ГЛАВА

1

О Kali Linux

Ключевые темы:

- дистрибуция Linux;
- производный дистрибутив Debian;
- предназначение;
- характеристики;
- политики.

Kali Linux (https://www.kali.org/) — это дистрибутив Linux для проверки корпоративной безопасности, основанный на Debian GNU/Linux. Операционная система Kali предназначена для специалистов по безопасности и ИТ-администраторов и позволяет им проводить профессиональное тестирование на проникновение в систему, информационный криминалистический анализ и аудит безопасности информационных систем.

Что такое дистрибутив Linux

Хотя обычно так называют целую операционную систему, Linux — это лишь название ядра, части программного обеспечения, которая обрабатывает взаимодействия между оборудованием и конечными пользовательскими приложениями.

В то же время выражение «дистрибутив Linux» определяет в целом операционную систему, построенную на ядре Linux, обычно содержащую программу установки и множество приложений, которые либо предварительно установлены, либо пакетированы для легкой установки.

Debian GNU/Linux (https://www.debian.org/) — ведущий универсальный дистрибутив Linux, известный своим качеством и стабильностью. Kali Linux основывается на работе проекта Debian, добавляя более 300 собственных специализированных пакетов, связанных с информационной безопасностью, особенно в области тестирования на проникновение.

Debian — это проект, относящийся к свободно распространяемому ПО и предоставляющий несколько версий операционной системы. Для обозначения его конкретной версии часто используют термин «дистрибутив», скажем, дистрибутивы Debian Stable или Debian Testing. То же самое относится и к Kali Linux — например, дистрибутив Kali Rolling.

1.1. Немного истории

Проект Kali Linux плавно стартовал в 2012 году, когда специалисты Offensive Security решили заменить свой почтенный проект Linux BackTrack, который поддерживался вручную, чем-то, что могло бы стать настоящим дериватом Debian (https://wiki.debian.org/Derivatives/Census), дополненным всеми необходимыми объектами и улучшенными методами пакетирования. Было принято решение построить Kali поверх дистрибутива Debian, известного своим качеством, стабильностью и широким выбором доступного программного обеспечения. Вот почему я (Рафаэль) участвовал в этом проекте как консультант Debian.

Первый релиз (версия 1.0) вышел год спустя, в марте 2013 года, и был основан на Debian 7 Wheezy, стабильном (в то время) дистрибутиве Debian. В течение первого года разработки мы компоновали сотни приложений, связанных с тестированием на возможность проникновения, и создавали инфраструктуру. И хотя количество приложений имеет значение, они были тщательно отобраны — мы отбросили те

из них, которые больше не работали, а также те, что дублировали функции, уже доступные в более эффективных инструментах.

На протяжении двух лет после выхода версии 1.0 у Kali появилось множество дополнительных обновлений, которые расширили диапазон доступных приложений и улучшили аппаратную поддержку благодаря новым версиям ядра. Вкладывая силы и средства в непрерывную интеграцию, мы стремились гарантировать, что все важные пакеты готовы к установке и пользователь всегда сможет создать собственные live-образы (отличительная черта дистрибутива).

В 2015 году, когда вышел релиз Debian 8 Jessie, шла работа над переносом на его базу Kali Linux. Хотя система Kali Linux 1.x обходилась без GNOME (используя вместо этого GNOME Fallback), в новой версии мы решили охватить и улучшить эту оболочку. В частности, мы добавили некоторые расширения GNOME для внедрения недостающих функций, в первую очередь меню Applications (Приложения). Результатом нашей деятельности стал дистрибутив Kali Linux 2.0, выпущенный в августе 2015 года.

GNOME — рабочая среда Kali Linux по умолчанию

Рабочая среда (среда рабочего стола, настольная среда) представляет собой набор графических приложений, которые используют общий графический инструментарий и предназначаются для совместного применения на рабочих местах пользователей. На серверах такие среды обычно отсутствуют. Чаще всего они предоставляют программу запуска приложений, менеджер файлов, браузер, почтовый клиент, офисный пакет и т. д.

