

LINUX BASICS FOR HACKERS

**Getting Started with Networking, Scripting, and Security in Kali by OccupyTheWeb**

**黑客LINUX基础**

**从学习Kali Linux中的网络、脚本和安全性开始**

San Francisco

**LINUX BASICS FOR HACKERS.** Copyright © 2019 by OccupyTheWeb.

版权所有。未经版权所有者和出版商事先书面许可，不得以任何形式或通过电子或机械方式（包括影印，录制或任何信息存储或检索系统）复制或传播本作品的任何部分。

ISBN­10: 1­59327­855­1

ISBN­13: 978­1­59327­855­7

出版商：William Pollock

制作编辑：Serena Yang and Meg Sneeringer

封面插图： Josh Ellingson

内图设计：Octopod Studios

发展编辑：Liz Chadwick

技术评论员：Cliff Janzen

编辑：Barton D. Reed

合成：Serena Yang and Meg Sneeringer

校对员：Paula L. Fleming

索引者：JoAnne Burek

翻译：byr0nchan(汉武安全实验室)

校对：

验证：

有关分发、翻译或批量销售的信息，请直接联系 No Starch出版社：

No Starch Press, Inc.

245 8th Street, San Francisco, CA 94103

phone: 1.415.863.9900; info@nostarch.com

www.nostarch.com

*Library of Congress Cataloging­in­Publication Data*

名称：OccupyTheWeb,作者

标题：Linux basics for hackers : getting started with networking,scripting,and security in Kali/OccupyTheWeb

说明：第一版|San Francisco : No Starch Press, Inc.,[2018].Identifiers: LCCN 2018030544 (print)|LCCN 2018032646 (ebook)|ISBN 9781593278564 (epub)|ISBN 159327856X (epub)|ISBN 9781593278557(print)|ISBN 1593278551(print)|ISBN 9781593278564(ebook)|ISBN 159327856X(ebook)

主题：LCSH: Penetration testing (Computer security)|Kali Linux.|Hackers.|Operating systems (Computers)

分类：LCC QA76.9.A25 (ebook)|LCC QA76.9.A25 O325 2018 (print)|DDC 005.8­­dc23

LC record available at <https://lccn.loc.gov/2018030544>

No Starch Press 和 No Starch Press 徽标是 No Starch Press Inc.的注册商标。此处提及的其他产品和公司名称可能是其各自所有者的商标。我们不是在每次出现商标名称时使用商标符号，而是仅以编辑方式使用这些名称，并且为商标所有者的利益而使用，而无意侵犯商标。

本书中的信息按“As Is”分发，不附带任何保证。虽然在准备这项工作时已经采取了一切预防措施，但作者和 No Starch Press 均不对任何人或实体对由于包含在其中的信息，直接或间接造成的任何损失或损害承担任何责任。

**绪 论**



骇客攻击是21世纪最重要的技能！我不轻易做出这种说法。近年来似乎每天早上新闻事件的标题重申了这一说法。各国正在互相监视以获取机密，网络犯罪分子正在窃取数十亿美元，要求赎金的数字蠕虫被释放，竞选对手正在影响彼此的选举，战斗人员相互拆台。这些都是骇客的工作，他们对我们日益数字化的世界的影响才刚刚凸显。

我决定在与成千上万有抱负的骇客通过NullByte（http：//www.hackersarise.com）以及美国军事和情报机构（NSA，DIA，CIA和FBI）的几乎所有分支机构合作写这本书。这些经历告诉我，许多有抱负的骇客对Linux几乎没有任何经验，而这种缺乏经验是他们开始成为职业骇客的主要障碍。几乎所有最好的骇客工具都是用Linux编写的，因此一些基本的Linux技能是成为专业骇客的先决条件。我写这本书是为了帮助有抱负的骇客克服这个障碍。

黑客是IT领域的精英职业。因此，它需要对IT概念和技术进行广泛而详细的理解。在最基础的层次上，Linux是一项需求。如果你想把黑客和信息安全作为你的职业，我强烈建议你投入时间和精力来使用和理解它。

本书不适合经验丰富的黑客或经验丰富的Linux管理员。

 相反，它适用于那些想要在黑客、网络安全和渗透测试这条激动人心的道路上起步的人而设计的。它也不是一篇关于Linux或黑客的完整论文，而是这些世界的起点。它从Linux的基本知识开始，并扩展到bash和Python的一些基本脚本。

在适当的情况下，我尝试使用来自黑客世界的示例来教授Linux原理。

在本简介中，我们将介绍信息安全的道德黑客行为的发展，我将带您完成安装虚拟机的过程，以便您可以在系统上安装Kali Linux，而不会干扰您已经运行的操作系统。

**这本书里有什么**

在第一章中，您将熟悉Linux的基础知识;

第1章将让您学习使用文件系统和终端，并为您提供一些基本命令。

第2章介绍如何操作文本以查找，检查和更改软件和文件。

在第3章中，您将管理网络。您将扫描网络，查找连接信息，并通过屏蔽网络和DNS信息来伪装自己。

第4章教您添加、删除和更新软件，以及如何简化系统。

在第5章中，您将操纵文件和目录权限来控制谁可以访问什么，您还将学习一些权限提升技术。

第6章教您如何管理服务，包括启动和停止进程以及分配资源以便更好地控制。

在第7章中，您将管理环境变量以获得最佳性能，便利性甚至隐身性。您将找到并过滤变量，更改PATH变量以及创建新的环境变量。

第8章向您介绍了bash脚本，这是任何认真的黑客的主要工具。您将学习bash的基础知识并构建一个脚本来扫描您可能稍后渗透的目标端口。

第9章和第10章为您提供了一些基本的文件系统管理技能，向您展示如何压缩和存档文件以保持系统整洁，复制整个存储设备以及获取有关文件和连接磁盘的信息。

后面的章节深入探讨了黑客主题。在第11章中，您将使用和操作日志系统来获取目标活动的信息，并覆盖您自己的轨迹。

第12章向您展示了如何使用和滥用三个核心Linux服务：Apache Web服务器，OpenSSH和MySQL。您将创建一个Web服务器，构建一个远程视频间谍，并了解数据库及其漏洞。

第13章将向您展示如何在代理服务器，Tor网络，VPN和加密电子邮件中保持安全和匿名。

第14章涉及无线网络。您将学习基本的网络命令，然后破解WiFi接入点并检测连接蓝牙信号。

第15章深入探讨了Linux本身，深层次了解内核如何工作以及如何滥用其驱动程序来传递恶意软件。

在第16章中，您将学习基本的调度技巧，以便自动化您的黑客脚本。

第17章将教你核心的Python概念，你将编写两个黑客工具：一个监视TCP / IP连接的扫描程序和一个简单的密码破解程序。

**什么是道德黑客？**

近年来，随着信息安全领域的发展，道德黑客领域也出现了迅猛的发展，也被称为白帽黑客(good guy)。道德黑客是试图渗透和利用一个系统，以找出其弱点和更好地保护它的实践做法。我将道德黑客分为两个主要部分:为合法信息安全公司进行渗透测试，以及为贵国的军事或情报机构工作。两者都是快速增长的领域，需求强劲。

***渗透测试***

随着组织越来越注重安全性并且安全漏洞的成本呈指数级增长，许多大型组织开始将安全服务外包出去。其中一项关键安全服务是渗透测试。渗透测试本质上是一个合法的、受委托的黑客行为，以证明公司的网络和系统的脆弱性。

 通常，组织首先进行漏洞评估，以发现其网络、操作系统和服务中的潜在漏洞。我强调是潜在的，因为此漏洞扫描包含大量误报（确定为漏洞的事实并非如此）。渗透测试人员的角色是试图破解或渗透这些漏洞。只有这样，组织才能知道漏洞是否真实，并决定投入时间和金钱来弥补漏洞。

