Содержание

Глава 7. Укрепление SSH 257

Об авторе

Дональд А. Треволт – можно просто Донни – пришел в мир Linux еще в 2006 году да так в нем и остался. Он обладатель сертификата Института профессионалов Linux третьего уровня и сертификата GIAC (Global Information Assurance Certification) по обработке инцидентов. Донни – профессиональный преподаватель Linux, а благодаря волшебству интернета он ведет занятия по всему миру, не покидая своей гостиной. Он также работал исследователем по безопасности в компании, специализирующейся на безопасности интернета вещей (IoT).

Я благодарю всех добрых людей в компании Packt Publishing, сделавших процесс публикации книги таким гладким. Я также благодарю своих кошек, любезно позволивших использовать свои клички в демонстрациях, и Майка, своего отважного технического рецензента, за предложения, позволившие сделать книгу лучше.

О рецензенте

Майкл Эрнстофф – специалист по инфраструктуре и безопасности Unix и Linux с 25-летним стажем. Является независимым консультантом уже больше 20 лет. Майкл работал по заказам многих ведущих компаний, преимущественно в банковской и финансовой сферах.

Располагая обширными знаниями в области хостовой безопасности, укрепления безопасности, а также управления идентификацией и доступом, Майкл разрабатывал и внедрял решения для обеспечения безопасности и выполнения нормативных требований.

На досуге любит музицировать, отец четырех детей.

Предисловие

Предполагаемая аудитория

Книга адресована всем администраторам Linux, независимо от того, специализируются они в области безопасности или нет. Описываемые методы можно использовать как на серверах, так и на рабочих станциях под управлением Linux.

Предполагается, что читатель имеет практический опыт работы с командной строкой и знаком с основами Linux.

Структура книги

В главе 1 «Запуск Linux в виртуальной среде» дается обзор ландшафта ИТ-безопасности. Мы поделимся с читателем своим мнением о том, почему изучение безопасности Linux может положительно сказаться на карьере. А также покажем, как настроить виртуальную среду для практических экспериментов.

В главе 2 «Защита административных учетных записей» рассказано, чем опасна постоянная работа от имени учетной записи root и какие преимущества сулит использование `sudo` вместо этого.

Глава 3 «Защита обычных учетных записей» посвящена безопасности учетных записей обычных пользователей и важности стойких паролей.

В главе 4 «Защита сервера с помощью брандмауэра, часть 1» речь пойдет о работе с разными типами брандмауэров.

В главе 5 «Защита сервера с помощью брандмауэра, часть 2» продолжено обсуждение работы с разными типами брандмауэров.

Глава 6 «Технологии шифрования» посвящена вопросу защиты важной информации – как на диске, так и в процессе передачи – с помощью подходящего шифрования.

В главе 7 «Укрепление SSH» рассматривается, как защитить данные в процессе передачи. Конфигурацию Secure Shell, подразумеваемую по умолчанию, никак не назовешь безопасной, и если ничего не предпринять, она может открыть брешь в системе защиты. В этой главе показано, как это исправить.

В главе 8 «Избирательное управление доступом» познакомимся с тем, как задавать владельцев и права доступа для файлов и каталогов. Мы рассмотрим, чем могут быть полезны биты SUID и SGID, а также последствия их использования для безопасности системы. И завершим главу обсуждением расширенных атрибутов файлов.

В главе 9 «Списки управления доступом и управление разделяемым каталогом» объясняется, что обычные права доступа к файлам и каталогам в Linux недостаточно детализированы. Списки управления доступом позволяют предоставить доступ к файлу только определенному лицу или несколь-

ким лицам, но с разными правами. Мы также применим полученные знания к управлению каталогом, разделяемым членами группы.

Глава 10 «Реализация мандатного управления доступом с помощью SELinux и AppArmor» посвящена технологии мандатного управления доступом SELinux, включенной в дистрибутивы на основе Red Hat Linux. Мы вкратце опишем, как использовать SELinux, чтобы не позволить противнику скомпрометировать систему. А также дадим краткое введение еще в одну технологию мандатного доступа, AppArmor, которая включена в дистрибутивы на основе Ubuntu и SUSE.

