

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)、L1i9n8g8、nJcx、ink247GG 、咸鱼

校对：HawooSeclab

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*

名字：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 记录可在此网址获取 <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**。那是你想要的情形吗？

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。



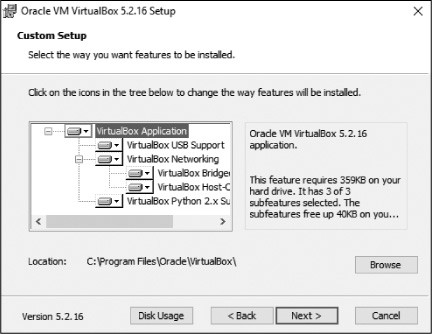
*图1:VirtualBox主页*

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**。

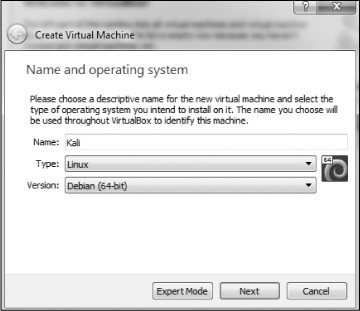
***设置虚拟机***

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。



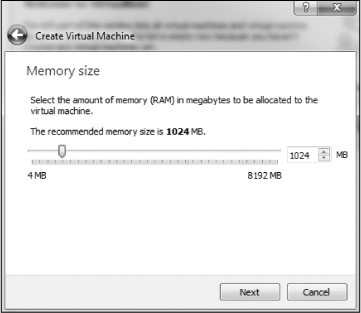
*图4: VirtualBox Manager*

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*

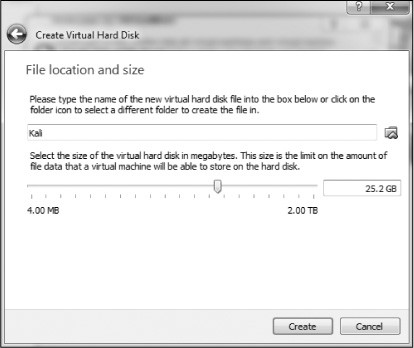
在这里，您需要选择要为此新虚拟机分配多少RAM。

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）。



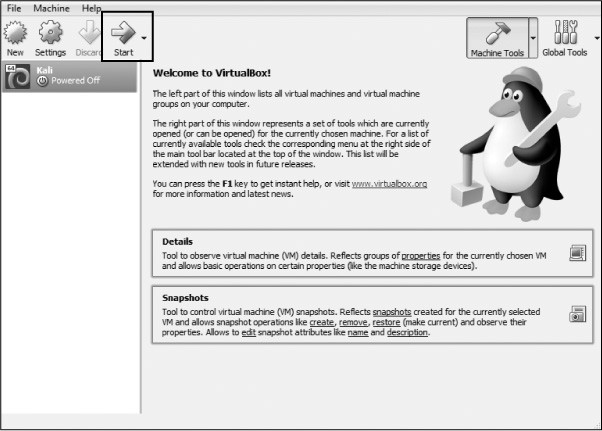
*图7: 分配硬盘空间*

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!

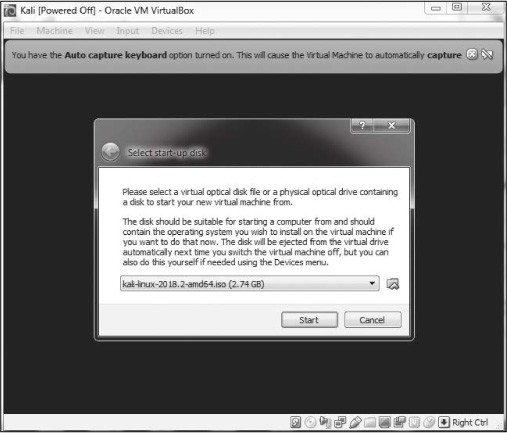
***在VM上安装Kali***

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*

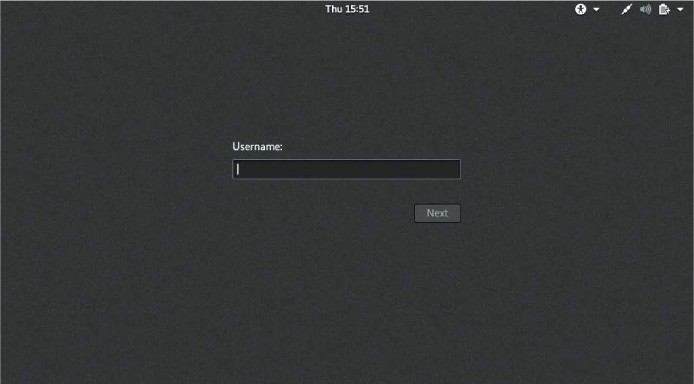
在下一个屏幕上，系统将提示您是自动还是手动安装GRUB引导加载程序。由于原因尚不清楚，如果您选择第二个选项，Kali将倾向于挂起并在安装后显示空白屏幕。选择手动输入设备**Enter device manually**，如图15所示。



*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。

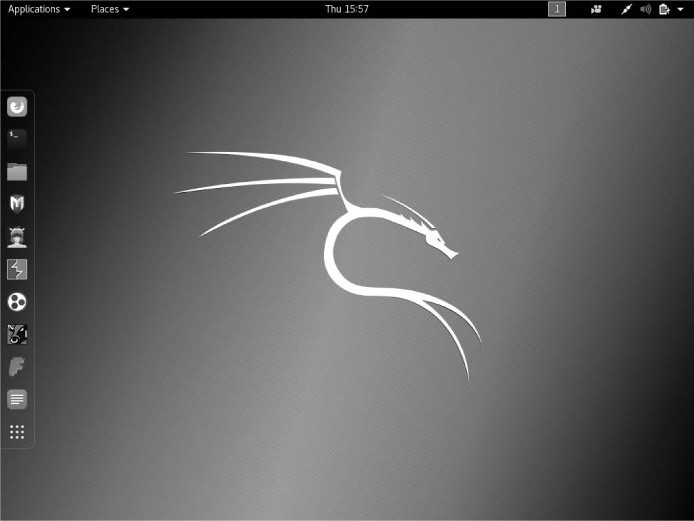
恭喜！你已经安装了Kali。单击**Continue**继续。Kali将尝试重新启动，在您最终遇到Kali 2019的登录屏幕之前，您将看到许多代码行穿过一个空白的黑色屏幕，然后如图16所示。



*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。

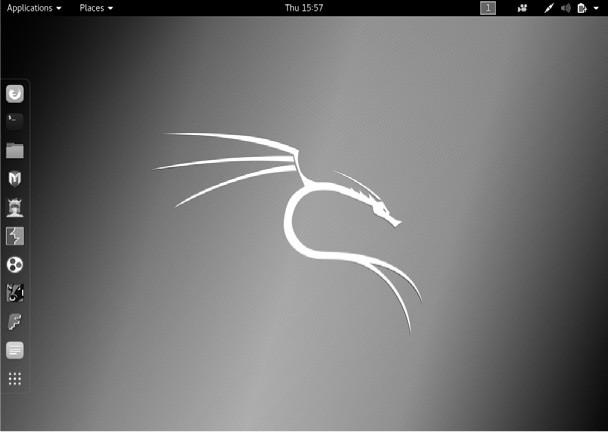
### KALI之旅

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*

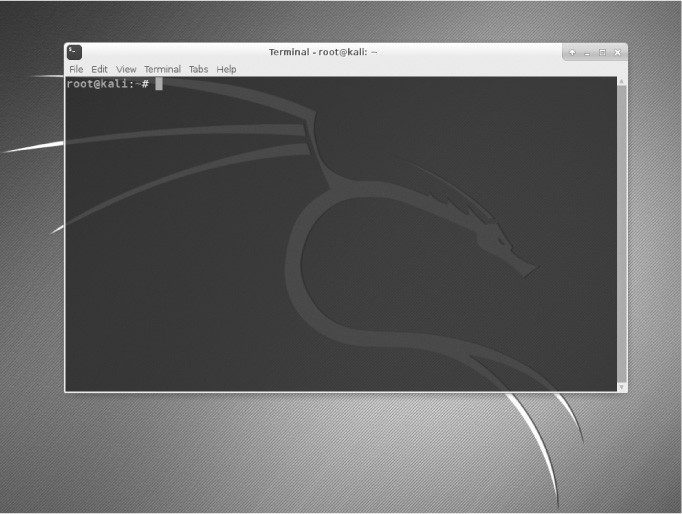
您现在应该可以访问您的Kali桌面（参见图1-2）。 我们将快速查看桌面的两个最基本的方面：终端接口和文件结构。



*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。



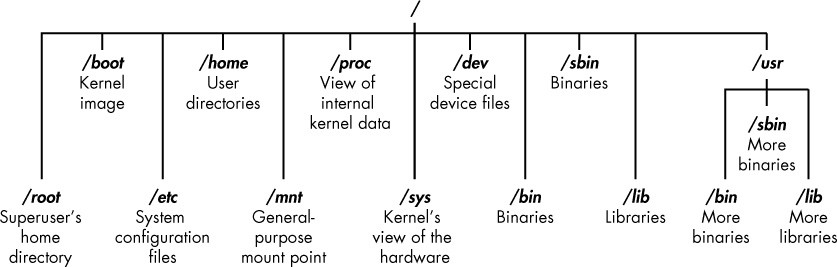
*图1­3: Kali终端*

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

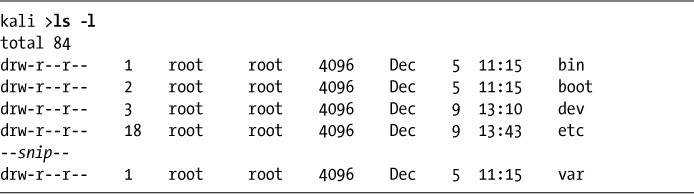
dev lib opt srv vmlinuz.old

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。

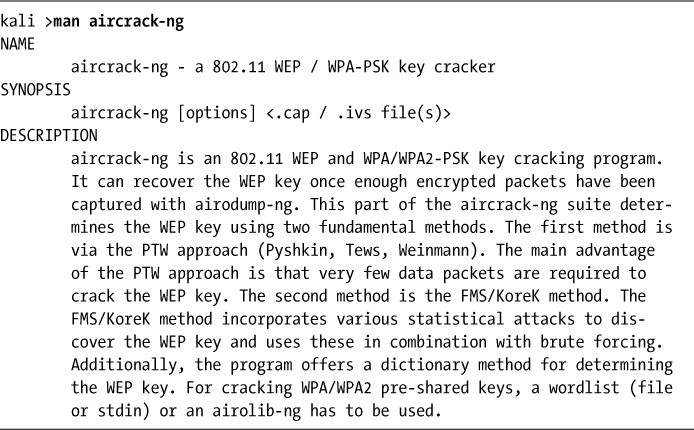
输入此命令时，您应该看到该工具的简短描述以及如何使用它的指导。在某些情况下，您可以使用-h或 -？ 转到帮助文件 例如，如果我在使用黑客最好的端口扫描工具nmap时需要帮助，我将输入以下内容：