***军事和间谍活动***

现在，世界上几乎每个国家都在进行网络间谍活动和网络战争。人们只需要浏览一下头条新闻，就会发现网络活动是监视和攻击军事和工业系统的选择方法。

黑客在这些军事和情报收集活动中起着至关重要的作用，随着时间的推移，这种情况才会更加真实。想象一下未来的战争，黑客可以获得对手的作战计划，并摧毁他们的电网、炼油厂和供水系统。这些活动现在每天都在进行。因此，黑客成为国家防御的关键组成部分。

**为什么黑客使用LINUX**

那么为什么黑客使用Linux而不是其他操作系统呢？主要是因为Linux通过几种不同的方法提供了更高级别的控制。

***Linux是开源的***

与Windows不同，Linux是开源的，这意味着您可以使用操作系统的源代码。因此，您可以随意更改和操作它。如果您试图使系统以它不希望的方式运行，那么能够操作源代码是必不可少的。

***Linux是透明的***

要有效地进行黑客攻击，您必须了解并理解您的操作系统，并在很大程度上了解您正在攻击的操作系统。Linux完全透明，这意味着我们可以查看和操作其所有工作部分。

Windows则不然。微软努力让它变得越来越难以了解其操作系统的内部工作方式，所以你永远不会真正知道“幕后”会发生什么，而在Linux中，你会直接看到操作系统的每一个组件。这使得使用Linux更加有效。

***Linux提供粒度控制***

Linux是细粒度的。这意味着您对系统几乎拥有无限的控制权。在Windows中，您只能控制Microsoft允许您控制的内容。在Linux中，一切都可以由终端控制，无论在最微小的级别或最宏观的级别。此外，Linux使任何脚本语言的脚本编写变得简单有效。

***多数黑客工具都是为Linux编写的***

超过90％的黑客工具都是为Linux编写的。当然，也有例外，如Cain and Abel以及Wikto，这些例外证明这一规则。即使在为Windows移植诸如Metasploit或nmap等黑客工具时，并非所有功能都能从Linux移植。

***未来属于Linux/Unix***

这似乎是一个激进的陈述，但我坚信信息技术的未来属于Linux和Unix系统。微软在20世纪80年代和90年代曾风光一时，但它的增长正在放缓并停滞。

自互联网诞生以来，由于其稳定性、可靠性和稳健性，Linux / Unix一直是Web服务器的首选操作系统。 即便在今天，Linux / Unix仍在三分之二的Web服务器中使用并占据市场主导地位。路由器，交换机和其他设备中的嵌入式系统几乎总是使用Linux内核，而虚拟化世界则由Linux主导，VMware和Citrix都基于Linux内核构建。

超过80％的移动设备运行Unix或Linux（iOS是Unix，Android是Linux），所以如果您认为计算机的未来在于平板电脑和手机等移动设备（否则很难争辩），那么未来就是Unix / Linux。Microsoft Windows仅占移动设备市场的7％**①**。 那是你想要的马车吗？

1. 2019年1月10日微软通过自己的官方博客宣布放弃Win10 Mobile，于2019年12月终止支持。

**下载KALI LINUX**

在开始之前，您需要下载并在计算机上安装Kali Linux。这是我们将在本书中使用的Linux发行版。Linux最初由Linus Torvalds于1991年开发，作为Unix的开源替代品。由于它是开源的，志愿者开发人员对内核、实用程序和应用程序进行提交编码。这意味着没有凌驾于其之上的公司实体来监督发展，因此，通常缺乏公约和标准化。

Kali Linux由Offensive Security开发，是一个基于Linux发行版的黑客操作系统。Linux有很多发行版，而Debian是最好的发行版之一。您可能最熟悉Ubuntu作为Linux的流行桌面发行版。Ubuntu也是基于Debian构建的。其他发行版包括Red Hat，CentOS，Mint，Arch和SUSE。虽然它们都共享相同的Linux内核（控制CPU，RAM等操作系统的核心），但每个内核都有自己的实用程序、应用程序和用于不同目的的图形界面选择（GNOME，KDE和其他）。因此，Linux的这些发行版中的每一个外观和感觉都略有不同。Kali专为渗透测试人员和黑客而设计，并配有大量黑客工具。

我强烈建议您在本书中使用Kali。虽然您可以使用其他发行版，但您可能需要下载并安装我们将使用的各种工具，这可能意味着可能需要花费数小时去下载和安装工具。此外，如果该发行版不是基于Debian构建的，则可能存在其他细微差别。您可以从https://www.kali.org/下载并安装Kali。

 在主页上，单击页面顶部的“Downloads”链接。在“Kali Linux Downloads”页面上，您将面临多种下载选择。选择正确的下载非常重要。在表的左侧，您将看到镜像名称，该名称是链接下载的版本的名称。例如，我看到的一个镜像名称列表是Kali Linux 64 Bit，这意味着它是完整的Kali Linux并且适用于64位系统 - 大多数现代系统使用64位Intel或AMD CPU。要确定系统上的CPU类型，请转至控制面板▸系统和安全性▸系统，应列出该系统信息。如果您的系统是64位，请下载并安装64位版本的完整Kali（不是Light或Lxde，或任何其他替代方案）。

如果您运行的是具有32位CPU的旧计算机，则需要安装32位版本，该版本显示在页面下方。

您可以选择通过HTTP或Torrent下载。如果您选择HTTP，Kali将直接下载到您的系统，就像任何下载一样，它将被放置在您的下载文件夹中。Torrent（bt）下载是许多文件共享站点使用的P2P下载。你需要像BitTorrent这样的种子应用程序才能做到这一点。然后，Kali文件将下载到torrenting应用程序存储其下载的文件夹中。

还有其他类型的CPU的其他版本，例如在许多移动设备中常见的ARM体系架构。如果您使用的是树莓派、平板电脑或其他移动设备（手机用户可能更喜欢Kali NetHunter），请确保下载并安装ARM架构版本的Kali，方法是向下滚动并单击以下载和安装Kali ARM映像。

您已经下载了Kali，但在安装任何软件之前，我想谈谈虚拟机。通常，对于初学者来说，将Kali安装到虚拟机中是学习和练习的最佳解决方案。

**虚拟机**

虚拟机（VM）技术允许您从笔记本电脑或台式机等硬件上运行多个操作系统。这意味着您可以继续运行您熟悉的Windows或MacOS操作系统，并在该操作系统中运行Kali Linux虚拟机。您不需要覆盖现有的操作系统来学习Linux。

VMware，Oracle，Microsoft和其他供应商提供了大量虚拟机应用程序。这些都很好用，但在这里我将向您展示如何下载和安装Oracle的免费VirtualBox。

***安装VirtualBox***

你可以从<https://www.virtualbox.org/>下载VirtualBox，如图1所示，单击左侧菜单中的下载链接，并为计算机当前操作系统选择VirtualBox安装包，该操作系统将承载VirtualBox VM。请务必下载最新版本。



