвимый веб-сервер под названием BadStore. Его размер не превышает 15 Мбайт (да, мегабайт), и он содержит несколько уязвимостей от межсайтовых сценариев до внедрения SQL. Хотя для прямой загрузки с официального сайта он больше не доступен, в Интернете его все еще можно найти.

На основную направленность этого сайта указывает имя его домена: https://www.vulnhub.com/ — центр для проектов уязвимостей.

Несколько уязвимых виртуальных машин вы найдете на странице загрузки. Это такие машины, как Linux, Kioptrix и т. д., которые можно использовать для перехвата флагов (CTF) и сценариев.

Существует несколько сайтов, предназначенных для тех, кто заинтересован в оттачивании своих практических навыков или обучении в замкнутой среде.

- *Wargames*. Бесплатные варгеймы, расположенные по адресу http://overthewire.org/wargames/, имеют как базовые уровни, так и уровни повышенной сложности (рис. 2.25).
- *Hack This Site*. Адрес этого сайта: https://Hackthissite.org. Здесь также собрано много уязвимостей (нижняя левая сторона). Сайт предлагает миссии как для начинающих тестеров, так и для программистов. Эти уязвимости бесплатны, но для входа на сайт требуется регистрация (рис. 2.26).
- *Hellbound Hackers*. Как и Hack This Site, сайт Hellbound Hackers (https://www.hellboundhackers.org/) предлагает многочисленные уязвимости, в том числе и для задач тестирования на проникновение. Для доступа к ресурсам, собранным на этом сайте, также требуется регистрация (рис. 2.27).