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**



在Linux系统中，我们处理的一切都是文件，并且绝大多数都是文本文件；举个例子，在Linux系统中，所有的配置文件都是文本文件。所以我们只需要打开文件，更改文件的内容，保存文件，再重新启动应用就可以更改应用配置。

由于存在大量文本文件，操作文本在Linux系统管理和Linux应用中显得尤为重要。在这一章节， 你可以通过一些命令和技巧，实现在Linux系统下操作文本。

为了方便演示，我将使用世界顶尖的网络入侵检测系统（NIDS）Snort的文件，Snort 最早由Marty Roesch 开发，现在属于Cisco。NIDS经常被用于检测黑客入侵，所以如果你想成为成功的黑客，你必须了解 NIDS如何检测攻击和绕过检测的方法。





*如果你使用的Kali Linux没有预装Snort， 你可以输入 apt-get install snort从Kali源下载Snort。*

### 查看文件

如第1章所示，最基本的打印文本命令是**cat**，但是它有它的限制，使用**cat**命令打印位于/etc/snort的Snort 配置文件（snort.conf）（参见文本清单2-1）

kali >cat /etc/snort/snort.conf

*清单 2-1: 在终端中打印snort.conf*

现在你的屏幕上应该显示了整个snort.conf文件，但这并不是最方便或最实际的使用这个文件的方法。

# include $SO\_RULE\_PATH/exploit.rules

# include $SO\_RULE\_PATH/exploit.rules

# include $SO\_RULE\_PATH/exploit.rules

# include $SO\_RULE\_PATH/exploit.rules

# include $SO\_RULE\_PATH/exploit.rules

--*snip*--

# event thresholding or suppressions commands...

kali >

在接下来的两个小章节，我将向你展示**head** 和**tail** 命令。这是两种只显示部分文件内容的方法，用来更简单地查看关键点。

#### *查看开头*

如果你只是想查看文件开头，你可以使用**head**命令，这个命令默认打印文件的前10行。例如，下面这条命令会打印snort.conf的前10行。

kali >head /etc/snort/snort.conf

#----------------------------------------------

# VRT Rules Packages Snort.conf

#

# For more information visit us at:

--*snip*--

#Snort bugs:bugs@snort.org

如果你想看多于或少于默认的10行，在**head**命令后和文件前输入连接符（**-**）和你想要的数量。例如，如果你想看文件的前20行，你需要输入如清单 2-2 上面的命令。

kali >head -20 /etc/snort/snort.conf

#--------------------------------------------

#VRT Rule Packages Snort.conf

#

#For more information visit us at:

#.

#.

#.

#Options : ­­enable­gre ­­enable­mpls ­­enable­targetbased

­­enable­ppm ­­enable­perfprofiling enable­zlib ­­enable­act live­response ­­enable­normalizer ­­enable­reload ­­enable­react

*清单 2-2: 在终端中打印snort.conf 的前20行*

你应该能在终端中看到snort.conf的前20行。

#### *查看结尾*

**tail**命令 和**head**命令相似。只是**tail**命令用于查看文件最后几行。使用**tail**查看snort.conf：

kali >tail /etc/snort/snort.conf

#include $SO\_RULE\_PATH/smtp.rules

#include $SO\_RULE\_PATH/specific¬threats.rules

#include $SO\_RULE\_PATH/web¬activex.rules

#include $SO\_RULE\_PATH/web¬client.rules

#include $SO\_RULE\_PATH/web¬iis.rules

#include $SO\_RULE\_PATH/web¬miscp.rules

#Event thresholding and suppression commands. See threshold.conf

注意这个命令打印了最后的一些include行，但没有打印所有的include行。因为和head相似，tail默认也是打印10行。你可以打印更多行如snort.conf最后20行。和使用head命令一样，你可以在tail命令和文件之间输入连接符（-）和你想要的行数。如以下清单 2-3

kali >tail -20 /etc/snort/snort.conf

#include $SO\_RULE\_PATH/chat.rules

#include $SO\_RULE\_PATH/chat.rules #include $SO\_RULE\_PATH/chat.rules

­­snip­­

#Event thresholding or suppression commands. See theshold.conf

*清单 2¬3: 在终端中打印snort.conf 的后20行*

现在我们可以一次性看到几乎所有的include行。

#### *标显行数*

有时-尤其是处理非常长的文件的时候-我们可能希望打印文件行号。因为snort.conf 超过600行，标上行号会有很大帮助，这样可以更容易地引用修改的位置并在以后返回到那个位置。

我们使用**nl**（number lines）命令打印行号。输入清单 2-4里的命令。

kali >nl /etc/snort/snort.conf

612 #################################################################

613 #dynamic library rules

614 #include $SO\_RULE\_PATH/bad¬traffic.rules

615 #include $SO\_RULE\_PATH/chat.rules

­­snip­­

630 #include $SO\_RULE\_PATH/web¬iis.rules

631 #include $SO\_RULE\_PATH/web¬misc.rules

*清单 2¬4: 在终端输出中显示行号*

现在每一行都有一个数字（代表行号），引用起来更方便。

### 使用 GREP过滤文本

命令**grep** 大概是使用最广泛的文本操作命令。它可以让你过滤打印出来的文件内容。例如，如果你想查看snort.conf文件里面所有带有output单词的行，你可以使用**cat** 然后要求只打印那些行。(参见清单 2-5)。

kali >cat /etc/snort/snort.conf | grep output

# 6) Configure output plugins

# Step #6: Configure output plugins

# output unified2: filename merged.log, limit 128, nostamp, mpls\_event\_types, vlan\_event\_types

output unified2: filename merged.log, limit 128, nostamp, mpls\_event\_types, vlan\_event\_types

# output alert\_unified2: filename merged.log, limit 128, nostamp

# output log\_unified2: filename merged.log, limit 128, nostamp

# output alert\_syslog: LOG\_AUTH LOG\_ALERT

# output log\_tcpdump: tcpdump.log

*清单 2¬5: 打印被grep规定含有关键词或段落的行*

这个命令或先查看snort.conf 然后使用管道 (|) 将它传递给 grep, 它将会把文件作为输入，寻找出现单词output的行，然后只打印这些行。**grep**命令是使用Linux中的一个非常强大和必要的命令，因为它可以节约搜索文件中每一个词或命令的时间。

#### *挑战: 使用grep, nl, tail, and head*

假设你想使用至少4个之前学过的命令打印 # Step #6: Configure output plugins 前面5行，你该怎么做？（提示：除了我们学过的命令，还有很多其他选择。你可以使用Linux内置命令man来学习更多命令。例如，man tail 会显示tail命令的帮助文档）。

有很多方法可以解决这个问题，我将向你展示通过更改那几行来实现其中一个方法，然后你需要寻找其他方法。

##### 第一步

kali >nl/etc/snort.conf | grep output

34 # 6) Configure output plugins

512 # Step #6: Configure output plugins

518 # output unified2: filename merged.log, limit 128, nostamp, mpls\_event\_types, vlan\_event\_types

521 # output alert\_unified2: filename snort.alert, limit 128, nostamp

522 # output log\_unified2: filename snort.log, limit 128, nostamp

525 # output alert\_syslog: LOG\_AUTH LOG\_ALERT

528 # output log\_tcpdump: tcpdump.log

我们可以看到行 # Step #6: Configure output plugins 是第512行，然后我们知道我们想要第512行前面的5行和第512行本身 (就是第507 到 512行)。

##### 第二步

kali >tail -n+507 /etc/snort/snort.conf | head -n 6

nested\_ip inner, \

whitelist $WHITE\_LIST\_PATH/white\_list.rules, \ blacklist $BLACK\_LIST\_PATH/black\_list.rules

###################################################

# Step #6: Configure output plugins

在这里，我们使用**tail**使文本从第507行开始，再把文本输出到head，然后我们返回文本开头的6行，从而获得Step #6 那行前的5行和Step #6那行本身。

### 使用sed查找和替换

**sed**命令让你可以搜索出现的单词或字段然后在这些字段上做些什么。命令的名字是stream editor（流编辑器）的缩写，因为它的概念和流编辑器是一致的。sed最基本的形式就像Windows系统里的查找和替换功能。

使用**grep**在snort.conf 里查找单词mysql，像这样：

kali >cat /etc/snort/snort.conf | grep mysql

include $RULE\_PATH/mysql.rules #include $RULE\_PATH/server¬mysql.rules

你可以看到 **grep** 命令查找到mysql 出现过两次。

假设你想要**sed** 将每一个出现的mysql 替换成MySQL（记住，Linux大小写敏感）然后保存到文件snort2.conf。你可以输入清单2-6中的命令 ：

kali >sed s/mysql/MySQL/g /etc/snort/snort.conf > snort2.conf

*清单 2¬6: 使用sed 查找替换关键词或字段*

**s**参数提供搜索，你先提供想要搜索的关键词 (mysql) 然后提供想要替换成的关键词 (MySQL), 用斜杠 (/)分开。**g**参数告诉Linux你希望全局替换，然后将结果保存到一个新文件snort2.conf。

现在，当你使用**grep**查找snort2.conf 中的mysql，你将看到没有找到mysql，但是当你搜索MySQL时，你将看到它出现了两次。

kali >cat snort2.conf | grep MySQL

#include $RULE\_PATH/server¬MySQL.rules

如果你只想替换第一个出现的 mysql，你需要去掉末尾的g参数。

kali >sed s/mysql/MySQL/ snort.conf > snort2.conf

你也可以使用sed 命令查找替换第一个出现字段以外的任意位置出现的字段。例如，如果你想只替换第二个出现的mysql，只需要在命令末尾加上出现的次数（这里是2）。

kali >sed s/mysql/MySQL/2 snort.conf > snort2.conf

这个命令值影响第二个出现的mysql。

### 使用more和less查看文件

尽管**cat**是个打开文件和创建小文件的好工具，在打开大文件时它依然有它的限制。当你用cat打开snort.conf,时，文件将一直被打印直到文件结束。如果你想要收集任何信息，这就变得很不实用。