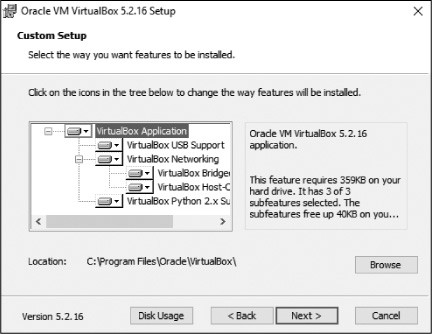
*图1:VirtualBox主页*

下载完成后，单击setup文件，您将看到一个熟悉的安装向导，如图2所示。



*图2:安装向导对话框*

单击**Next**，您应该会看到自定义安装设置屏幕，如图3中所示。



*图3:自定义设置对话框*

在此屏幕上，只需单击**Next**。继续单击**Next**，直到到达网络接口警告屏幕，然后单击**Yes**。

单击**Install**开始该过程。在此过程中，可能会多次提示您安装设备软件。这些是虚拟机通信所需的虚拟网络设备。单击**Install**。

安装完成后，单击**Finish**。

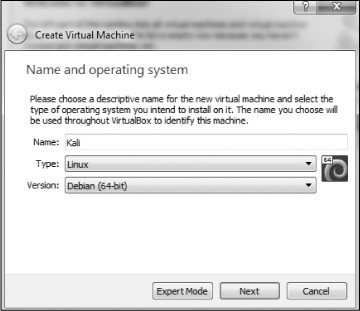
***设置虚拟机***

现在让我们开始使用您的虚拟机。VirtualBox应该在安装后打开 - 如果没有，则手动打开它 - 你应该看到VirtualBox Manager的欢迎，如图4所示。



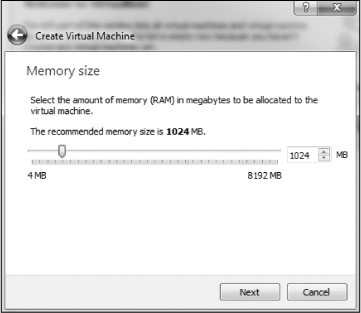
*图4: VirtualBox Manager*

由于我们将使用Kali Linux镜像创建新的虚拟机，因此请单击左上角的“新建”。 这将打开图5中所示的Create Virtual Machine对话框。



*图5: Create Virtual Machine对话框*

给你的机器命名（任何名称都可以，但我只是使用Kali）然后从“**Type**”下拉菜单中选择Linux。 最后，从第三个下拉菜单中选择Debian（64bit）（除非您使用的是32位版本的Kali，在这种情况下选择Debian 32bit版本）。单击“**Next**”，您将看到如图6所示的屏幕。



*图6: 分配内存*

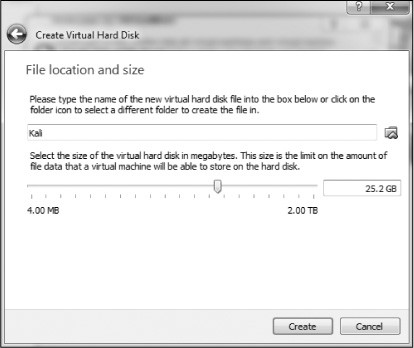
在这里，您需要选择要为此新虚拟机分配多少RAM。

根据经验，我不建议使用超过总系统内存RAM的25％。这意味着如果您在物理系统或主机系统上安装了4GB，则为虚拟机选择仅1GB，如果物理系统上只有16GB，则选择4GB。您为虚拟机提供的RAM越多，运行的速度越快。虽速度越快，但您还必须为主机操作系统和您可能希望同时运行的任何其他虚拟机留下足够的RAM。当您不使用此虚拟机时，它们将不使用任何RAM，但它们将使用硬盘空间。

单击**Next**，您将看到硬盘屏幕。选择“**Create Virtual Hard Disk**”，单击“**Create**”。

在下一个屏幕中，您可以决定是要将要创建的硬盘动态分配还是以固定大小分配。如果选择**动态分配**，系统将不会占用您为虚拟硬盘分配的最大大小，直到需要时，它为主机系统节省更多未使用的硬盘空间。我建议你选择动态分配。

单击**Next**，您将选择要分配给VM的硬盘空间量以及VM的位置（请参见图7）。



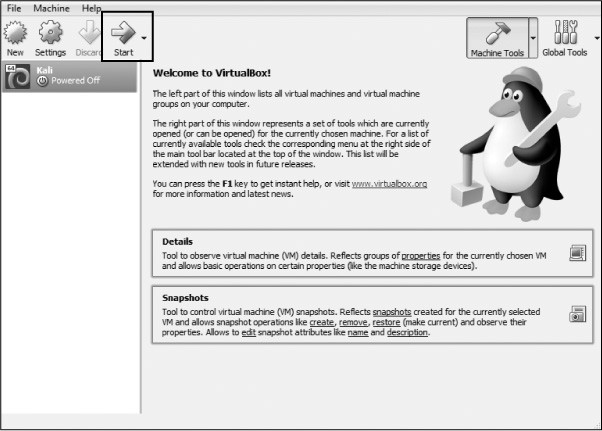
*图7: 分配硬盘空间*

默认值为8GB。我通常发现它有点小，建议你至少分配20-25GB。请记住，如果您选择动态分配硬盘空间，那么直到您需要它时，它才会使用该空间，并且在已经分配好硬盘空间之后再扩展它可能比较棘手，所以最好还是选择偏高的空间。

单击**Create**，就可以开始了!

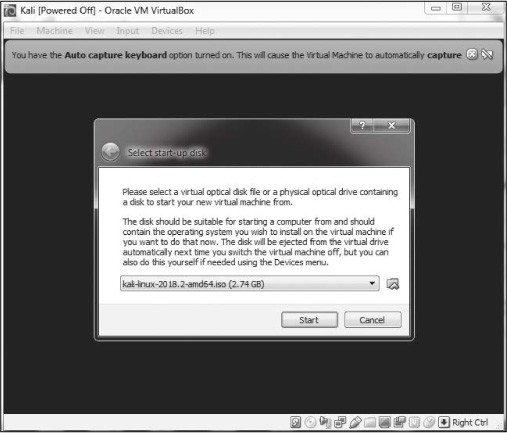
***在VM上安装Kali***

此时，您应该看到如图8所示的屏幕。现在您需要安装Kali。请注意，在VirtualBox Manager的左侧，您应该看到Kali VM已关闭的指示。单击**Start**按钮（绿色箭头图标）。



*图8:VirtualBox欢迎屏幕*

然后，VirtualBox Manager将询问在哪里可以找到启动盘。您已经下载了扩展名为.iso的磁盘映像，该映像应位于您的Downloads文件夹中（如果您使用torrent下载Kali，则.iso文件将位于您的Torrenting应用程序的Downloads文件夹中）。单击右侧的文件夹图标，导航到Downloads文件夹，然后选择Kali映像文件（参见图9）。



*图9:选择启动盘*

然后单击**Start**。恭喜，您刚刚在虚拟机上安装了Kali Linux！

***设置KALI***

Kali现在将打开如图10所示的屏幕，为您提供多种启动选择。我建议为初学者使用图形安装**(graphical install)**。使用键盘键导航菜单。

如果在将Kali安装到VirtualBox时出现错误，可能是因为您没有在硬件系统的BIOS中启用虚拟化。每个系统及其BIOS略有不同，因此请与您的制造商联系或在线搜索您的硬件系统和BIOS的解决方案。 此外，在Windows系统上，您可能需要禁用任何具有竞争的虚拟化软件，如HyperV。同样，您的系统的互联网搜索引擎应该能够指导您这样做。



*图10:选择install方法*

接下来会要求您选择语言。确保选择最适合的语言，然后单击**Continue**。接下来，选择您的位置，单击**Continue**，然后选择键盘布局。

单击**Continue**时，VirtualBox将执行检测硬件和网络适配器的过程。只要耐心等待。最终，您将看到一个要求您配置网络的屏幕，如图11所示。



*图11:输入主机名*

它要求输入的第一项是您的主机名称。你可以随心所欲地命名，但我用默认的“kali”作为名字。

接下来，系统会要求您输入域名。没有必要在这里输入任何东西。单击**Continue**。下一个屏幕非常重要，如图12所示。在这里，系统会要求您输入要用于root用户的密码。



