1 Установка и настройка Kali Linux

Данная глава откроет перед вами удивительный мир Kali Linux 2018.2. Это специализированный дистрибутив Linux, предназначенный для тестирования на проникновение. В главе будут рассмотрены следующие темы.

- Краткая история Kali.
- Несколько распространенных сфер применения Kali.
- Загрузка и установка Kali.
- Настройка и обновление Kali.

Технические условия

Для этой главы и всей книги вам понадобится ноутбук или настольный компьютер с объемом оперативной памяти не менее 6 Гбайт и 100 Гбайт свободного места на жестком диске — оно потребуется для установки Kali Linux и тестовых лабораторных сред, в качестве которых будут использованы виртуальные машины. При установке Kali Linux на флеш-накопитель или карту SD/micro-SD минимальное пространство для хранения должно составлять 8 Гбайт (рекомендуется 16 Гбайт или более).

Кроме того, нужно будет загрузить следующее программное обеспечение:

- VirtualBox (https://www.virtualbox.org/wiki/Downloads);
- Vmware Player (https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0);
- Kali Linux (https://www.kali.org/downloads/).

Категории инструментов Kali Linux

На момент написания книги последней версией Kali Linux была 2018.2. Она включает:

- улучшенную поддержку графических процессоров AMD;
- исправления в архитектуре x86 и x64 для устранения уязвимостей Spectre и Meltdown;

- облегченный доступ к Metasploit с Metasploit-framework-4.16.34-0Kali2;
- обновленные инструменты Bloodhound v1.51, Reaver 1.6.4, PixieWPS 1.42, BurpSuite 1.7.32, Hashcat 4.0, Wpscan, Openvas, Xplico, Responder и Dradis.

Kali Linux содержит инструменты, назначение которых — тестирование на проникновение. Их можно разделить на следующие категории.

- Information gathering (Инструменты для сбора информации). Эта категория включает несколько инструментов для сбора информации о DNS, IDS/IPS, сетевом сканировании, операционных системах, маршрутизации, SSL, SMB, VPN, а также прослушивания IP, SNMP, адресов электронной почты и VPN.
- Vulnerability assessment (Оценка уязвимостей). В данной категории вы можете найти инструменты для общего сканирования уязвимостей. Здесь также содержатся инструменты для анализа сети Cisco и поиска уязвимостей в серверах баз данных. В этой категории также представлены несколько инструментов fuzzing.
- Web applications (Веб-приложения). Эта категория включает такие инструменты, связанные с веб-приложениями, как сканеры системы управления контентом, базы данных уязвимостей, прокси-службы, сканеры поисковых роботов и сканеры веб-уязвимостей.
- Database assessment (Оценка баз данных). Инструменты этой категории проверяют безопасность различных баз данных. Существует ряд инструментов, разработанных специально для тестирования баз данных SQL.
- Password attacks (Атаки на пароли). В этой категории вы найдете несколько инструментов, которые можно использовать в режиме онлайн или офлайн для выполнения атак паролей.
- Wireless attacks (Беспроводные атаки). В настоящее время все более актуальным становится вопрос безопасности беспроводной связи. Эта категория включает в себя инструменты для атаки Bluetooth, RFID/NFC и беспроводных устройств.
- Exploitation tools (Эксплуатационные инструменты). В этой категории содержатся инструменты, позволяющие эксплуатировать обнаруженные в целевой среде уязвимости. Здесь вы найдете инструменты для эксплуатации сети, Интернета и баз данных. В этой категории также представлены инструменты социальной инженерии, позволяющие искать и использовать информацию.
- Sniffing and spoofing (Анализ и подмена). Инструменты этой категории применяются для отслеживания сетевого трафика. В ней также представлены инструменты сетевого спуфинга (подмены), такие как Ettercap (большой набор инструментов для атаки «человек посередине») и Yersinia (сетевой инструмент, созданный для получения преимущества из некоторых слабостей различных сетевых протоколов).
- Post exploitation (После эксплуатации). Инструменты этой категории помогут вам сохранить полученный ранее доступ к целевому компьютеру. Перед установкой этих инструментов вам, возможно, потребуется получить наивысший уровень

привилегий на компьютере. Здесь вы найдете инструменты для скрытого управления операционной системой компьютера (backdoor, что в переводе значит «черный ход») и веб-приложениями, а также инструменты для туннелирования.