为了打开大文件，我们有另外两个查看工具：**more** 和**less**。

#### *使用more控制显示文件*

**more** 命令一次只显示一页文件，并且让你可以使用**ENTER** 键翻页。这是**man**命令使用的工具,现在我们来使用它。使用**more**命令打开snort.conf （参见清单2-7） 。

kali >more /etc/snort/snort.conf

­­snip­­

# Snort build options:

# Options: ­­enable­gre ­­enable­mpls ­­enable­targetbased

­­enable­ppm ­­enable­perfprofiling enable­zlib ­­enable­active

­response ­­enable­normalizer ­­enable­reload ­­enable­react

­­enable­flexresp3 #

­­More­­(2%)

*清单 2-7: 使用more命令在终端里一次显示一页*

注意**more** 命令只显示一页然后就停止了，并且它会在左下角显示已经显示了多少内容（这里是2%）。按**ENTER**键查看额外的行或页。按**q**键（quit）退出more。

#### *使用less显示和过滤文件*

**less**命令和**more**命令非常相似，但是less有额外的功能，有句话叫 “Less is more。” 使用less，你不但可以滚动查看一个文件，还可以过滤这个文件，清单2-8，使用less打开snort.conf ：

kali >less /etc/snort/snort.conf

­­snip­­

# Snort build options:

# Options: ­­enable­gre ­­enable­mpls ­­enable­targetbased

­­enable­ppm ­­enable­perfprofiling enable­zlib ­­enable­active

­response ­­enable­normalizer ­­enable­reload ­­enable­react

/etc/snort/snort.conf

*清单 2-8: 使用less命令在终端里一次显示一页和过滤内容*

注意**less**在屏幕左下角高亮了文件的路径。如果你按下斜杠键（/），less会让你搜索文件里的字段。例如，当你开始设置Snort时，你需要先确定你想在何时向何处发送攻击警告输出。要想从配置文件中找到这一段，你只需要搜索output，像这样：

# Snort build options:

# Options: ­­enable­gre ­­enable­mpls ­­enable­targetbased

­­enable­ppm ­­enable­perfprofiling enable­zlib ­­enable­active

­response ­­enable­normalizer ­­enable­reload ­­enable­react

/output

这会立即将你带到第一个出现output的地方，并且高亮了output。然后你可以按**n**键（next）到下一个出现output的地方。

# Step #6: Configure output plugins

# For more information, see Snort Manual, Configuring Snort - Output Modules ###################################################################

unified2

# Recommended for most installs

# output unified2: filename merged.log, limit 128, nostamp, mpls\_event\_types,

Vlan\_event\_types

output unified2: filename snort.log, limit 128, nostamp, mpls\_event\_types, vlan\_event\_types

# Additional configuration for specific types of installs

# output alert\_unified2: filename snort.alert, limit 128, nostamp

# output log\_unified2: filename snort.log, limit 128, nostamp

# syslog

# output alert\_syslog: LOG\_AUTH LOG\_ALERT

:

如你所见，less去掉了接下来出现的output并且高亮了所有搜到的字段。在这里, 它直接跳到Snort的输出段，真是方便啊！

### 总结

Linux系统有许多操纵文本的方法，每种方法都有其优缺点。在本章中，我们已经接触了一些最有用的方法，但是我建议您尝试每一种方法，并建立您自己的感觉和偏好。例如，我认为**grep**是不可缺少的，并且我广泛的使用**less**，但是您可能会有不同的观点。

**练习**

在你开始学习第3章之前, 尝试使用你在这章学到的技能完成下面的练习题:

1.进入/usr/share/wordlists/metasploit. 这个目录包含了多个使用metasploit暴力破解受密码保护设备时使用的字典。metasploit 是最受欢迎的渗透测试和黑客框架。

2.使用 **cat** 命令查看文件 passwords.lst 的内容。

3.使用 **more** 命令查看文件 passwords.lst 。

4.使用 **less** 命令查看文件 passwords.lst 。

5.使用 **nl** 命令让文件 passwords.lst 显示行数。这里应该有88,396个密码。

6.使用 **tail** 命令查看文件 passwords.lst 中最后 20 个密码。

7.使用 **cat** 命令查看文件 passwords.lst 然后使用管道查找所有含有123的密码。

## 3

## ANALYZING AND MANAGING NETWORKS

**分析和管理网络**



了解网络对任何一个有追求的黑客都是至关重要的。在许多情况下，你将通过网络攻击某些东西，而优秀的黑客需要知道怎样去和目标网络连接和交互。例如，您可能需要连接到视图中隐藏了Internet协议（IP）地址的计算机，或者你可能需要将目标的域名系统(DNS)查询重定向到您的系统，这些任务都相对比较简单，但是都需要一点Linux网络知识。本章节将向你展示一些在你的网络黑客冒险过程中进行分析和管理网络的基本的Linux工具。

### 使用ifconfig分析网络

**ifconfig**命令是检测活动网络接口并与之交互最基本的工具之一。你可以简单地在终端（terminal）输入ifconfig命令来查询你所在的网络活动连接状态。请自己尝试一下，你应该看到和清单3­1相似的输出。

kali >ifconfig

➊eth0Linkencap:EthernetHWaddr 00:0c:29:ba:82:0f

➋inet addr:192.168.181.131 ➌Bcast:192.168.181.255 ➍Mask:255.255.255.0

­­snip­­

➎lo Linkencap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0

­­snip­­

➏wlan0 Link encap:EthernetHWaddr 00:c0:ca:3f:ee:02

*清单 3­1: 使用ifconfig获取网络信息*

正如你所看到的，ifconfig命令显示了有关系统上活动网络接口的一些有用信息。在输出的顶部是第一个侦测到的接口的名称 eth0 ➊，它是Ethernet0的缩写（Linux从0开始计数而不是1）.这是第一个有线以太网连接接口。如果这里有更多的以太网接口，它们将使用同样的格式 (eth1, eth2 等等)。

接下来列出正在使用的网络类型 (Ethernet - 以太网)，然后是 HWaddr 和一个地址，这是在每个网络硬件上标记的全局唯一地址。在这种情况下，网络接口卡 network interface card (NIC), 通常指的是媒体访问控制 media access control (MAC) 地址。

第二行包含有关当前分配给它的IP地址信息的网络接口 (本例中为 192.168.181.131 ➋); 其次是 Bcast ➌，或者说广播地址，用于向子网上的所有IP发送信息的地址;最后是子网掩码 (Mask ➍)，用于确定IP地址的哪个部分连接到本地网络。你还可以在输出的这一部分中找到更多技术信息，但它超出了Linux网络基础章节的范围。

输出的下一部分显示另一个被称为 lo ➎的网络连接，它是环回地址（loopback address）的缩写，并且有时称为localhost。这是个特殊的软件地址，可帮助你连接到自己的系统。未在系统上运行的软件和服务将无法被使用。你可以使用 lo 在你的系统测试某些内容，例如你自己的web服务器。本地主机通常用IP地址127.0.0.1表示。

第三个连接是接口 wlan0 ➏。只有当你拥有无线接口或适配器时，才会出现这种情况。请注意，它还会显示该设备 (HWaddr)的MAC地址。

来自ifconfig的此信息使您可以连接并操作局域网 (LAN) 设置，这是黑客攻击的基本技能。

### 使用IWCONFIG检查无线网络设备

如果你拥有一个无线网络适配器，你可以使用 **iwconfig** 命令来收集无线攻击的关键信息，例如适配器（网卡）的IP地址，MAC地址，它所处的模式等等。当你使用像 aircrack­ng 这样的无线攻击工具时，你可以从使用该命令来收集特别重要的信息开始。

使用终端(terminal)，让我们使用 **iwconfig**查看一些无线设备（详见清单 3­2）

kali >iwconfig

wlan0 IEEE 802.11bg ESSID:off/any

Mode:Managed Access Point: Not Associated Tx­Power=20 dBm

­­snip­­

lo no wireless extensions

eth0 no wireless extensions

*清单 3­2: 使用 iwconfig来获取无线适配器（网卡）信息*

这里的输出告诉我们，唯一具有无线扩展的网络接口是wlan0，这正是我们所期望的。lo 和 eth0 都没有任何无线扩展。

对于 wlan0，我们了解了我们的设备能够支持的802.11 IEEE无线标准：b 和 g ， 两种早期的无线通信标准。现在大多数无线设备也包括 n ( n 是最新的标准)。

我们还从 iwconfig 中学习了无线扩展的模式(本例中为Mode:Manage，不同于monitor或promiscuous mode)。在破解无线密码时，我们需要使用到混杂模式(promiscuous mode)。

接下来，我们将看到无线网卡（适配器）未连接（未关联）到接入点 (AP) ，并且其功率为 20 dBm，这表示信号强度。 我们将在第14章节 中花更多时间介绍这些信息。

### 更改你的网络信息

具备更改你的IP地址和其他网络信息是一项十分有用的技能，因为它将帮助你来回穿梭于作为可信设备出现时才允许访问的其他网络。例如，在拒绝服务攻击 (DoS) 中，你可以使用欺骗的IP以致于攻击看上去来自其他地方，从而帮助你规避取证分析人员分析IP来源的可能。这在Linux上是一个相当简单的任务，使用 **ifconfig** 命令就可以完成它。

#### *更改你的 IP地址*

要更改IP地址，请输入 **ifconfig** ，然后输入要重新分配的网络接口以及要分配给该接口的新IP地址。 例如，要将IP地址 192.168.181.115 分配给接口 eth0，请输入以下内容：

kali >ifconfig eth0 192.168.181.115

kali >

当你正确地执行此操作时，Linux将简单地返回一个命令提示符并且没有任何输出。这是件好事（没有输出错误信息即代表执行成功）！

然后，当你再次使用 **ifconfig** 命令检查你的网络连接状态时，你应该能查看到你的 IP 地址被更改成你刚刚分配的那个新的IP地址。

#### *更改你的子网掩码和广播地址*

你也可以使用**ifconfig**命令改变你的子网掩码（netmask）和广播地址。例如，如果你想给相同的 eth0 接口分配信息，子网掩码为 255.255.0.0 a，广播地址为 192.168.1.255你可以输入以下内容：

kali >ifconfig eth0 192.168.181.115 netmask 255.255.0.0 broadcast 192.168.1.255

kali >

再一次声明，如果你正确地执行此操作，Linux仅以一个新的命令提示符作为响应。现在请再次输入 **ifconfig** 来验证每一个相关参数是否已相应更改。

#### *欺骗你的MAC地址*

你也可以使用 ifconfig 命令来改变你的 MAC 地址 (或者说 HWaddr). 这个 MAC 地址是全球唯一并且经常被当做一种安全措施来阻击黑客在网络外——或者说跟踪他们。更改你的 MAC 地址来欺骗不同的 MAC 地址几乎是很平常的操作，并且帮助你抵消这些安全措施。因此，这是一项非常有用的绕过网络访问控制技术。