*图12:设置root密码*

Linux中的root用户是强大的系统管理员。您可以使用任何您认为安全的密码。如果这是我们在互联网上使用的物理系统，我建议您使用非常长且复杂的密码来限制攻击者破解它的能力。由于这是人们在没有首先访问主机操作系统的情况下无法访问的虚拟机，因此在此虚拟机上进行密码验证并不重要，但您仍应明智地选择。

单击**Continue**继续，系统将要求您设置时区。这样做，然后继续。

下一个屏幕询问关于分区磁盘（分区就是硬盘的一部分）。选择**Guided – use entire disk**，Kali将检测您的硬盘并自动设置分区。

然后，Kali会警告您，您选择的磁盘上的所有数据都将被删除，但别担心！这是一个虚拟磁盘，磁盘是新的并且是空的，所以这实际上不会做任何事情。单击**Continue**继续。

Kali现在会询问您是希望将所有文件放在一个分区中，还是想要单独的分区。如果这是一个生产系统，您可能会为/ home，/ var和/ tmp选择单独的分区，但考虑到我们将其用作虚拟环境中的学习系统，您可以安全地选择将全部文件放在一个分区中。

现在，将询问您是否将更改写入磁盘。选择**Finish partitioning**并将更改写入磁盘。Kali将再次提示您是否要将更改写入磁盘，选择**Yes**并单击**Continue**继续（参见图13）。



*图13:将更改写入磁盘*

Kali现在将开始安装操作系统。这可能需要一段时间，所以请耐心等待。现在是时候休息一下，喝上自己喜欢的饮料吧。

安装完成后，系统将提示您是否要使用网络镜像。这真的没有必要，所以点击**No**。

然后Kali将提示您是否要安装**GRUB（Grand Unified Bootloader）**，如图14所示。引导加载程序使您可以选择不同的操作系统启动，这意味着当你启动你的机器，你可以启动 Kali或其他操作系统。选择**Yes**并单击**Continue**继续。



*图14:安装GRUB*

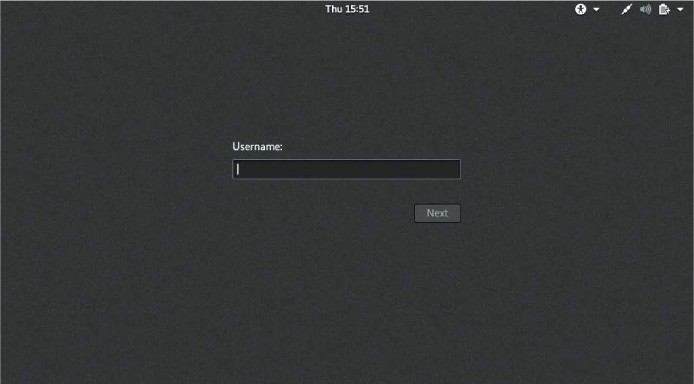
在下一个屏幕上，系统将提示您是自动还是手动安装GRUB引导加载程序。由于原因尚不清楚，如果您选择第二个选项，Kali将倾向于挂起并在安装后显示空白屏幕。选择手动输入设备**Enter device manually**，如图15所示。



*图15:手动输入设备*

在下面的屏幕上，选择GRUB引导加载程序应安装的驱动器（它可能类似于/dev/sda）。单击进入下一个屏幕，该屏幕应告知您安装已完成。

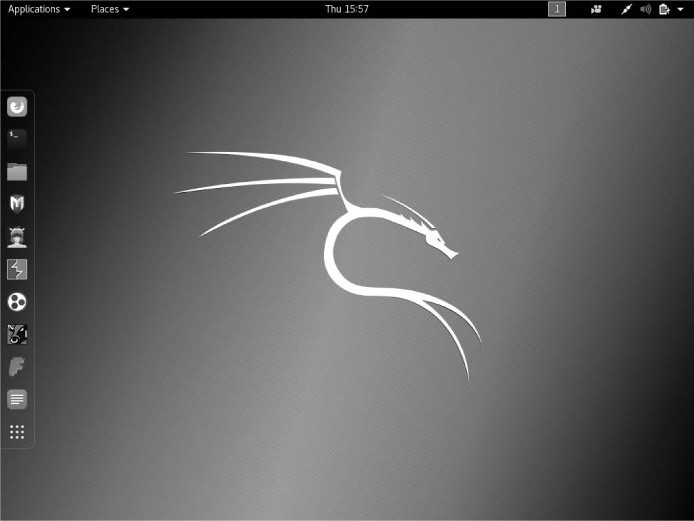
恭喜！你已经安装了Kali。单击**Continue**继续。Kali将尝试重新启动，在您最终遇到Kali 2019的登录屏幕之前，您将看到许多代码行穿过一个空白的黑色屏幕，然后如图16所示。



*图16:Kali登录屏幕*

以root身份登录，系统将询问您的密码。输入您为root用户选择的密码。

以root身份登录后，您将看到Kali Linux桌面，如图17中所示。



*图17:Kali主屏幕*

您现在已准备好开始进入令人兴奋的黑客攻击领域！欢迎！

## 1

## GETTING STARTED WITH THE BASICS

**开始学习基础知识**



从本质上而言，黑客就是行动者。我们想要触摸和玩弄一些东西，我们也希望创造并且有时可能会破坏一些事物。在我们能够做我们最喜欢的事情之前，我们中很少有人想要阅读信息技术理论的长篇大论：黑客攻击。考虑到这一点，本章旨在为您提供一些基本技能，帮助您在Kali中启动和运行。 现在！

在本章中，我们不会详细介绍任何一个概念 - 我们将覆盖足够的内容，让您在黑客的操作系统中进行游戏和探索：Linux。我们将为后面的章节保存更深入的讨论。

### 介绍术语和概念

在开始我们的黑客Linux基础知识奇妙世界之旅之前，我想介绍几个术语，这些术语应该澄清本章后面讨论的一些概念。

**二进制文件**此术语是指可以执行的文件，类似于Windows中的可执行文件。 二进制文件通常位于/ usr/bin或usr/sbin目录中，包括ps，cat，ls和cd等实用程序（我们将在本章中介绍所有四个）以及无线应用程序黑客工具aircrackng和入侵检测系统（IDS）Snort。

**区分大小写**与Windows不同，Linux区分大小写。 这意味着**Desktop**与**desktop**不同，与**DeskTop**不同。 其中每个都代表不同的文件或目录名称。许多来自Windows环境的人都会发现这令人沮丧。 如果您收到错误消息“找不到文件或目录”（“**file or directory not found**”），并且您确定文件或目录存在，则可能需要检查您的大小写。

**目录**这与Windows中的文件夹相同。目录提供了一种组织文件的方式，通常是采用分层方法。

**Home**每个用户都有自己的/ home目录，这通常是默认情况下保存您创建的文件的位置。

**Kali Linux**是专为渗透测试而设计的Linux发行版。它预装了数百种工具，可以节省您自己下载和安装它们所需的时间。在撰写本文时，我将使用最新版本的Kali：Kali 2018.2，于2018年4月首次发布。

**root**与几乎所有操作系统一样，Linux拥有管理员或超级用户帐户，专为可以在系统上执行任何操作的受信任人员使用而设计。这包括重新配置系统，添加用户和更改密码等内容。在Linux中，该帐户称为root。作为黑客或测试者，您通常会使用root帐户来控制系统。实际上，许多黑客工具都要求您使用root帐户。