- Forensics (Судебная экспертиза). В этой категории содержатся инструменты для сбора цифровых криминалистических данных, восстановления данных, реагирования на инциденты и вырезания файлов.
- Reporting tools (Инструменты отчетности). Здесь вы найдете инструменты, позволяющие задокументировать процесс и результаты тестирования на проникновение.
- Social engineering tools (Инструменты социальной инженерии). В данной категории содержится очень мощный инструмент Maltego и *набор инструментов социальной инженерии (SET)*. Они могут быть очень полезны на этапах разведки, тестирования на проникновение и эксплуатации.
- System services (Системные сервисы). Данная категория инструментов включает несколько сервисов, которые могут быть полезны во время выполнения задачи тестирования на проникновение, например Apache, MySQL, SSH и Metasploit.

Для упрощения процедуры тестирования на проникновение в Kali Linux предусмотрена категория под названием Top 10 Security Tools (Топ-10 инструментов безопасности). Как следует из названия, это десять наиболее часто используемых инструментов безопасности. В эту категорию входят такие инструменты, как aircrackng, burp-suite, hydra, john, maltego, metasploit, nmap, sqlmap, wireshark и zaproxy.

В Kali Linux вы также найдете несколько инструментов, которые можно использовать для следующих целей.

- Reverse engineering (Инженерный анализ). В этой категории содержатся средства для отладки программ или разборки исполняемого файла.
- Stress testing (Стресс-тест). Эти инструменты предназначены для стресс-теста проводной и беспроводной сети, веб-среды и VOIP (IP-телефония).
- Hardware hacking (Взлом оборудования). Инструменты этой категории используются при работе с приложениями Android и Arduino.
- Forensics (Судебная экспертиза). Представленные здесь инструменты могут быть использованы для различных цифровых криминалистических задач. Они позволяют создавать образы дисков, проводить анализ образов памяти и вырезать файлы. Одним из лучших криминалистических инструментов Kali Linux является Volatility. Он управляется из командной строки и имеет ряд функций для анализа изображений, находящихся в памяти. В Kali Linux есть и несколько графических инструментов, таких как Autopsy и Guymager, а также исправленный xplico.

В этой книге мы рассмотрим только инструменты тестирования на проникновение.

Загрузка Kali Linux

Перед установкой и использованием Kali Linux нужно загрузить ее образ. Вы можете получить его с сайта Kali Linux (http://www.kali.org/downloads/).

На странице Downloads (Загрузки) можно выбрать официальный образ Kali Linux на основе следующих элементов (рис. 1.1).

Image Name	Download	Size	Version	sha256sum
Kali Linux Light 64 Bit	HTTP | Torrent	867M	2018.4	ad63589f761a4344e930486e05e9d3652b8c8badb2e0f808951861ed489db1f6
Kali Linux Light Armhf	HTTP | Torrent	630M	2018.4	4b409b7f0650741400b2c3c9076333f6c52211205c4a2828d677f1099d3e5d64
Kali Linux Light 32 Bit	HTTP | Torrent	863M	2018.4	0659674f841d91b71bd2503e352ded588ec17d0e976c9fee4345dad35ace83b1
Kali Linux 64 Bit	HTTP | Torrent	3.0G	2018.4	7c65d6a319448efe4ee1be5b5a93d48ef30687d4e3f507896b46b9c2226a0ed0
Kali Linux 32 Bit	HTTP | Torrent	3.1G	2018.4	14e53cd797d673db31437c36d51bab0f0a0b6ef9ab277c6c90b9f1fc9d96c291
Kali Linux Mate 64 Bit	HTTP | Torrent	2.9G	2018.4	3e045904582879e4c2ba75a4486f93d7d74de63e0ed54a5108804cefd7287ffb
Kali Linux Kde 64 Bit	HTTP | Torrent	3.0G	2018.4	baf5c29371aca86ed28a87a32282f801e041876fd19152ea621ce84e4e0ff5dc
Kali Linux Xfce 64 Bit	HTTP | Torrent	2.8G	2018.4	f262287286ef5fc630bd0ea219ecc03f767dd2ff9ad1b769bfcc35dfe1fa66e2
Kali Linux E17 64 Bit	HTTP | Torrent	2.8G	2018.4	b7236b7747454fea12b5fb81be85ad7530bc6416e07127558e98f80dfbef2bd9
Kali Linux Lxde 64 Bit	HTTP | Torrent	2.8G	2018.4	612aebd78f570aac62511b049a45ebf0be027a28c9b4732e0b5d799fa818ca6d

Рис 1.1. Архитектура машины: i386, x64 и armhf

Образы для VMware, VirtualBox и Hyper-V также можно загрузить со страницы загрузок Offensive Security, расположенной по адресу https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/, как показано на рис. 1.2.