В главе 11 «Укрепление ядра и изоляция процессов» рассказывается, как сделать ядро Linux еще более защищенным от атак некоторых типов. Рассматриваются некоторые способы изоляции процессов, предотвращающие эксплойты в Linux.

В главе 12 «Сканирование, аудит и укрепление» речь пойдет о том, что вирусы, представляющие большую проблему в Windows, пока еще не стали таковой в Linux. Если в вашей организации имеются Windows-клиенты, обращающиеся к файловым серверам Linux, то эта глава для вас. Вы можете использовать `auditd` для аудита доступа к файлам, каталогам и системным вызовам в Linux. Это не закроет бреши в системе, но зато вы будете знать, что кто-то пытается получить несанкционированный доступ к конфиденциальной информации. SCAP, протокол автоматизации управления данными безопасности (Security Content Automation Protocol), – это инфраструктура обеспечения соответствия, пропагандируемая Национальным институтом стандартов и технологий США (NIST). Реализацию с открытым исходным кодом, OpenSCAP, можно использовать для применения политики укрепления к компьютеру под управлением Linux.

В главе 13 «Протоколирование и защита журналов» излагаются основы работы с `ryslog` и `journald`, двумя самыми распространенными системами протоколирования в Linux. Мы покажем, как упростить просмотр журналов и как настроить безопасный центральный сервер протоколирования. И для этого нам не потребуется ничего, кроме пакетов, уже входящих в состав большинства дистрибутивов Linux.

В главе 14 «Поиск уязвимостей и обнаружение вторжений» объясняется, как организовать проверку систем на предмет упущений в конфигурациях защиты. Мы также кратко рассмотрим систему обнаружения вторжений.

В главе 15 «Предотвращение запуска нежелательных программ» описано, как с помощью программы `fapolicyd` и параметров монтирования раздела воспрепятствовать исполнению недоверенных программ в системе.

В главе 16 «Полезные советы по безопасности для неутомимых тружеников» констатируется, что всякий, кто занимается безопасностью, трудится как пчелка. И даются полезные советы, как облегчить эту работу.

Как извлечь максимум пользы из этой книги

- Необходимы практические навыки работы с основными командами Linux и ее файловой системой.
- Требуются базовые знания таких средств, как `less` и `grep`.

Скачайте примеры кода

Весь код, на который есть ссылки в этой книге, размещен на GitHub по адресу https://github.com/PacktPublishing/Mastering-Linux-Security-and-Hardening-3E. На сайте https://github.com/PacktPublishing/ имеется также код для других книг и видео из нашего обширного каталога. Поинтересуйтесь!

Скачайте цветные изображения

Мы также предлагаем PDF-файл, содержащий цветные изображения всех снимков экрана и рисунков. Его можно скачать по адресу https://packt.link/wcaG3.

Графические выделения

В этой книге применяется ряд соглашений о наборе текста.

`CodeInText`: код в тексте, имена таблиц базы данных, папок и файлов, расширения имен файлов, пути к файлам, данные и адреса в Твиттере. Например: «откройте Firefox и перейдите по адресу `https://localhost:9392`».

Блок кода выглядит следующим образом:

```
Метод HTTP TRACK активен, а значит, хост уязвим к XST-куку wordpress_test_cookie,
созданному без флага httponly.
```

Входные данные и результаты команд выглядят так:

```
sudo apt update
sudo apt install podman
```

Полужирный: новые термины и важные слова, а также части пользовательского интерфейса. Так выделяются команды меню и текст в диалоговых окнах, например: «Задайте для одного режим **Bridged**, а другой оставьте в режиме **NAT**».

Предупреждение и важные замечания выглядят так.

Полезные советы выглядят так.

—Часть I—

Подготовка безопасной Linux-системы

В этой части мы настроим «лабораторный стенд» с виртуальными машинами под управлением Ubuntu, CentOS и AlmaLinux.