**脚本**这是在解释环境中运行的一系列命令，可将每行转换为源代码。许多黑客工具都是简单的脚本。 脚本可以使用bash解释器或任何其他脚本语言解释器运行，例如Python，Perl或Ruby。Python是目前黑客中最受欢迎的解释器。

**Shell**这是一个在Linux中运行命令的环境和解释器。最广泛使用的shell是bash，它代表Bourneagain shell，但其他流行的shell包括C shell和Z shell。我将在本书中专门使用bash shell。

**终端(**Terminal**)**这是命令行界面（CLI）。

有了这些基础知识，我们将尝试有条不紊地强化成为黑客或渗透测试人员所需的基本Linux技能。在第一章中，我将引导您开始使用Kali Linux。

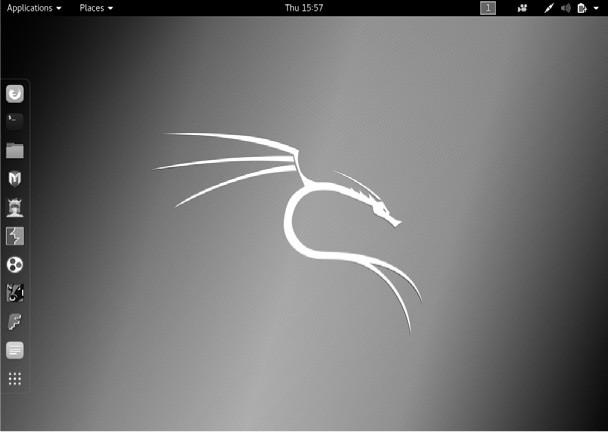
### KALI之旅

一旦你启动Kali，你就会看到一个登录界面，如图1-1所示。使用**root**帐户用户名*root*和默认密码*toor*登录。



*图1­1: 使用root帐户登录Kali*

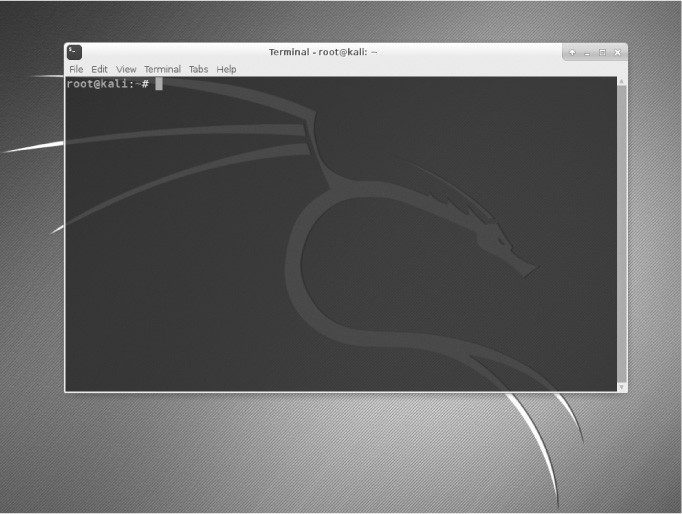
您现在应该可以访问您的Kali桌面（参见图1-2）。 我们将快速查看桌面的两个最基本的方面：终端接口和文件结构。



*图1­2: Kali 桌面*

#### *终端*

使用Kali的第一步是打开终端，这是我们将在本书中使用的命令行界面。在Kali Linux中，您将在桌面底部找到终端的图标。双击此图标以打开终端或**CTRL­ALT­T**。您的新终端应如图1-3所示。



*图1­3: Kali终端*

此终端打开命令行环境（称为shell），使您可以在底层操作系统上运行命令并编写脚本。虽然Linux有许多不同的shell环境，但最受欢迎的是**bash shell**，它也是Kali和许多其他Linux发行版中的默认shell。

要更改密码，可以使用命令**passwd**。

#### *Linux文件系统*

Linux文件系统结构与Windows有些不同。Linux在文件系统的基础上没有物理驱动器（例如C：驱动器），而是使用逻辑文件系统。在文件系统结构的最顶层是/，它通常被称为文件系统的根，就好像它是一个倒置树（见图1-4）。请记住，这与root用户不同。这些术语起初可能看起来令人困惑，但是一旦习惯了Linux，它们就会变得更容易区分。

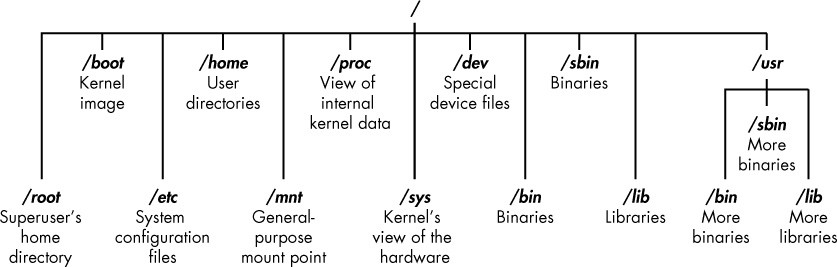


图1­4: Linux 文件系统

文件系统的根（/）位于文件系统目录树的顶部，以下是要了解的最重要的子目录：

**/root** root用户的主目录

**/etc** 通常包含Linux配置文件 - 控制程序启动时间和方式的文件

**/home** 用户的主目录

**/mnt** 将其他文件系统附加或安装到文件系统的位置

**/media** CD和USB设备通常连接或安装到文件系统的位置

**/bin** 其中包含应用程序二进制文件（相当于Microsoft Windows中的可执行文件）

**/lib** lib库文件（与Windows DLL类似的共享程序）

在本书中，我们将花更多时间在这些关键目录上。了解这些一级目录对于从命令行导航文件系统非常重要。

在开始之前，知道在执行例行任务时不应该以root用户身份登录也很重要，因为当你以root身份登录时，任何攻击你的系统的人（是的，黑客有时会被黑客入侵）会立即获得root权限，从而“拥有”你的系统。在启动常规应用程序，浏览Web，运行Wireshark等工具时以常规用户身份登录。

### LINUX基本命令

首先，让我们看看一些基本命令，它们将帮助您在Linux中启动和运行。

#### *用pwd查看当前目录*

与在Windows或macOS等图形用户界面（GUI）环境中工作的情况不同，Linux中的命令行并不总是能够明确显示您当前所在的目录。要导航到新目录，通常需要知道你现在的位置。显示当前工作目录使用命令**pwd**。

在目录结构中的位置输入**pwd**。在您的终端输入密码以查看您的所在目录位置：

kali>pwd

/root

在这种情况下，Linux返回/root，告诉我当前在root用户的目录中。并且因为您在启动Linux时以root用户身份登录，所以您也应该位于root用户的目录中，该目录位于文件系统结构顶部（/）的一级目录。

如果您在另一个目录中，pwd将返回该目录名称。

#### *使用whoami查看登录用户*

在Linux中，超级用户或系统管理员名为root，它具有添加用户、更改密码、更改权限等所需的所有系统权限。显然，您不希望任何人有能力进行此类更改；您希望有人可以信任并且对操作系统有正确的了解。作为黑客，您通常需要拥有所有这些权限来运行您需要的程序和命令（除非您拥有root权限，否则许多黑客工具将无法运行），因此您需要以root用户身份登录。

如果您忘记了以root用户身份还是以其他用户身份登录，则可以使用**whoami**命令查看您登录的用户：

kali>whoami

root

如果我以其他用户身份登录，例如我的个人帐户，那么whoami会返回我的用户名，如下所示：

kali >whoami

OTW

#### *浏览Linux文件系统*

从终端导航到文件系统是一项重要的Linux技能。要完成任何工作，您需要能够寻找位于其他目录中的应用程序、文件和目录。在基于GUI的系统中，您可以直观地看到目录，但是当您使用命令行界面时，结构完全基于文本，导航文件系统意味着使用某些命令。

##### 使用cd更改目录

要从终端更改目录，请使用更改目录命令**cd**。例如，以下是如何进入用于存储配置文件的/ etc目录：

kali >cd /etc

root@kali:/etc#

提示符更改为**root @ kali:/ etc**，表示我们位于/ etc目录中。我们可以通过输入**pwd**来确认：

root@kali:/etc# pwd

/etc

要在文件结构中向上移动一级（朝向文件结构的根目录，或/），我们使用cd后跟双点（..），如下所示：

root@kali:/etc# cd ..

root@kali:/# pwd

/

root@kali:/#

这会将我们从/ etc升级到/ root目录，但您可以根据需要向上移动多个级别。只需使用相同数量的双点对（..）作为要移动的级别数：

你会使用 .. 向上移动一级。

你会使用 .. .. 向上移动两级目录。

您可以使用 .. .. .. 向上移动三级，依此类推。

因此，例如要向上移动两级目录，请输入cd，然后输入两组双点，其间有空格：

kali >cd .. ..