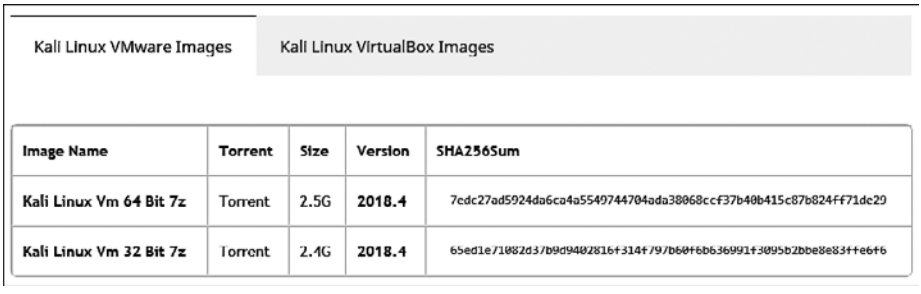

Рис. 1.2. Эти файлы образов доступны как по прямым ссылкам, так и в виде архивированных файлов, загружаемых с помощью торрента

Пользователь может загрузить ARM Kali Linux с сайта по адресу https://www.offensive-security.com/kali-linux-arm-images/. Здесь можно загрузить образы для таких устройств, как Chromebook, Raspberry Pi и т. д., щелкнув на стрелке справа от названий устройств.

Kali NetHunter v3.0 можно загрузить с сайта Offensive Security: https://www.offensive-security.com/kali-linux-nethunter-download/ (рис. 1.3).

Подробнее о выборе, установке и использовании соответствующей версии NetHunter будет рассказано в последующих главах.

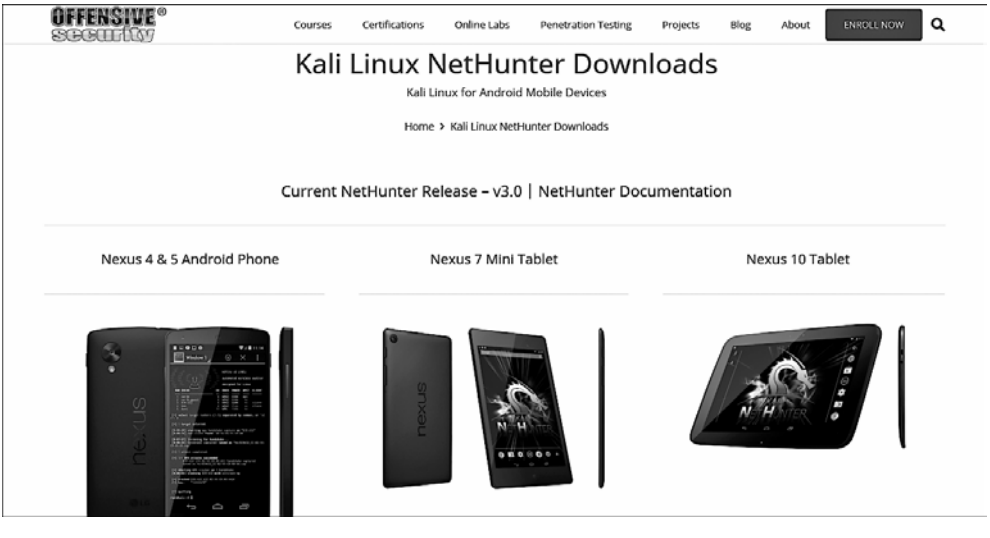

Рис. 1.3. Страница загрузки Kali Nethunter для Linux

Чтобы записать образ на DVD или установить Kali Linux на свой компьютер, загрузите версию образа ISO. Если же вы хотите установить и использовать Kali Linux в виртуальной среде на виртуальной машине, такой, например,

как VirtualBox, VMWare или Hyper-V, возьмите файлы образов для виртуальных машин. С их помощью установка и настройка виртуальной среды пойдет быстрее. Эти образы доступны по адресу https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/.

После успешной загрузки файла необходимо сравнить хеш-значение SHA загруженного образа со значением хеша `sha256sum`, который указан на странице загрузки. Значение SHA-256 проверяется, чтобы избежать установки поврежденного или поддельного образа.