如果你打算伪装你的 MAC 地址，简单地使用 ifconfig 命令的 down 选项来关闭该接口 (在本例中是 eth0) 。然后输入 **ifconfig** 命令并加上接口名称 (hw 表示硬件，ether 表示以太网) a和新的伪造 MAC 地址。最后，使用选项 up 备份接口以进行更改。

这里有个例子：

kali >ifconfig eth0 down

kali >ifconfig eth0 hw ether 00:11:22:33:44:55

kali >ifconfig eth0 up

现在，当你使用 ifconfig 检查你的设置信息时，你应该能看到 HWaddr 更改成你新伪造的MAC地址。（*原书英文版IP address勘误，根据上下文译者判断此处应为MAC地址*）。

#### *从DHCP服务器分配新的IP地址*

Linux有一个动态主机配置协议 (DHCP) 服务，它运行一个守护进程(daemon)— 一个在后台运行的进程—称为 dhcpd，或者说 dhcp daemon。DHCP 服务器为子网上的所有机器分配IP地址，并在随时维护将IP地址分配给哪台机器的日志文件。这使得它成为取证分析人员在攻击后追踪黑客的绝佳资源。出于这个原因，了解 DHCP 服务器的工作原理对一名黑客很有用。

通常来说，从局域网（LAN）连接到internet，你必须有一个 DHCP分配的 IP。因此，在你设置一个静态 IP 后，你必须返回和获取到一个新的 DHCP分配的 IP 地址。为了这么做，你总是需要重启你的系统，但是我将向你演示怎么检索一个新的 DHCP 而不必关闭你的系统并重启它。

要从 DHCP 请求 IP 地址，可以使用 dhclient 命令并在其后加上相应网络接口简单地调用DHCP 服务器，告知你希望分配地址。不同的Linux发行版使用不同的 DHCP 客户端，但是 kali 基于 Debian ，因而使用 **dhclient** 命令。因此，您可以指定一个新地址，如下所示：

kali >dhclient eth0

命令**dhclient**从指定地网络接口（这里是eth0）发送DHCPDISCOVER请求。然后，它会从DHCP服务器（本例中是192.168.181.131）获得一个offer（DHCPOFFER）并使用dhcp请求确认对DHCP服务器的IP分配。

kali >ifconfig

eth0Linkencap:EthernetHWaddr 00:0c:29:ba:82:0f

inet addr:192.168.181.131 Bcast:192.168.181.131 Mask:255.255.255.0

根据DHCP服务器的配置情况，在每种情况下IP地址分配可能是不同的。

当你现在输入 **ifconfig** 时，你应该能看到DHCP服务器已经分配了新的IP地址，广播地址，子网掩码给你的网络接口 eth0。

### 熟练控制你的域名系统

黑客可以很容易从目标的域名系统（DNS）中找到一个信息宝库。DNS在internet是一个至关重要的组成部分，尽管它的设计初衷是把域名转换成IP地址，但是黑客可以使用它从目标处收集信息。

#### *使用dig检测DNS*

DNS是把像hackers­arise.com这样的域名转换成相应的IP地址的服务；通过这种方式，你的机器知道如何到达它。没有DNS我们将不得不记住成千上万我们最喜欢的网站的IP地址——即使对于一个专业学者来说，这也不是一项小任务。

对于有尖端的黑客来说，**dig**是众多有用的Linux命令之一，它提供一种途径来收集目标域名的相关DNS信息。在进行攻击之前，存储在这里的DNS信息可以被认为是前期侦察获取信息的关键部分。这些信息可能包含目标名称服务器（将目标名称转换成IP地址的服务器）的IP地址，目标邮件服务器以及潜在的所有子域名和IP地址。

例如，输入**dig hackers-arise.com**并加入选项ns(nameserver的缩写)。对于hackers­arise.com这个名称服务器显示在清单 3­3的ANSWER SECTION部分。

kali >dig hackers-arise.com ns

­­snip­­

;; QUESTION SECTION:

;hackers­arise.com. IN NS

;; ANSWER SECTION:

hackers­arise.com. 5 IN NS ns7.wixdns.net.

hackers­arise.com. 5 IN NS ns6.wixdns.net.

;; ADDITIONAL SECTION:

ns6.wixdns.net. 5 IN A 216.239.32.100

­­snip­­

*清单 3­3: 使用 dig 和它的 ns 选项从一个域名服务器获取信息*

另外请注意，在ADDITIONAL SECTION部分，dig查询显示了为hackers­arise.com 提供服务的DNS服务器的IP地址(216.239.32.100)。

你也可以使用**dig**命令来获取电子邮件服务器信息，通过连接一个域名并加上选项mx(mx是邮件交换服务的缩写)。该信息对于电子邮件系统的攻击中至关重要。例如，www.hackers­arise.com电子邮件服务器上的信息在显示在清单 3­4的AUTHORITY SECTION部分中。

kali >dig hackers-arise.com mx

­­snip­­

;; QUESTION SECTION:

;hackers­arise.com. IN MX

;; AUTHORITY SECTION:

hackers­arise.com. 5 IN SOA ns6.wixdns.net. support.wix.com 2016052216 10800

3600 604 800 3600

­­snip­­

*清单 3­4: 使用 dig 和它的 mx 选项来获取域名邮件交换服务器上的信息*

最常见的Linux DNS 服务是Berkeley Internet Name Domain(BIND)。在某些情况下，Linux用户将DNS称为BIND，但是不要混淆：DNS和BIND都将各个域名映射到IP地址。

#### *更改你的DNS服务器*

在某些情况下，你可能希望使用其他DNS服务器。为了这么做，你将编辑一个在操作系统名为/etc/resolv.conf纯文本文件。使用文本编辑器打开这个文件——这里我使用Leafpad。然后，在你的命令行输入你选择的编辑器准确的名称并在后面加上文件的位置和文件名。例如：

kali >leafpad /etc/resolv.conf

将我指定的图形文本编辑器Leafpad里打开位于/etc目录下的resolv.conf文件在。这个文件的内容看上去应该如图 3­1所示。



*图 3­1: 在文本编辑器中的典型的resolv.conf 文件*

正如你在第三行看到的，我的名称服务器在这里设置为192.168.181.2的本地DNS服务器。它正常工作，但是如果我希望添加或者替换DNS服务器为8.8.8.8的Google公共DNS服务器。我需要在/etc/resolv.conf文件中添加以下行来指定这个名称服务器 ：

nameserver 8.8.8.8

然后我需要保持这个文件。但是，你也可以通过输入以下指定命令达到同样的效果：

kali >echo "nameserver 8.8.8.8"> /etc/resolv.conf

这个命令回显字符串nameserver 8.8.8.8并将其重定向（>）到文件/etc/resolv.conf中，替换掉当前的内容。你的/etc/resolv.conf文件现在应如图3-2所示。



*图 3­2: 更改 resolv.conf 文件信息来指定 Google DNS 服务器*

如果你现在打开/etc/resolv.conf文件，你将看到它将DNS请求指向Google的DNS服务器而不是本地DNS服务器。你的机器现在将转到Google公共DNS服务器来解析域名成IP地址。这意味着域名解析将花费更长的时间(可能是几毫秒)。因此，为了保持速度但保留使用公共服务器的选项，你可能需要在resolv.conf文件中重新保存本地DNS服务器，然后使用公共DNS服务器进行后续操作。操作系统按/etc/resolv.conf文件中列出的顺序查询每个DNS服务器，因此只有在本地DNS服务器中找不到域名时，系统才会引用公共DNS服务器。



*如果你正在使用 DHCP 地址和 DHCP 服务器提供一个 DNS 设置，则　DHCP 服务器将在更新DHCP地址时替换文件的内容。*

**NOTE**

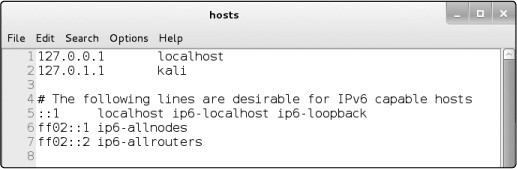
#### *映射您自己的 IP 地址*

在你的操作系统中一个被称为hosts的特殊文件总是执行域名——IP地址转换。这个hosts文件位于/etc/hosts，与DNS有点类似，你可以使用它来指定你自己的IP地址——域名映射。换句话说，当你在浏览器输入www.microsoft.com（或者其他任何域名）时，你可以决定浏览器将访问哪个IP地址而不是让DNS服务决定。对于黑客，这对于劫持局域网上的TCP连接以使用dnsspoof等工具将流量定向到恶意Web服务器非常有用。

在命令行中，输入以下命令 (你可以将首选文本编辑器替换为Leafpad):

kali >leafpad /etc/hosts

你应该看到你的hosts文件，如图3-3所示



*图 3­3: 默认 Kali Linux hosts 文件*

默认情况下，hosts文件只包含localhost的映射(127.0.0.1)和你的系统主机名(本例中为Kali, 位于127.0.0.1)。但是你可以按照你的意愿添加任何IP地址映射到任何域名。举个如何使用它的例子，你可以将www.bankofamerica.com映射到你的本地网站，地址为192.168.181.131。

127.0.0.1 localhost

127.0.1.1 kali

192.168.181.131 bankofamerica.com

# The following lines are desirable for IPv6 capable hosts

::1 localhost ip6­localhost ip6­loopback ff02::1 ip6­allnodes

ff02::2 ip6­allrouters

在IP地址和域名中间请确保你输入的是TAB键，而不是空格键。

随着您越来越多地参与黑客攻击工作并了解像dnsspoof和Ettercap这样的工具，您将能够使用hosts文件将访问www.bankofamerica.com的局域网上的任何流量定向到您的Web服务器192.168.181.131。