您还可以通过输入cd /，从任何地方升级到文件结构中的根级别，其中/表示文件系统的根目录。

##### 使用ls列出目录的内容

要查看目录（文件和子目录）的内容，我们可以使用**ls**（list）命令。这与Windows中的dir命令非常相似。

kali >ls

bin initrd.img media run var

boot initrd.img.old mnt sbin vmlinuz

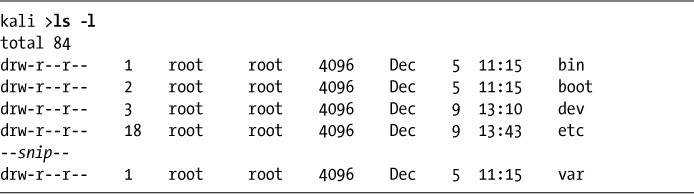
dev lib opt srv vmlinuz.old

etc lib64 proc tmp

home lost+found root usr

此命令列出目录中包含的文件和目录。您也可以在任何特定目录上使用此命令，而不仅仅是您当前所在的目录，方法是在命令后列出目录名称，例如，**ls /etc**显示/etc目录中的内容。

要获取有关文件和目录的更多信息，例如它们的权限、所有者、大小以及上次修改它们的时间，可以在**ls**之后添加**-l**参数（l代表long）。这通常被称为长列表。我们来试试吧：



如您所见，**ls -l**为我们提供了更多信息，例如对象是文件还是目录、链接数、所有者、组、大小、创建或修改时的时间及其名称。

我通常在Linux中进行列出文件列表时添加-l参数，但是每个参数都需要自己添加。我们将在第5章中详细讨论**ls -l**。

Linux中的某些文件是隐藏的，不会通过简单的**ls**或**ls -l**命令显示。要显示隐藏文件，请添加小写**-a**参数，如下所示：

kali >ls -la

如果平时（使用**ls**）你没有看到你期望看到的文件，那么值得尝试使用ls加上 –a参数。

#### *获取帮助*

几乎每个命令，应用程序或实用程序都在Linux中有一个专用的帮助文件，为其使用提供指导。例如，如果我需要使用最好的无线破解工具aircrackng的帮助，我只需输入aircrack-ng命令，然后输入**--help** 命令:

kali >aircrack-ng --help

请注意这里的双破折号（--）。Linux中的约定是在单词类选项参数之前使用双短划线（--），例如帮助，在单字母选项参数之前使用单个短划线（ - ），例如-h。

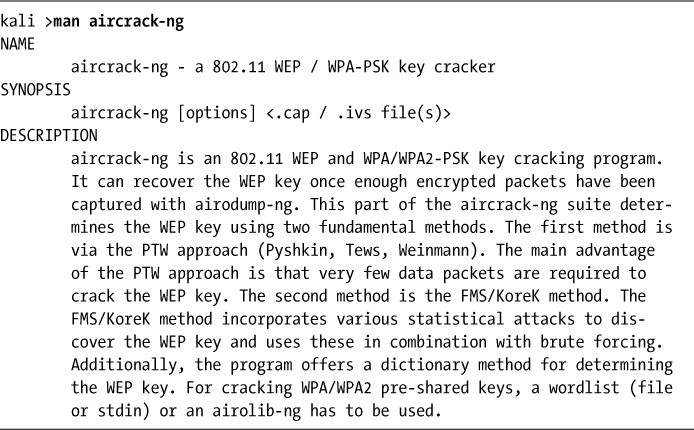
输入此命令时，您应该看到该工具的简短描述以及如何使用它的指导。在某些情况下，您可以使用-h或 -？ 转到帮助文件 例如，如果我在使用黑客最好的端口扫描工具nmap时需要帮助，我将输入以下内容：

kali >nmap -h

不幸的是，虽然许多应用程序支持所有三个选项（ **--help**，**-h**和 **-？**），但无法保证您正在使用的应用程序。因此，如果其中一个选项不起作用，请尝试另一个。

##### 使用man引用手册页

除了帮助信息之外，大多数命令和应用程序都有一个手册（man）页面，其中包含更多信息，例如命令或应用程序的描述和概要。只需在命令、实用程序或应用程序之前键入**man**即可查看手册页。例如，要查看aircrackng的手册页，请输入以下内容：



这将打开aircrackng手册，为您提供比帮助信息更详细的信息。您可以使用**ENTER**键滚动浏览此手册文件，也可以分别使用**PG DN**和**PG UP**键向上和向下翻页。要退出，只需输入**q**（退出），然后返回命令提示符。

### 搜索查找

在你熟悉Linux之前，找到自己的方法会很令人沮丧，但是对一些基本命令和技术的了解将大大有助于使命令行更加友好。以下命令可帮助您从终端查找内容。

#### *使用locate搜索*

可能最容易使用的命令是**locate**。接下来是一个关键字，表示您想要查找的内容，此命令将遍历整个文件系统并找到该单词的每个匹配项。

例如，要查找aircrackng，请输入以下内容：

kali >locate aircrack-ng

/usr/bin/aircrack­ng

/usr/share/applications/kali­aircrack­ng.desktop

/usr/share/desktop­directories/05­1­01­aircrack­ng.directory

­­snip­­

/var/lib/dpkg/info/aircrack­ng.mg5sums

但是，**locate**命令并不完美。有时，定位的结果可能是压倒性的，给你太多的信息。此外，**locate**使用的数据库通常每天只更新一次，因此如果您刚刚在几分钟或几小时前创建了一个文件，它可能会在第二天才显示在此列表中。了解这些基本命令的缺点，以便您可以更好地决定何时最好使用每个命令。

#### *用whereis查找二进制文件*

如果您要查找二进制文件，可以使用**whereis**命令找到它。此命令不仅返回二进制文件的位置，还返回其源和手册页（如果可用）。以下是一个例子：

kali >whereis aircrack-ng

aircarck­ng: /usr/bin/aircarck­ng /usr/share/man/man1/aircarck­ng.1.gz

在这种情况下，**whereis**只返回aircrackng二进制文件和手册页，而不是每次出现aircrackng这个词。 更有效率和更有启发性，你不觉得吗？

#### *用which在PATH变量中查找二进制文件*

**which**命令更具体：它只返回Linux中PATH变量中二进制文件的位置。我们将在第7章中更仔细地查看PATH变量，但是现在知道PATH保存操作系统查找在命令行执行的命令的目录就足够了。例如，当我在命令行上输入aircrack-ng时，操作系统会查看PATH变量以查看它应该在哪些目录中查找aircrackng：

kali >which aircrack-ng

/usr/bin/aircrack­ng

在这里，它能够在PATH变量中列出的目录中找到单个二进制文件。 至少，这些目录通常包含/usr/bin，但可能包括/usr/sbin以及其他一些目录。

#### *使用find执行更强大的搜索*

**find**命令是搜索实用程序中功能最强大且最灵活的。它能够在任何指定的目录中开始搜索，并查找许多不同的参数，当然包括文件名，还包括创建或修改的日期，所有者，组，权限和大小。

这是**find**的基本语法：

find *directory options expression*

因此，如果我想在根目录中搜索一个名为apache2(开放源码web服务器)的文件，我将输入以下命令:

kali >find /➊ -type f➋ -name apache2➌

首先，➊是说明了开始搜索的目录，在这种情况下是 / 。然后➋我指定要搜索的文件类型，在本例中为f表示普通文件。最后，➌我给出了我正在搜索的文件的名称，在本例中为apache2。