В операционной системе UNIX/Linux/BSD для проверки хеш-значения SHA-256 загруженного файла образа используется команда `sha256sum`. Учтите, что из-за большого размера файла образа Kali Linux эта операция может занять некоторое время. Чтобы сгенерировать хеш-значения для образа, например, `kali-linux-2018.2-amd64.iso`, используйте следующую команду:

```
sha256sum kali-linux-2018.2-amd64.iso
```

Пользователям Windows для проверки хеш-значения можно воспользоваться утилитой под названием MD5 & SHA checksum Utility. Этот инструмент вычисляет MD5, SHA-1, SHA-256, а также хеши файлов SHA-512 и позволяет сравнивать и проверять хеши.

Утилиту MD5 & SHA Checksum можно загрузить по адресу https://download.cnet.com/MD5-SHA-Checksum-Utility/3000-2092_4-10911445.html. После загрузки и запуска нажмите кнопку Browse (Обзор) и укажите путь к загруженному файлу. Мы будем использовать файл `kali-linux-2018.2-amd64.iso`, как показано на рис. 1.4.

Рис. 1.4. Утилита MD5 & SHA Checksum запущена

В поле ввода Hash (Хеш) для проверки был вставлен скопированный со страницы загрузки Kali Linux хеш файла `kali-linux-2018.2-amd64.iso`.

Для сравнения и проверки хеша SHA-256 нажмите кнопку Verify (Проверить) (рис. 1.5).

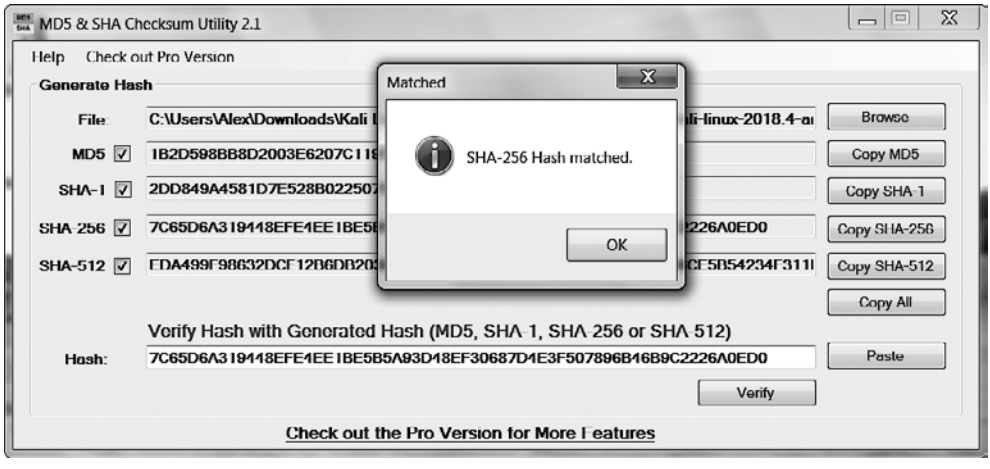

Рис. 1.5. Совпадение хешей SHA-256

Если оба значения совпадают, можно сразу перейти к разделу «Начинаем работать с Kali Linux». Если же значения не совпадают, то файл образа поврежден. В этом случае загрузите повторно файл образа с официального зеркала загрузки и снова проверьте контрольные суммы.

Начинаем работать с Kali Linux

Чтобы начать работать с Kali Linux, операционную систему нужно установить на жесткий диск компьютера или запустить с загрузочного диска. Для этого вы можете воспользоваться Kali Linux одним из следующих способов:

- запустить Kali Linux непосредственно с загрузочного диска Live DVD;
- установить на жесткий диск компьютера;
- установить на USB (портативная Kali Linux).

Далее мы расскажем о каждом способе установки и запуска.

Запуск Kali Linux с Live DVD

Если вы не желаете устанавливать Kali Linux на жесткий диск компьютера, запишите файл образа ISO на DVD. После того как ISO-образ операционной системы будет записан на диск, его можно использовать для запуска вашего компьютера. Для загрузки компьютера с DVD нужно убедиться, что в BIOS выбрана следующая очередность загрузки: сначала компьютер ищет загрузочный сектор на DVD, а только после этого (если DVD не вставлен или на нем отсутствует загрузочный сектор) обращается к загрузочному сектору жесткого диска. Преимущество Kali Linux Live DVD перед остальными способами загрузки в том, что запускать компьютер