这些实际上都非常简单，对吧？

### 总结

任何黑客都需要一些基本的Linux网络技能来连接、分析和管理网络。随着你的进步，这些技能在侦察、欺骗和连接目标系统中将变得越来越有用。

**练习**

在继续第4章之前，通过完成以下练习，精进从本章学到的技能：

1.查找有关主动网络接口的信息。

2.将eth0上的IP地址更改为192.168.1.1。

3.在eth0上更改硬件地址。

4.检查是否有任何可用的无线接口处于活动状态。

5.将IP地址重置为DHCP分配的地址。

6.找到您喜欢的网站的名称服务器和电子邮件服务器。

7.将Google的DNS服务器添加到/etc/resolv.conf文件中，以便系统在无法使用本地DNS服务器解析域名查询时引用该服务器。

## 4

## ADDING AND REMOVING SOFTWARE

**添加和删除软件**



Linux或任何操作系统中最基本的任务之一便是添加和删除软件。您经常需要安装发行版中没有附带的软件，或者删除不需要的软件，这样就不会占用硬盘空间。

有些软件安装需要依赖其他软件才能运行，有时您会发现您可以在软件包安装过程中一次性下载所需的所有软件，软件包是一组文件(通常是库和其他依赖项)，您需要这些文件才能使软件成功运行。当您安装一个包时，包中的所有文件连同一个脚本一起安装，以简化软件的加载。

在本章中，我们将研究添加新软件的三个关键方法:apt包管理器、基于gui的安装管理器和git。

### 使用APT处理软件

在基于debian的Linux发行版(包括Kali和Ubuntu)中，默认的软件包管理器是高级打包工具apt，其主要命令是apt-get。在最简单和最常见的形式中，您可以使用apt-get下载和安装新的软件包，但也可以使用它更新和升级软件。

#### *搜索软件包*

在下载软件包之前，您可以检查所需的软件包是否在存储库中可用，存储库是操作系统存储信息的地方。apt工具有一个搜索功能，可以检查包是否可用。语法很简单:

apt­cache search keyword

注意，我们使用apt-cache命令搜索apt缓存，或者它存储软件包名的位置。例如，如果您正在搜索入侵检测系统Snort，您将输入图表 4-1所示的命令。

kali >apt-cache search snort

fwsnort ­ Snort­to­iptables rule translator

ippl ­ IP protocols logger

- snip -

snort ­ flexible Network Intrusion Detection System

snort­common ­ flexible Network Intrusion Detection System ­ common files

- snip -

*清单4-1:使用apt-cache在系统中搜索Snort*

如您所见，许多文件中都有**snort**关键字，但是在输出的中间我们看到*snort - flexible Network Intrusion Detection System*。这就是我们要找的!

#### *添加软件*

现在您已经知道snort包存在于存储库中，可以使用apt-get下载软件。

要在终端中从操作系统的默认存储库中安装软件，请使用apt-get命令，后面是关键字install，然后是要安装的包的名称。语法是这样的:

apt­get install packagename

让我们通过在系统上安装Snort来尝试一下。输入apt-get install snort作为命令语句，如清单4-2所示。

kali >apt-get install snort

Reading package lists... Done

Building dependency tree

Reading state information... Done

Suggested packages:

snort­doc

The following NEW packages will be installed: snort

­­snip­­

Install these packages without verification [Y/n]?

*清单4-2:使用apt-get安装安装Snort*

您看到的输出结果告诉您正在安装什么。如果一切正常，在出现提示时输入**y**，您的软件安装将继续。

#### *删除软件*

在删除软件时，使用带有remove选项的apt-get，后面跟着要删除的软件的名称(参见清单4-3)。

kali >apt-get remove snort

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following packages were automatically installed and are no longer

required:

libdaq0 libprelude2 oinkmaster snort­common­libraries snort­rules­default

­­snip­­

Do you want to continue [Y/n]?

*清单4-3:使用apt-get remove删除Snort*

同样，您将看到实时完成的任务，并将询问您是否希望继续。您可以输入**Y**来卸载，但是您可能希望继续使用Snort，因为我们将再次使用它。remove命令不会删除配置文件，这意味着您可以在将来重新安装相同的包，而无需重新配置。如果您确实希望在删除包的同时删除配置文件，可以使用清除选项，如清单4-4所示。

kali >apt-get purge snort

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following packages were automatically installed and are no longer required: libdaq0 libprelude2 oinkmaster snort­common­libraries snort­rules­default

­­snip­­

Do you want to continue [Y/n]?

*清单4-4:使用apt-get清除删除Snort和附带的配置文件*

只需在提示符处输入**Y**，继续清除软件包和配置文件。

您可能已经注意到，在输出中显示有提示：The following packages were automatically installed and are no longer required 。为了保持事物的小型和模块化，许多Linux包被分解成许多不同程序可能使用的软件单元。在安装Snort时，您安装了Snort运行所需的几个依赖项或库。现在您正在删除Snort，不再需要其他库或依赖项，因此也删除了它们。

#### *更新软件*

软件库将定期使用新软件或现有软件的新版本进行更新。这些更新不会自动进行，因此您必须手动请求它们，以便将这些更新应用到您自己的系统中。更新（update）与升级（upgrade）不同：更新只是更新可从存储库下载的包列表，而升级将把包升级到存储库中的最新版本。

您可以通过输入apt-get命令和关键字**update**来更新您的系统。这将搜索系统上的所有包并检查是否有更新。如果是，则下载更新(请参见清单4-5)。

kali >apt-get update

Get:1 http://mirrors.ocf.berkeley.edu/kali kali­rolling InRelease [30.5kb] Get:2 http://mirrors.ocf.berkeley.edu/kali kali­rolling/main amd64 Packages

[14.9MB]

Get:3 http://mirrors.ocf.berkeley.edu/kali kali­rolling non­free amd64 Packages [163kb]

Get:4 http://mirrors.ocf.berkeley.edu/kali kali­rolling/contrib amd64 Packages [107 kB]

Fetched 15.2 MB in 1min 4s (236 kB/s) Reading package lists... Done

*清单4-5:使用apt-get更新更新所有过时的包*

系统存储库中可用软件的列表将被更新。如果更新成功，您的终端将声明 Reading package lists... Done，如清单4-5所示。注意，存储库的名称和值(时间、大小等等)在您的系统上可能是不同的。

#### *升级软件*

要升级系统上的现有软件包，请使用apt-get升级。因为升级包可能会更改软件，所以必须以root用户身份登录，或者在输入apt-get升级之前使用**sudo**命令。这个命令将升级apt列表存在的系统上的每个软件包，这意味着只升级存储在存储库中的包(参见清单4-6)。升级可能很耗时，因此您可能暂时无法使用您的系统。

kali >apt-get upgrade

Reading package lists... Done

Building dependency tree... Done

Calculating upgrade... Done

The following packages were automatically installed and no longer required:

­­snip­­

The following packages will be upgraded:

­­snip­­

1101 upgraded, 0 newly installed, 0 to remove and 318 not upgraded. Need to get 827 MB of archives.

After this operation, 408 MB disk space will be freed.

Do you want to continue? [Y/n]

*清单4-6:使用apt-get升级升级所有过时的包*

您应该在输出中看到系统估计软件包所需的硬盘空间。如果您想继续，并且有足够的硬盘空间进行升级，请输入**Y**。

### 添加软件仓库到SOURCES.LIST文件

为Linux的特定发行版保存软件的服务器称为存储库。几乎每个发行版都有自己的软件存储库(为该发行版开发和配置的)，这些存储库可能不能很好地工作，或者根本不能与其他发行版一起工作。尽管这些存储库通常包含相同或类似的软件，但它们并不相同，有时它们具有相同软件的不同版本或完全不同的软件。

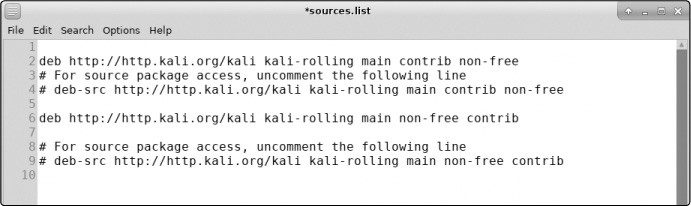
当然，您将使用Kali存储库，它有大量的安全和黑客软件。但由于Kali专门从事安全和黑客攻击，它不包括一些特殊的软件和工具，甚至一些普通的软件。如果系统没有在Kali软件存储库中找到特定的软件，那么值得添加一两个备份存储库供系统搜索。

您的系统将搜索的软件存储库存储在*sources.list*文件中。您可以更改此文件，以定义要从哪个存储库下载软件。我经常在*sources.list*中的Kali存储库之后添加Ubuntu存储库。这样，当我请求下载一个新的软件包时，我的系统将首先查看Kali存储库，如果没有软件包，它将查看Ubuntu存储库。

你可以找到*sources.list*文件在/etc/apt/*sources.list*。使用任何文本编辑器列出并打开它。我还是用Leafpad打开此文件。*sources.list*文件在终端中输入以下内容，用你自己使用的编辑器名称替换leafpad:

kali >leafpad /etc/apt/sources.list

输入此命令后，您应该会看到一个类似于Kali默认存储库列表中的窗口。



*图4-1:source .list中Kali的默认存储库*

许多Linux发行版将存储库划分为不同的类别。例如，Ubuntu将其存储库分类如下:

**main**包含受支持的开源软件

**universe**包含社区维护的开源软件

**multiverse**包含受版权或其他法律问题限制的软件

**restricted** 包含专有设备驱动程序

**backports**包含来自后续版本的包

我不建议在*sources.list*中使用测试、实验性或不稳定的存储库。因为他们可以下载有问题的软件到你的系统。没有经过全面测试的软件可能会破坏您的系统。

当您要求下载一个新的软件包时，系统会按顺序查看*sources.list*中列出的存储库。并在找到所需的包时停止，首先检查存储库是否与您的系统兼容。和Ubuntu一样，Kali也是在Debian上构建的，所以这些存储库在每个系统上都能很好地工作。

要添加存储库，只需编辑*sources.list*。打开文件通过向列表中添加存储库的名称，然后保存该文件。例如，您想在Kali上安装Oracle Java 8。默认的Kali源代码中没有适用于Oracle Java 8的apt包，但是在线快速搜索显示WebUpd8的优秀人员已经创建了一个。如果您将它们的存储库添加到*sources.list*中，那么您可以使用apt-get install oracle-java8-installer安装程序命令来安装Oracle Java 8。在编写本文时，您需要将以下存储库位置添加到*sources.list*中，以便添加必要的存储库:

deb http://ppa.launchpad.net/webupd8team/java/ubuntu trusty main

deb­src http://ppa.launchpad.net/webupd8team/java/ubuntu precise main

### 使用基于Gui的安装程序

Kali的新版本不再包含基于gui的软件安装工具，但是您可以使用apt-get命令来安装它。最常见的两种基于gui的安装工具是Synaptic和Gdebi。让我们安装Synaptic并使用它来安装Snort包:

kali >apt-get install synaptic

Reading package lists... Done

Building dependency tree

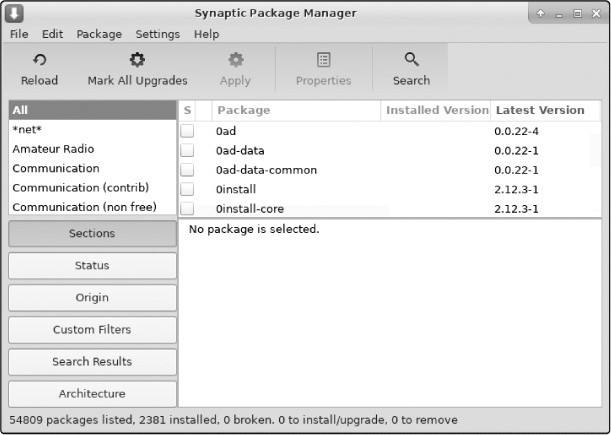
Reading state information... Done

­­snip­­

Processing triggers for menu (2.1.47)...