Пользователи Windows узнают, как удаленно обратиться к Linux-машине из Windows.

1

Запуск Linux в виртуальной среде

Вы, наверное, задаетесь вопросом: «Зачем мне изучать защиту Linux? Разве Linux не безопасна изначально? Ведь это же не Windows». Но на самом деле причин много.

Да, действительно, у Linux есть кое-какие преимущества перед Windows в плане безопасности, а именно:

- в отличие от Windows, Linux с самого начала проектировалась как многопользовательская операционная система. Поэтому с безопасностью в ней дело обстоит немного лучше;
- в Linux лучше организовано разделение между администраторами и непривилегированными пользователями. Это создает некоторые препятствия для злоумышленников, а обычному пользователю случайно заразить Linux чем-то неподобающим чуть сложнее;
- Linux значительно более стойка к вирусам и вредоносным программам, чем Windows. В некоторые дистрибутивы Linux уже встроены механизмы, такие как SELinux в Red Hat и его бесплатных клонах и AppArmor в Ubuntu и SUSE, которые не позволяют вторгшемуся злоумышленнику получить контроль над системой;
- Linux – свободное программное обеспечение с открытым исходным кодом. Это позволяет любому человеку, обладающему достаточными знаниями, провести аудит кода Linux на предмет наличия ошибок или закладок.

Но даже со всеми этими преимуществами Linux не отличается от любого другого творения человека. То есть она несовершенна.

И вот какие вопросы мы рассмотрим в этой главе:

- обзор угроз;
- почему любой администратор Linux должен изучать защиту системы;
- немного о конкретных угрозах с примерами того, как злоумышленникам иногда удавалось взломать систему Linux;

- ресурсы, на которых публикуются актуальные новости о безопасности ИТ;
- различия между физической, виртуальной и облачной системами;
- подготовка Ubuntu Server и виртуальных машин типа Red Hat с помощью VirtualBox, а также установка репозитория **Extra Packages for Enterprise Linux** (**EPEL**) для виртуальных машин типа Red Hat;
- создание моментальных снимков виртуальной машины;
- установка Cygwin на хост-компьютер под управлением Windows, чтобы пользователи Windows могли подключаться к виртуальной машине;
- использование оболочки Bash в Windows 10/11 для доступа к системам Linux;
- поддержание систем Linux в актуальном состоянии.

Обзор угроз

Если вы следили за ИТ-технологиями на протяжении последних нескольких лет, то, вероятно, встречали хотя бы несколько статей о том, как злоумышленникам удавалось скомпрометировать Linux-серверы. Например, хотя Linux и в самом деле невосприимчива к заражениям вирусами, имело место несколько случаев, когда злоумышленникам удалось внедрить на сервер другие типы вредоносного ПО. Приведем несколько примеров:

- ботнет: сервер заставляют присоединиться к ботнету, контролируемому удаленным злоумышленником. В одном из самых известных случаев такого рода Linux-серверы, присоединившиеся к ботнету, запускали атаку типа «отказ в обслуживании» (DoS-атаку) против других сетей;
- программы-вымогатели: шифруют все пользовательские данные и требуют выкуп за расшифровку. Но даже после уплаты выкупа нет никакой гарантии, что данные можно будет восстановить;
- программы майнинга криптовалют: заставляют процессор сервера-жертвы работать на полную мощность и потреблять больше энергии. Добытая криптовалюта переводится на счета злоумышленников, внедривших программу.

И разумеется, существует немало брешей, не связанных с установкой вредоносного ПО, например когда злоумышленник находит способ украсть учетные данные пользователя, данные кредитных карт и другую конфиденциальную информацию.

Причина некоторых брешей – тривиальная беспечность. В статье по адресу https://arstechnica.com/information-technology/2017/09/in-spectacular-fail-adobe-security-team-posts-private-pgp-key-on-blog/ описывается, как беспечный администратор Adobe разместил закрытый ключ компании в публичном блоге по безопасности.

А теперь поговорим подробнее о брешах в системе защиты.