GNOME (https://www.gnome.org/) — одна из самых популярных сред рабочего стола (вместе с KDE (https://www.kde.org/), Xfce (https://xfce.org/), LXDE (https://lxde.org/), MATE (http://mate-desktop.org/)), устанавливается на основные ISO-образы, предоставляемые Kali Linux. Если вам не нравится GNOME, то можете легко создать пользовательский ISO-образ со средой рабочего стола по вашему выбору. Инструкции описаны в главе 9.

В то же время мы еще тщательнее проработали инструменты, отвечающие за защиту от несанкционированного доступа, с целью гарантировать, что Kali Linux всегда содержит последнюю версию приложений для тестирования на проникновение. К сожалению, данная задача немного расходилась с использованием Debian Stable в качестве основы дистрибутива, поскольку для ее выполнения требовалось резервировать множество пакетов. Это связано с тем, что в Debian Stable приоритетом является стабильность программного обеспечения, результатом чего выступает большой промежуток от момента выпуска обновления до его интеграции в дистрибутив. Учитывая наше стремление к непрерывной интеграции, было вполне естественным шагом перенести Kali Linux на базу Debian Testing, чтобы мы могли воспользоваться последней версией пакетов Debian, как только они становились доступными. У Debian Testing гораздо более интенсивный цикл обновления, который оптимально соответствует философии Kali Linux.

По сути, это концепция релиза Kali Rolling. В то время как дистрибутивы с плавающими релизами были доступны в течение уже довольно длительного времени, Kali 2016.1 стал первым релизом, официально принявшим плавающий характер. Когда вы устанавливаете последнюю версию Kali, ваша система фактически отслеживает дистрибутив Kali Rolling и *каждый день вы получаете новые обновления*. Раньше выпуски Kali представляли собой снимки базового дистрибутива Debian с установленными в него пакетами Kali.

Дистрибутив с плавающим релизом имеет много преимуществ, но сопряжен и со множеством проблем как для тех из нас, кто работает над ним, так и для пользователей, которым приходится справляться с бесконечным потоком обновлений, а иногда и обратно-несовместимыми изменениями. Эта книга предоставит вам информацию, необходимую для решения всех проблем, которые могут возникнуть при управлении установкой Kali Linux.

1.2. Взаимоотношения с Debian

Дистрибутив Kali Linux основан на версии Debian Testing (https://www.debian.org/releases/testing/) (это текущее состояние разработки следующего стабильного дистрибутива Debian). Как следствие, большинство пакетов, доступных в Kali Linux, исходят прямо из репозитория Debian.

Хотя Kali Linux в значительной степени зависит от Debian, он также полностью независим в том смысле, что есть собственная инфраструктура, в которую можно вносить любые изменения по своему желанию.

Движение пакетов

Создатели Debian ежедневно ведут работу над обновлением пакетов и загрузкой их в дистрибутив Debian Unstable. Оттуда пакеты переносятся в дистрибутив Debian Testing сразу после удаления самых вредоносных ошибок. Процесс переноса также гарантирует нерушимость каких-либо зависимостей в Debian Testing. Задача состоит в том, чтобы поддерживать Debian Testing всегда в удобном для пользователя (или даже общедоступном!) состоянии.

Цели Debian Testing и Kali Linux полностью совпадают, так что мы взяли их за основу. Чтобы добавить в дистрибутив пакеты, специфичные для Kali, мы следуем процессу, состоящему из двух этапов.

Для начала мы берем Debian Testing и принудительно внедряем наши собственные пакеты Kali (расположенные в нашем хранилище kali-dev-only) для создания репозитория kali-dev. Время от времени последний будет недоступен: например, наши пакеты, специфичные для Kali, могут не устанавливаться до тех пор, пока не будут перекомпилированы в отношении более новых библиотек. В других ситуациях пакеты, которые мы разветвляли, могут требовать обновлений, чтобы снова стать готовыми к установке или исправить проблему невозможности установки другого пакета, зависящего от более новой версии разветвленного пакета. В любом случае kali-dev не предназначен для конечных пользователей.

kali-rolling — это дистрибутив, обновления которого пользователи Kali Linux должны отслеживать и который основан на репозитории kali-dev таким же образом, как и Debian Testing базируется на Debian Unstable. Пакеты переносятся в данный дистрибутив только после проверки соответствия всех зависимостей в целевом дистрибутиве.