此搜索的结果如下所示：

kali >find / -type f -name apache2

/usr/lib/apache2/mpm­itk/apache2

/usr/lib/apache2/mpm­event/apache2

/usr/lib/apache2/mpm­worker/apache2

/usr/lib/apache2/mpm­prefork/apache2

/etc/cron.daily/apache2

etc/logrotate.d/apache2

/etc/init.d/apache2

/etc/default/apache2

find命令从文件系统（/）的顶部开始，遍历每个目录，在文件名中查找apache2，然后列出找到的所有实例。

正如您可能想象的那样，在每个目录中查找的搜索可能很慢。加快速度的一种方法是只查看您希望找到所需文件的所在目录。在这种情况下，比如我们正在寻找配置文件，因此我们可以在/etc目录中开始搜索，而Linux只会搜索其子目录。我们来试试吧：

kali >find /etc -type f -name apache2

/etc/init.d/apache2

/etc/logrotate.d/apache2

/etc/cron.daily/apache2

这个更快的搜索只在/etc目录及其子目录中发现了apache2的出现。同样重要的是，要注意与其他一些搜索命令不同，find只显示确切的名称匹配。如果文件apache2有扩展名，例如apache2.conf，则搜索找不到匹配项。我们可以通过使用通配符来解决此限制，这使我们能够匹配多个字符。通配符有几种不同的形式：**\* . , ?** 和 **[]** 。

让我们在/etc目录中查看以apache2开头并具有任何扩展名的所有文件。为此，我们可以使用以下通配符编写find命令：

kali >find /etc -type f --name apache2.\*

/etc/apache2/apache2.conf

当我们运行此命令时，我们发现/etc目录中有一个文件符合**apache2.\***模式。当我们使用一个点后跟\*通配符时，终端会在文件名apache2之后查找任何扩展名。这对于查找您不知道文件扩展名的文件非常有用。

当我运行此命令时，我在/etc目录中找到两个以apache2开头的文件，包括apache2.conf文件。

**快速查看通配符**

假设我们正在搜索包含*cat，hat，what*和*bat*的文件目录。 则通配符？用于表示单个字符，因此搜索？at会找到*hat，cat*和*bat*而不是*what*，因为在此文件名 *?at* 中前面有两个字母。[]通配符用于匹配方括号内显示的字符。例如，搜索*[c，b]at*会匹配*cat*和*bat*而不是*hat*或别的什么。最常用的通配符是星号（\*），它匹配任何长度的任何字符，从无字符到无限数量的字符。例如，搜索\* at会找到*hat，cat*，*bat*及*what*。

#### *用grep过滤*

通常在使用命令行时，您需要搜索特定关键字。 为此，您可以使用**grep**命令作为过滤器来搜索关键字。

当输出从一个命令传送到另一个命令时，通常使用**grep**命令。我在第2章介绍了管道，但是现在，只要说Linux（和Windows就此问题）允许我们获取一个命令的输出并将其作为输入发送到另一个命令就足够了。这叫做管道，我们使用 | 命令符号执行此操作（|键通常位于键盘上的ENTER键上方）。

**ps**命令用于显示有关计算机上运行的进程的信息。我们将在第6章中更详细地介绍这一点，但是对于这个示例，假设我想看到我的Linux系统上运行的所有进程。在这种情况下，我可以使用**ps**（进程）命令，然后使用**aux**参数来指定要显示的进程信息，如下所示：

kali >ps aux

这为我提供了在这个系统中运行的所有进程的列表 - 但是如果我只是想找到一个进程来查看它是否正在运行呢？

我可以通过将**ps**的输出信息，管道输出到**grep**并搜索关键字来完成此操作。例如，要查明apache2服务是否正在运行，我将输入以下内容。

kali >ps aux | grep apache2

root 4851 0.2 0.7 37548 7668 ? Ss 10:14 0:00 /usr/sbin/apache2 ­k start

root 4906 0.0 0.4 37572 4228 ? S 10:14 0:00 /usr/sbin/apache2 ­k start

root 4910 0.0 0.4 37572 4228 ? Ss 10:14 0:00 /usr/sbin/apache2 ­k start

­­snip­­

此命令告诉Linux显示我的所有服务，然后将该输出发送到**grep**，后者将查看关键字apache2的输出，然后仅显示apache2相关的输出，从而为我节省了大量时间和视力。

### 修改文件和目录

找到文件和目录后，您将希望能够对它们执行操作。在本节中，我们将介绍如何创建文件和目录，复制文件，重命名文件以及删除文件和目录。

#### *创建文件*

有许多方法可以在Linux中创建文件，但是现在我们只看两个简单的方法。第一个是**cat**，它是连接（concatenate）的缩写，意思是将各个部分组合在一起（不是你最喜欢的驯养猫科动物cat）。**cat**命令通常用于显示文件的内容，但也可用于创建小文件。要创建更大的文件，最好在文本编辑器（如vim，emacs，leafpad，gedit或kate）中输入代码，然后将其另存为文件。

##### 使用cat连接

**cat**命令后跟一个文件名将显示该文件的内容，但是为了创建一个文件，我们遵循带有重定向的cat命令，用 **>** 符号表示，以及我们想要创建的文件的名称。以下是一个例子：

kali> cat > hackingskills

Hacking is the most valuable skill set of the 21st century!

当您按**ENTER**键时，Linux将进入交互模式并等待您开始输入该文件的内容。这可能令人费解，因为提示符（ kali >）消失了，但只要你开始打字，无论你输入什么都将写入文件内（在这种情况下，输入hackingskills）。在这里，我键入“Hacking is the most valuable skill set of the 21st century!”。

要退出并返回提示，请按**CTRL­D**。然后，当我想查看文件hackingskills中的内容时，我输入以下内容：

kali> cat hackingskills

Hacking is the most valuable skill set of the 21st century!

如果您不使用重定向符号，Linux将直接在终端打印出文件的内容。要向文件添加或附加更多内容，可以使用带有双重定向（>>）的**cat**命令，然后使用要添加到文件末尾的任何内容。以下是一个例子：

kali> cat >> hackingskills

Everyone should learn hacking

Linux再次进入人机交互模式，等待输入内容附加到文件。当我键入“Everyone should learn hacking”并按**CTRL­D**，我回到了终端提示符。现在，当我用cat显示该文件的内容时，我可以看到该文件已经附加了内容“Everyone should learn hacking”，如下所示：

kali > cat hackingskills

Hacking is the most valuable skill set of the 21st century! Everyone should learn hacking

如果我想用新内容信息覆盖文件，我可以简单地再次使用**cat**命令和一个重定向符号（>），如下所示：

kali > cat > hackingskills

Everyone in IT security without hacking skills is in the dark

kali > cat hackingskills

Everyone in IT security without hacking skills is in the dark

命令的含义如下：

cat > hackingskills #是打开或创建一个文件并(以人机交互模式)写入内容

cat hackingskills #在控制台终端上打印查看文件内容

正如您在此处看到的，Linux进入交互模式，然后输入新文本然后退回到提示符。当我再次使用**cat**来查看文件的内容时，我发现我之前的单词已被最新文本覆盖。

##### 用touch创建文件

文件创建的第二个命令是**touch**。此命令最初开发是用来用户只需touch文件即可更改其某些详细信息，例如创建或修改日期。但是，如果该文件尚不存在，则此命令默认情况下会创建该文件。