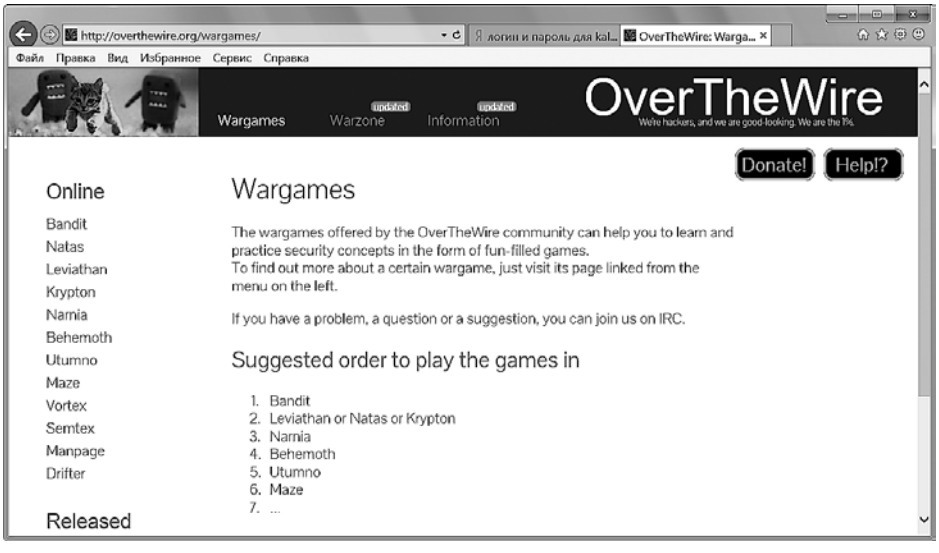

Рис. 2.25. Wargames

Рис. 2.26. Сайт Hackthissite.org

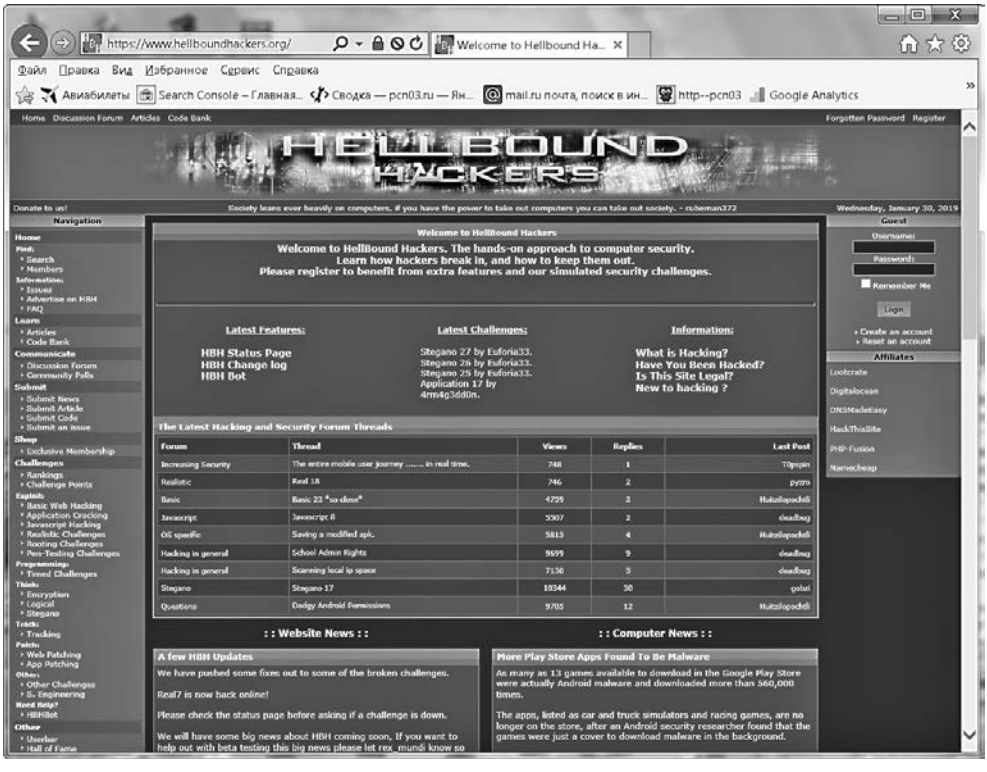

Рис. 2.27. Сайт Hellbound Hackers

Резюме

В этой главе мы рассмотрели создание лабораторной среды для тестирования на проникновение. В главе говорилось, что лабораторная установка будет зависеть исключительно от доступных ресурсов, таких как ЦП, ОЗУ и место на жестком диске. Для получения опыта работы в контролируемой среде, позволяющей легально выполнять тестирование, вы можете поэкспериментировать с такими операционными системами, как Windows, Linux, Mac, Android и даже ARM (доступна на https://www.vulnhub.com/).

При работе с сервером Metasploitable мы настоятельно рекомендуем не только новичкам, но и профессионалам, время у которых ограничено, использовать вместо сложного в установке и настройке Metasploitable 3 сервер Metasploitable 2.

Пользователи с ограниченными ресурсами могут работать с такими уязвимыми серверами, как BadStore и DVL. Эти серверы имеют маленькие размеры и сохранены в формате ISO, поэтому очень легко устанавливаются.

В лаборатории мы рекомендуем установить хотя бы одну операционную систему Windows и одну систему Linux. В следующих главах мы рассмотрим различные методы, позволяющие выполнять тесты на проникновение.

Вопросы

1. Какие платформы виртуализации мы можем использовать для создания виртуальных машин?
2. Для чего предназначен файл с расширением `.vmdk`?
3. Какие логин и пароль используются по умолчанию для входа в Metasploitable 2?
4. Какое дополнительное программное обеспечение потребуется для сборки сервера Metasploitable 3 с нуля?
5. Какая команда используется в Kali Linux для установки нового или обновления существующего пакета?
6. Какая команда применяется для запуска сервиса MySQL?
7. Какая команда используется для запуска сервиса SSH?

Дополнительные материалы

- Установка Metasploitable 2: https://metasploit.help.rapid7.com/docs/metasploitable-2.
- Сборка Metasploitable 3: https://github.com/rapid7/metasploitable3.