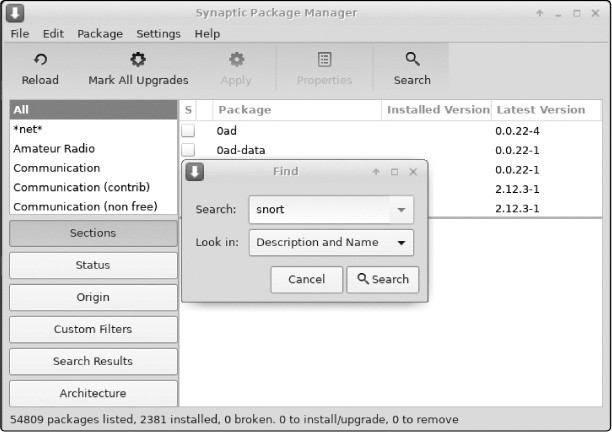
kali >

一旦你安装了synaptic,你可以从设置▸新立得软件包管理器（Settings ▸ Synaptic Package Manager）,应该打开窗口如图4­2。



*图4-2:Synaptic包管理器接口*

现在您可以搜索您正在寻找的包，只需单击Search选项卡打开一个搜索窗口。因为您再次寻找Snort，所以在搜索窗口中输入Snort并单击search。向下滚动搜索结果以找到您要查找的包。选中snort旁边的复选框，然后单击Apply选项卡，如图4-3所示。Synaptic现在将从存储库下载并安装Snort以及任何必要的依赖项。



*图4-3:从Synaptic包管理器下载Snort*

### 使用GIT安装软件

有时，您想要的软件在任何存储库中都不可用——尤其是在它是全新的情况下——但是它可能在github (https://www.github.com/)上可用，这个站点允许开发人员与其他人共享他们的软件，以便下载、使用和提供反馈。例如，如果您想要蓝牙攻击和渗透套件bluediving，但是在Kali存储库中找不到它，那么您可以通过在浏览器搜索栏中输入*bluediving*来搜索。如果它存在于github上，您应该在搜索结果中看到它的存储库。

在github上找到软件后，可以通过输入git clone命令及其github URL从终端安装软件。例如，bluediving位于https://www.github.com/balle/bluediving.git。要将其克隆到您的系统中，请输入清单4-7所示的命令。

kali >git clone https://[www.github.com/balle/bluediving.git](http://www.github.com/balle/bluediving.git)

Cloning into 'bluediving'...

remote: Counting objects: 131, Done.

remote: Total 131 (delta 0), reused 0 (delta 0), pack­reused 131 Receiving objects: 100% (131/131), 900.81 KiB | 646.00 KiB/s, Done.

Resolving deltas: 100% (9/9), Done.

Checking connectivity... Done.

*清单4-7:使用git* *clone 克隆bluediving*

git clone命令将所有数据和文件从该位置复制到您的系统中。您可以使用目标目录上的长列表命令ls -l检查它们是否已成功下载，如下所示:

kali >ls -l

如果您已经成功地将bluediving克隆到您的系统中，您应该会看到以下输出:

total 80

drwxr­xr­x 7 root root 4096 Jan 10 22:19 bluediving

drwxr­xr­x 2 root root 4096 Dec 5 11:17 Desktop

drwxr­xr­x 2 root root 4096 Dec 5 11:17 Documents

drwxr­xr­x 2 root root 4096 Dec 5 11:17 Downloads

drwxr­xr­x 2 root root 4096 Dec 5 11:17 Music

­­snip­­

如您所见，bluediving已成功地克隆到系统中，并为其文件创建了一个名为bluediving的新目录。

### 总结

在本章中，您学习了许多在Linux系统上下载和安装新软件的方法。软件包管理器(如apt)、基于gui的安装程序和git clone是有抱负的黑客需要知道的最常见和最关键的方法。你很快就会发现自己对它们都很熟悉了。

**练习**

在继续学习第5章之前，通过完成以下练习来尝试复习你从本章中学到的技能:

1.从Kali存储库安装一个新的软件包。

2.删除相同的软件包。

3.更新存储库。

4.升级软件包。

## 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**



在Linux术语中，服务是在后台运行的应用程序，等待您使用它。您的Linux系统预装了许多服务。其中最著名的是无处不在的Apache Web Server，它用于创建，管理和部署Web服务器，还有更多。出于本章关于服务的目的，我只选择了对黑客特别重要的四个：Apache Web Server，OpenSSH，MySQL和PostgreSQL。

在本章中，您将学习如何使用Apache设置web服务器、使用OpenSSH进行物理监视、使用MySQL访问数据以及使用PostgreSQL存储黑客信息。

### 启动、停止和重新启动服务

在开始使用这四个关键的服务之前，让我们先研究一下如何在Linux中启动、停止和重新启动服务。

有些服务可以通过Kali Linux中的GUI停止和启动，就像在Windows或Mac这样的操作系统上一样。下面是管理服务的基本语法:

service servicename start|stop|restart

要启动**apache2**服务（Web服务器或HTTP服务），请输入以下内容：

kali >service apache2 start

要停止Apache Web服务器，请输入：

kali >service apache2 stop

通常，当您通过更改其纯文本配置文件对应用程序或服务进行配置更改时，需要重新启动该服务以捕获新配置。因此，您可以输入以下内容：

kali >service apache2 restart

既然您已经了解了如何从命令行启动，停止和重新启动服务，那么让我们继续讨论针对黑客的四个最关键的Linux服务。

### 使用APACHE Web服务器创建HTTP Web服务器

Apache Web Server可能是Linux系统上最常用的服务。Apache在全球60％以上的Web服务器上都可以找到，因此任何自重的Linux管理员都应该熟悉它。作为一个渴望破解网站的黑客，了解Apache，网站和这些网站的后端数据库的内部工作方式至关重要。您还可以使用Apache设置自己的Web服务器，您可以通过网站脚本（XSS）向访问您网站的任何人提供恶意软件，或者您可以通过滥用域名克隆网站并将流量重定向到您的网站名称系统（DNS）。 在任何一种情况下，都需要Apache的基本知识。

#### *从Apache开始*

如果您的系统上运行了Kali，则已安装Apache。许多其他Linux发行版也默认安装它。如果您没有安装Apache，可以通过输入以下命令从存储库下载并安装它：

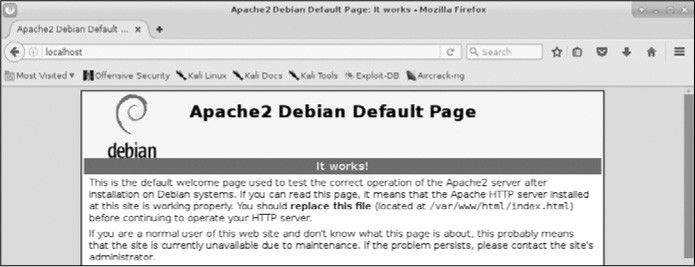
kali >apt-get install apache2

Apache Web Server通常与MySQL数据库相关联（我们将在下一节中讨论），这两种服务通常与脚本语言（如Perl或PHP）配对以开发Web应用程序。Linux，Apache，MySQL和PHP或Perl的这种组合形成了一个强大而强大的平台，用于开发和部署基于Web的应用程序，统称为LAMP。这些是用于在Linux世界中开发网站的最广泛使用的工具 - 它们在微软世界中也很受欢迎，它们通常被称为WAMP，W代表Windows。

当然，第一步是启动我们的Apache守护进程。在Kali中，转到应用程序▸服务▸HTTPD（Applications ▸ Services ▸ HTTPD）并单击Apache start。您可以通过输入以下命令从命令行完成相同的操作：

kali >services apache2 start

现在Apache正在运行，它应该能够提供其默认网页。 在您喜欢的Web浏览器中输入http:// localhost /以显示网页，该网页应类似于图12-1。

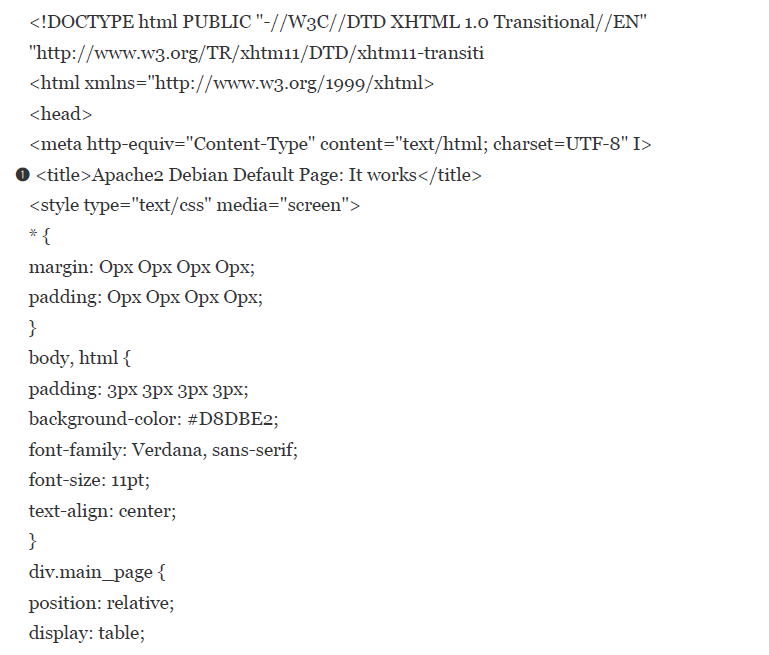


*图12­1: Apache2 Web Server 默认页*

如您所见，Apache将“**It works**”显示为其默认网页。现在你知道你的Apache Web服务器正在运行，让我们来自定义它吧！

#### *编辑index.html文件*

Apache的默认网页位于/var/www/html/index.html。您可以编辑index.html文件以提供您想要的任何信息，所以让我们创建自己的信息。为此，您可以使用任何文本编辑器，我将使用Leafpad打开/var/www/html/index.html，你会看到类似于列表12-1的信息。