 让我们用**touch**创建一个文件名为newfile：

kali >touch newfile

现在，当我使用**ls -l**查看目录的长列表时，我看到已经创建了一个名为**newfile**的新文件。 请注意，它的大小为0，因为**newfile**中没有内容。

#### *创建目录*

在Linux中创建目录的命令是**mkdir**，它是创建目录(make directory)的缩写。要创建名为newdirectory的目录，请输入以下命令：

kali >mkdir newdirectory

要导航进入到这个新创建的目录下，只需输入：

kali >cd newdirectory

#### *复制文件*

要复制文件，我们使用**cp**命令。这会在新的目录位置创建文件的副本，并保留旧文件。

在这里，我们将使用**touch**在根目录中创建一个文件oldfile，并将其复制到/root/newdirectory，在进程中重命名并保留原始oldfile：

kali >touch oldfile

kali >cp oldfile /root/newdirectory/newfile

重命名文件是可选的，只需将您想要的名称添加到目录路径的末尾即可。如果在复制文件时不重命名该文件，则默认情况下该文件将保留原始名称。

当我们导航进入到newdirectory下时，我们看到有一个名为newfile的oldfile的精确副本：

kali >cd newdirectory

kali >ls

newfile oldfile

#### *重命名文件*

不幸的是，Linux没有专门用于重命名文件的命令（如Windows和其他一些操作系统那样），但它确实有**mv**（move）命令。

**mv**命令可用于将文件或目录移动到新的目录位置，或者只是为现有文件指定一个新名称（重命名）。要将newfile重命名为newfile2，请输入以下内容：

kali >mv newfile newfile2

kali >ls

oldfile newfile2

现在当您列出（**ls**）该目录时，您会看到newfile2而不是newfile，因为它已被重命名。你可以对目录做同样的事情。

#### *删除文件*

要删除文件，只需使用**rm**命令，如下所示：

kali >rm newfile2

如果您现在在目录上执行长列表的**ls**命令，则可以确认该文件已被删除。

#### *删除目录*

删除目录的命令类似于删除文件的**rm**命令，但附加了**dir**（用于目录），如下所示：

kali >rmdir newdirectory

rmdir:failed to remove 'newdirectory': Directory not empty

重要的是要注意**rmdir**不会删除非空的目录，但会给你一条警告信息“目录不为空”(Directory not empty)，如本例所示。在删除目录之前，必须先删除该目录下的所有内容。这是为了阻止您意外删除您不想删除的对象文件。

如果你想一次性删除一个目录及其下的内容，你可以在**rm**之后使用**-r**参数，如下所示：

kali >rm -r newdirectory

但需要注意的是：要小心使用**-r**选项和**rm**，至少在开始时，因为错误地删除有价值的文件和目录非常容易。例如，在主目录（/）中使用**rm -r**会删除那里的每一个文件和目录 – 这不是你想要的致命性的动作。

### 现在开始!

现在您已经掌握了一些在文件系统中导航切换的基本技能，您可以在进行（黑客游戏）之前稍微使用Linux系统。使用终端的最佳方法是立即尝试使用新发现的技能。在随后的章节中，我们将深入探讨我们的黑客游戏。

**练习**

在继续讨论第2章之前，请尝试使用从中学到的技能完成以下小节的练习：

1.使用根（/）目录中的**ls**命令来探索Linux的目录结构。使用**cd**命令移动到每个目录并运行**pwd**以验证您在目录结构中的位置。

2.使用**whoami**命令验证您以哪个用户身份登录。

3.使用**locate**命令查找可用于密码破解的单词列表。

4.使用**cat**命令创建新文件，然后附加内容到该文件。请记住 > 将输入重定向到文件（覆盖），而 >> 将内容附加到文件中。

5.创建一个名为hackerdirectory的新目录，并在该目录中创建一个名为hackedfile的新文件。现在将该文件复制到/root目录下并将其重命名为secretfile。

## 2

## TEXT MANIPULATION

**文本操作**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 3

## ANALYZING AND MANAGING NETWORKS

**分析和管理网络**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 4

**ADDING AND REMOVING SOFTWARE**

**添加和删除软件**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 5

**CONTROLLING FILE AND DIRECTORY PERMISSIONS**

**控制文件和目录权限**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 6

**PROCESS MANAGEMENT**

**流程管理**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 7

**MANAGING USER ENVIRONMENT VARIABLES**

**管理用户环境变量**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 8

**BASH SCRIPTING**

**BASH脚本编程**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 9

**COMPRESSING AND ARCHIVING**

**压缩和归档**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 10

**FILESYSTEM AND STORAGE DEVICE MANAGEMENT**

**文件系统和存储设备管理**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 11

**THE LOGGING SYSTEM**

**日志系统**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 12

**USING AND ABUSING SERVICES**

**使用和滥用服务**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 13

**BECOMING SECURE AND ANONYMOUS**

**安全和匿名**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 14

**UNDERSTANDING AND INSPECTING WIRELESS NETWORKS**

**理解和检查无线网络**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 15

**MANAGING THE LINUX KERNEL AND LOADABLE KERNEL MODULES**

**管理LINUX内核和可加载内核模块**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 16

**AUTOMATING TASKS WITH JOB SCHEDULING**

**使用作业调度自动化任务**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## 17

**PYTHON SCRIPTING BASICS FOR HACKERS**

**黑客的PYTHON脚本基础**



By our very nature, hackers are doers. We want to touch and play with things. We also want to create and, sometimes, break things. Few of us want to read long tomes of information technology theory before we can do what we love most: hacking. With that in mind, this chapter is designed to give you some fundamental skills to get you up and running in Kali . . . now!

## SPIRING HACKER? START HERE.

**顶级黑客？从这开始**



**COVERS KALI LINUX AND PYTHON 3**

如果你开始沿着黑客、网络安全和渗透测试的这条激动人心的道路开始，Linux Basics for Hackers是一个很好的第一步。使用Linux的高级渗透测试版Kali Linux，您将学习使用Linux操作系统的基础知识，并获得控制Linux环境所需的工具和技术。

首先，您将学习如何在虚拟机上安装Kali并了解基本的Linux概念。接下来，您将处理更广泛的Linux主题，如操作文本、控制文件和目录权限以及管理用户环境变量。然后，您将专注于基础黑客概念，如安全性和匿名性，并使用bash和Python学习脚本技能。

实践教程和练习将贯穿始终，将强化和测试您的技能，因为您将学习如何：

* 通过更改网络信息和操作rsyslog日志记录实用程序来覆盖您的痕迹，编写工具以扫描网络连接，并连接和收听无线网络
* 使用Tor、代理服务器、VPN和加密电子邮件保持您的互联网活动隐秘
* 编写bash脚本以扫描开放端口以查找潜在的目标
* 使用和滥用，如MySQL，Apache WebServer和OpenSSH等服务
* 构建自己的黑客工具，例如远程视频间谍摄像头和密码破解程序

黑客攻击很复杂，而且没有单一的方法。为什么不从一开始就使用Linux Basics for Hackers？

**关于作者**

OccupyTheWeb是一名信息安全顾问，调查取证专家员和培训师，拥有超过20年的行业经验。他负责维护HackersArise培训网站（https://www.hackersarise.com/），并培训美国军方人员、国防部承包商和联邦员工进行信息安全和黑客攻击。



**THE FINEST IN GEEK ENTERTAINMENT™**

www.nostarch.com

**关于译者**

汉武安全实验室专注国际范围内主流数据库安全漏洞和数据安全攻防技术研究，是杭州汉领信息科技有限公司（www.leadsino.com）旗下数据安全防护与综合安全解决方案能力研究团队，同时是一支独立的、持久的针对数据库安全漏洞、攻击技术模拟和数据库安全防护技术进行研究的专业队伍。



www.hawoo.net