Управление различиями с Debian

В качестве конструктивного решения мы стараемся минимизировать количество разветвленных пакетов, насколько это возможно. Однако реализация некоторых из уникальных особенностей Kali требует внесения определенных изменений. В целях ограничения влияния этих изменений мы стремимся отправить их «выше по течению», интегрируя особенность напрямую или добавляя необходимые методы таким образом, чтобы непосредственно включить нужные функции было легко без дальнейшей модификации самих вышестоящих пакетов.

Kali Package Tracker (http://pkg.kali.org/derivative/kali-dev/) помогает нам отслеживать расхождения с Debian. В любой момент можно увидеть, какой пакет был разветвлен, синхронизирован ли он с Debian или не требуется ли ему обновление. Все наши пакеты хранятся в репозиториях Git, где рядом находятся ветки Debian и Kali. Благодаря этому обновление разветвленного пакета — простой двухэтапный процесс: обновление ветки Debian, а затем объединение ее с веткой Kali.

Хотя разветвленных пакетов в Kali сравнительно немного, количество дополнительных пакетов довольно внушительное: в апреле 2017 года их было почти 400. Большинство из них — это бесплатное ПО, соответствующее Руководству по свободному программному обеспечению Debian (Debian Free Software Guidelines) (https://www.debian.org/social_contract), и наша конечная цель заключается в том, чтобы всегда поддерживать эти пакеты в Debian. Вот почему мы стремимся следовать политике Debian (https://www.debian.org/doc/debian-policy/) и придерживаться хороших методов пакетирования, используемых в Debian. К сожалению, есть также немало исключений, когда правильное пакетирование практически невозможно. В результате нехватки времени несколько пакетов были перемещены в Debian.

1.3. Предназначение и варианты использования

Хотя основная цель Kali обобщенно может быть сформулирована как «тестирование на проникновение и аудит безопасности», за этими словами скрыто большое количество различных задач. Kali Linux создан как *фреймворк*, поскольку включает множество инструментов, предназначенных для самых различных задач (при этом они могут применяться комбинированно во время тестирования на проникновение).

К примеру, Kali Linux можно использовать на разных типах компьютеров: конечно же, на ноутбуках специалистов по тестированию на проникновение (пентестеров — penetration tester), но также и на серверах системных администраторов, желающих контролировать свою сеть, на рабочих системах криминалистических аналитиков. Что еще более неожиданно, дистрибутив можно применять на скрытых

встроенных устройствах, как правило, с процессорами ARM, которые могут работать удаленно в диапазоне беспроводной сети или быть подключенными к компьютеру целевых пользователей. Кроме того, многие ARM-устройства — прекрасные атакующие машины благодаря своим компактным размерам и небольшому количеству потребляемой энергии. Kali Linux также может работать в облаке для создания «армии» машин, занимающихся взломом паролей, и на смартфонах и планшетах, чтобы обеспечить действительно портативное тестирование на проникновение.

Но это еще не все. Пентестеры также нуждаются в серверах: чтобы задействовать программное обеспечение для совместной работы в команде, настраивать веб-сервер для использования в фишинговых кампаниях, запускать инструменты для сканирования уязвимости и для прочих соответствующих действий.

После загрузки Kali вы обнаружите, что главное меню Kali Linux организовано по темам различных задач и действий, подходящих для пентестеров и других специалистов по информационной безопасности (рис. 1.1).

Рис. 1.1. Меню приложений Kali Linux

Эти задачи и действия включают следующие.

- **Сбор информации** — сбор данных о целевой сети и ее структуре, идентификация компьютеров, их операционных систем и служб, которые они запускают. Определение потенциально уязвимых частей информационной системы. Извлечение всех видов листингов из запущенных сервисов каталогов.
- **Анализ уязвимостей** — быстрое тестирование локальной или удаленной системы на предмет подверженности влиянию ряда известных уязвимостей или ненадежных конфигураций. Сканеры уязвимостей используют базы данных, содержащие тысячи сигнатур, для выявления потенциальных уязвимостей.