*列表12­1: Apache Web Server 的index.html页面*

请注意，默认网页是我们将浏览器打开到localhost时显示的文本，默认格式为➊。我们需要做的就是编辑或替换此文件，让我们的Web服务器显示我们想要的信息。

#### *添加HTML*

现在我们已启动并运行Web服务器并打开index.html文件，我们可以添加我们希望Web服务器提供的任何文本。我们将创建一些简单的HTML模块。

我们来创建这个页面。在文本编辑器的新文件中，输入列表12-2中显示的代码。

<html>

<body>

<h1>Hackers­Arise Is the Best! </h1>

<p> If you want to learn hacking, Hackers­Arise.com </p>

<p> is the best place to learn hacking!</p>

</body>

</html>

*列表12­2:一些简单的HTML添加到index.html*

完全按照清单12-2中的内容输入文本后，将此文件另存为/var/www/html/index.html并关闭文本编辑器。 然后，您的文本编辑器将提示您该文件已存在，没关系，只需覆盖现有的/var/www/html/index.html文件即可。

#### *看会发生什么*

保存了我们的/var/www/html/index.html文件后，我们可以查看Apache将提供的服务。再次浏览浏览器到http:// localhost，您应该会看到类似于图12-2的内容。



*图12-2：新的HackersArise网站*

Apache就像我们创建它一样提供了我们的网页！

### OPENSSH和树莓派

SSH是Secure Shell的首字母缩写，它基本上使我们能够安全地连接到远程系统上的终端 - 这是多年前常见的不安全telnet的替代品。当我们构建Web服务器时，SSH使我们能够创建访问列表（可以使用此服务的用户列表），使用加密密码对用户进行身份验证，以及加密所有通信。这减少了不需要的用户使用远程终端的机会（由于添加的认证过程）或拦截我们的通信（由于加密）。可能最广泛使用的Linux SSH服务是OpenSSH，它几乎安装在所有Linux发行版上，包括Kali。

系统管理员经常使用SSH来管理远程系统，而黑客经常使用SSH连接到受感染的远程系统，所以我们在这里也会这样做。在这个例子中，我们使用SSH设置一个远程Raspberry Pi系统进行间谍活动，我称之为“Raspberry Spy Pi”。为此，你需要一个Raspberry Pi和随之而来的Raspberry Pi相机模块。

不过，在我们这样做之前，使用现在熟悉的命令在您的Kali系统上启动OpenSSH：

kali >service ssh start

我们将使用SSH来构建和控制远程间谍Raspberry Pi。如果您还不熟悉它，Raspberry Pi是一款小巧但功能强大的信用卡大小的计算机，可作为远程监视工具使用。我们将使用带有相机模块的Raspberry Pi作为远程间谍设备。您可以以低于50美元的价格购买几乎所有电子产品零售商（包括亚马逊）的Raspberry Pi，您可以以15美元的价格购买相机模块。

在这里，我们将在与Kali系统相同的网络上使用Raspberry Spy Pi，这允许我们使用私有的内部IP地址。当然，在现实世界中进行黑客攻击时，您可能希望将其设置在另一个远程网络上，但这将难以触及本书的范围。

#### *设置Raspberry Pi*

确保您的Raspberry Pi正在运行Raspbian操作系统，这只是另一个专门为Raspberry Pi CPU移植的Linux发行版。您可以在https://www.raspberrypi.org/downloads/raspbian/找到Raspbian的下载和安装说明。您在本书中学到的几乎所有内容都适用于Raspberry Pi上的Raspbian OS以及Kali，Ubuntu和其他Linux发行版。

下载并安装Raspbian操作系统后，您需要将Raspberry Pi连接到显示器，鼠标和键盘，然后将其连接到互联网。如果这对您来说是全新的，请查看https://www.raspberrypi.org/learning/hardwareguide/上的说明。 设置好所有内容后，使用用户名pi和密码raspberry登录。

#### *构建Raspberry Spy Pi*

第一步是确保在Raspberry Spy Pi上运行并启用SSH。默认情况下，SSH通常是关闭的，因此要启用它，请转到“首选项”菜单并启动Raspberry Pi配置。然后转到**Interfaces**选项卡，在**SSH**旁边，单击**Enabled**（如果尚未选中），然后单击**OK**。

启用SSH后，您可以通过打开终端并输入以下内容在Raspberry Spy Pi上启动它：

kali >service ssh start

接下来，您需要连接相机模块。如果你使用的是Raspberry Pi版本3的板，那么只有一个地方可以连接它。关闭Pi，将模块连接到相机端口，然后重新打开。请注意，相机非常脆弱，绝不能与通用输入/输出（GPIO）引脚接触，否则，它可能会短路并烧坏。

现在，在SSH服务启动并运行的情况下，将Raspberry Spy Pi放置在您家，学校或您想要监视的其他位置的某个位置。当然，它必须通过以太网电缆或理想情况下通过WiFi连接到局域网。（新的Raspberry Pi 3和Raspberry Pi Zero都内置了WiFi。）

现在，您需要获取Raspberry Pi的IP地址。正如您在第3章中学到的，您可以使用**ifconfig**获取Linux设备的IP地址：

pi >ifconfig

我的Pi的IP地址是**192.168.1.101**，但请确保您使用的是Raspberry Spy Pi的IP地址，无论我的地址出现在本章的哪个位置。现在，从您的Kali系统，您应该能够直接连接并控制您的Raspberry Spy Pi并将其用作远程间谍系统。在这个简单的示例中，您的系统需要与Pi在同一网络上。

要从Kali系统通过SSH连接到远程Raspberry Spy Pi，请输入以下内容，记住使用您自己的Pi的IP地址：

kali >ssh pi@192.168.1.101

pi@192.168.1.101's password:

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, the extent permitted by applicable law

last login: Tues Jan. 1 12:01:01 2018

pi@raspberyypi:: $

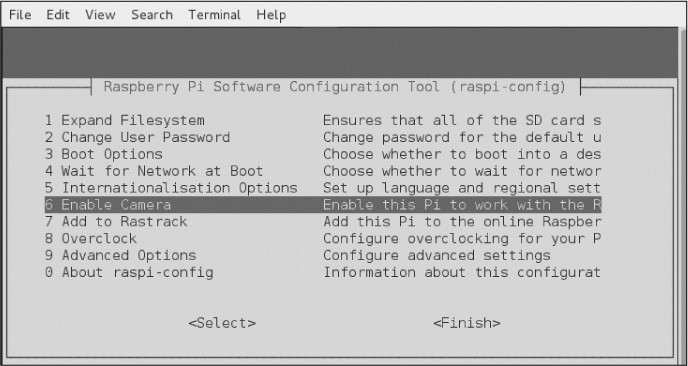
Spy Pi会提示您输入密码。在这种情况下，默认密码是**raspberry**，除非您已更改它。

#### *配置相机*

接下来，我们需要配置相机。为此，请输入以下命令启动Raspberry Pi配置工具：

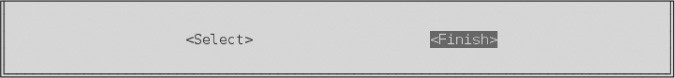
pi >sudo raspi-config

这应该启动一个图形菜单，如图12-3所示。



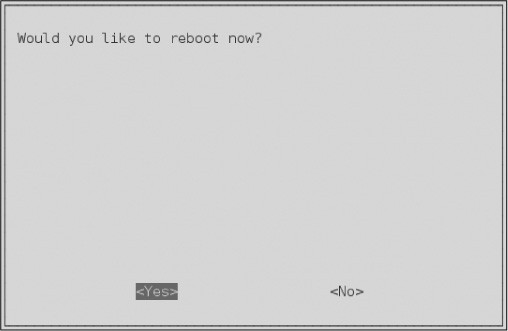
*图123：Raspberry Pi配置工具*

向下滚动至6启用相机（**Enable Camera**），然后按ENTER。现在，滚动到此菜单的底部并选择**Finish**并按**ENTER**，如图12-4所示。



*图12-4：完成配置*

当配置工具询问您是否要重新启动时，如图12-5所示，选择**Yes**，然后再次按**ENTER**。



*图12-5：重新启动Pi以启用更改。*

现在你的Raspberry Spy Pi相机应该启用并准备好进行间谍活动了！

#### *启动Spy*

一旦您的Raspberry Spy Pi重新启动并且您已经从Kali终端通过SSH登录，您就可以开始使用它来拍摄静态照片了。

Raspbian操作系统有一个名为raspistill的应用程序，我们将用它来从我们的小Raspberry Spy Pi中拍照。 在终端中输入**raspistill**以查看工具的帮助屏幕及其所有选项：

pi@raspberrypi: raspistill

raspistill Camera App v1.3.8

Runs camera for specific time, and takes JPG capture at end if requested

usage: raspistill [options] Image parameter commands

­­snip­­

现在让我们使用Raspberry Spy Pi拍摄一些远程的间谍照片吧！**raspistill**命令有很多你应该探索的选项，但在这里我们只使用默认值。要拍摄照片并将其另存为JPEG，请输入以下内容：

pi@raspberrypi: raspistill -v -o firstpicture.jpg

raspistill Camera App v1.3.8

width 2592, Height 1944, quality 85, filename firstpicture.jpg Time delay 5000, Raw no

­­snip­­

我们使用**-v**选项给我们详细的输出和**-o**选项告诉raspistill我们将要给它一个文件名，然后我们给出文件名。当我们在Raspberry Spy Pi上使用长列表格式列出文件时，我们可以看到文件**firstpicture.jpg**，如下所示：

pi@raspberrypi: ls -l

total 2452

drwxr­xr­x 2 pi pi 4096 Mar 18 2019 Desktop

drwxr­xr­x 2 pi pi 4096 Mar 18 2019 Documents

drwxr­xr­x 2 pi pi 4096 Mar 18 2019 Downloads

­rw­r­­r­­ 1 pi pi 2472219 Mar 18 2019 firstpicture.jpg

drwxr­xr­x 2 pi pi 4096 Mar 18 2019 Music

drwxr­xr­x 2 pi pi 4096 Mar 18 2019 Pictures

­­snip­­

我们使用SSH在我们的远程Raspberry Spy Pi上拍摄了我们的第一张谍照！ 随意进一步探索这种多功能武器。

### 从MYSQL中提取信息

MySQL是数据库驱动Web应用程序背后使用最广泛的数据库。在我们现代的Web 2.0技术时代，几乎每个网站都是数据库驱动的，这意味着MySQL拥有大部分网络的数据。

数据库是黑客的“金羊毛”。它们包含有关用户的重要信息以及信用卡号等机密信息。出于这个原因，黑客通常以数据库为目标。

与Linux一样，MySQL是开源和通用公共许可（GPL），你会发现它几乎预装在每个Linux发行版上。

作为免费，开源和强大的MySQL，MySQL已成为许多Web应用程序的首选数据库，包括WordPress，Facebook，LinkedIn，Twitter，Kayak，almart.com，Wikipedia和YouTube等热门网站。

其他流行的内容管理系统（CMS），如Joomla，Drupal和Ruby on Rails也都使用MySQL。你明白了，如果您想开发或攻击Web应用程序的后端数据库，您应该了解MySQL。让我们开始吧。

#### *启动MySQL*

幸运的是，Kali已经安装了MySQL（如果您正在使用其他发行版，则可以从软件镜像库或直接从https：//www.mysql.com/downloads/下载并安装MySQL）。

要启动MySQL服务，请在终端中输入以下内容：

kali >service mysql start

接下来，您需要通过登录进行身份验证。输入以下内容，并在提示输入密码时，只需按**ENTER**键：

kali >mysql -u root -p

Enter password:

Welcome to MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 4

Server version: 5.6.30­1 (Debian)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement

mysql >

在MySQL的默认配置中，**root**用户的密码为空。显然，这是一个主要的安全漏洞，您应该在首次登录后添加密码来解决此问题。请注意，操作系统和MySQL的用户名和密码是独立且不同的。我们现在更改MySQL root用户的密码以确保安全。

**MYSQL的过去和未来**

MySQL最初由瑞典的MySQL AB于1995年开发，然后在2008年被Sun Microsystems收购，而后者又于2009年被Oracle收购 - 因此MySQL现在归Oracle所有。甲骨文是世界上最大的数据库软件发行商，因此开源社区对甲骨文保持MySQL开源的承诺存在重大挑战。因此，现在有一个名为“Maria”的MySQL数据库软件的分支，致力于保持该软件及其后续版本的开源。作为Linux管理员或黑客，你应该关注MariaDB。

#### *与MySQL交互*

SQL是一种用于与数据库连接的解释型编程语言。数据库通常是关系数据库，这意味着数据存储在多个交互的表中，每个表都有一个或多个列和行中的值。

SQL有几种实现，每种都有自己的命令和语法，但这里有几个常用的命令：

**select**用于检索查找数据

**union**用于组合两个或多个select操作的结果

**insert**用于插入添加新数据

**update**用于修改更新现有数据

**delete**用于删除数据

您可以为每个命令提供条件，以便更具体地了解您要执行的操作。 例如，如下行

select user,password from customers where user='admin';

将返回customers表中用户值等于“admin”的任何用户的用户名和密码字段的值。

#### *设置MySQL密码*

通过输入以下内容，让我们看看已经在我们的MySQL系统中的用户。（请注意，MySQL中的命令以分号结束。）

mysql >select user,host,password from mysql.user;

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­

| user | host | password

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­

|root |localhost |

|root |aphrodite.kali.org |

|root |127.0.0.1 |

­­snip­­

这表明root用户没有设置密码。我们给root分配一个密码。为此，我们将首先选择要使用的数据库。 您系统上的MySQL将附带一些已设置的数据库。使用**show**列出所有数据库，命令查看所有可用的数据库：

mysql >show databases;

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

| Database |

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

| information\_schema |

| mysql |

| performance\_schema |

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

3 rows in set (0.23 sec)

MySQL默认带有三个数据库，其中两个（**information\_schema**和**performance\_schema**）是我们在这里不会使用的管理数据库。我们将使用非管理数据库mysql，它包含在您的目标数据库中。要开始使用mysql数据库，请输入：

mysql >use mysql;

Reading table information for completion of table and column names You can turn off this feature to get a quicker startup with ­A

Database changed

这个命令将我们连接到mysql。现在，我们可以使用以下命令将root用户的密码设置为**hackers-arise**：

mysql >update user set password = PASSWORD("hackers-arise") where user = 'root';

此命令将通过将用户的root密码设置为**hackers­ arise**来更新用户。

#### *访问远程数据库*

要访问localhost上的MySQL数据库，我们使用以下语法：

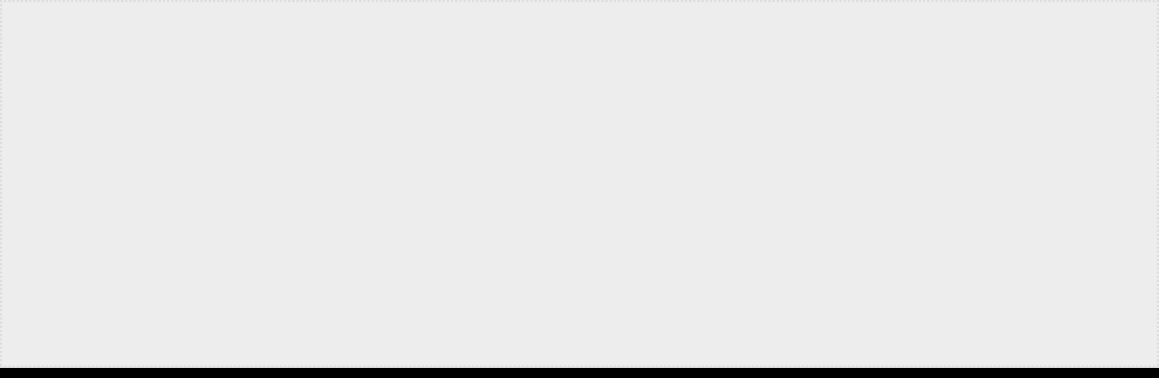
kali >mysql -u <username> -p

如果没有给出主机名或IP地址，则此命令默认使用localhost上的MySQL实例。因此，要访问远程数据库，我们需要提供托管MySQL数据库的系统的主机名或IP地址。以下这是一个例子：

kali >mysql -u root -p 192.168.1.101

这会将我们连接到192.168.1.101的MySQL实例并提示我们输入密码。出于演示目的，我将连接到局域网（LAN）上的MySQL实例。如果您在其他互联网网络上安装了MySQL系统，请在此处使用其IP地址。我假设您已设法绕过密码并以root身份登录系统（您已经知道默认情况下，mysql数据库没有密码）。

这打开了MySQL命令行界面，它为我们提供了**mysql>**提示符。除了这个命令行界面，MySQL还有GUI界面 - 原生（MySQL Workbench）和第三方（Navicat和TOAD for MySQL）。作为一名黑客，命令行界面可能是利用MySQL数据库的最佳机会，因此我们将重点关注这一点。作为未经授权的数据库参与者，您将不可能获得易于使用的 GUI。



此屏幕提醒我们所有命令必须以分号或\ g结尾（与Microsoft的SQL Server不同），并且我们可以通过输入help或\ h获得帮助。

**NOTE**

现在我们以系统管理员身份登录，我们可以畅通无阻地浏览数据库。如果我们以普通用户身份登录，则我们的导航将受到系统管理员为该用户提供的权限的限制。

#### *连接到数据库*

通过访问系统，我们想要一探究竟。我们的下一步是找出是否有值得访问的数据库。以下是查找所访问系统上的数据库的命令：

mysql >show databases;

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

| Database |

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

| information schema |

| mysql |

| creditcardnumbers |

| performance\_schema |

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

4 rows in set (0.26 sec)

啊哈！我们找到了一个值得探索的名字为**creditcardnumbers**的数据库。让我们尝试连接到它。

在MySQL中，与其他数据库管理系统（DBMS）一样，我们可以通过输入**use databasename** 连接到我们感兴趣的数据库。

mysql >use creditcardnumbers;

Database changed

数据库更改的响应表明我们现在已连接到**creditcardnumbers**数据库。

当然，不言而喻，数据库管理员不太可能如此容易地将数据库命名为信用卡号，因此您可能需要进行一些探索以找到感兴趣的数据库。

#### *数据库表*

我们现在已连接到**creditcardnumbers**数据库，可以进行一些探索以查看它可能包含的信息。数据库中的数据被组织成表格，每个表格可能包含一组不同的相关数据。我们可以通过输入以下命令找出此数据库中的表：

mysql >show tables;

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

| Tables\_in\_creditcardnumbers |

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

| cardnumbers |

+­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­+

1 row in set (0.14 sec)

在这里，我们可以看到该数据库中只有一个表，称为**cardnumbers**。通常，数据库中会有很多表，因此您可能需要进行更多的监听。在这个示例数据库中，我们很幸运能够将注意力集中在这个单独的表格中，以提取黑客的金羊毛！

既然我们想要检查一个表，我们需要了解该表的结构。一旦我们知道如何设置表，我们就可以提取相关信息。

您可以使用**describe**语句查看数据库的表的结构，如下所示：

mysql >describe cardnumbers;

+­­­­­­­­­­­­­­­+­­­­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­+

| Field | Type | Null | Key | Default | Extra |

+­­­­­­­­­­­­­­­+­­­­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­+

| customers | varchar(15) | YES | | NULL | |

| address | varchar(15) | YES | | NULL | |

| city | varchar(15) | YES | | NULL | |

| state | varchar(15) | YES | | NULL | |

| cc | int(12) | NO | | 0 | |

+­­­­­­­­­­­­­­­+­­­­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­+

MySQL使用我们感兴趣的表结构的关键信息进行响应。我们可以看到每个字段的名称以及它所拥有的数据类型（通常是文本类型varchar或整数类型int）。我们还可以看到它是否会接受NULL值，密钥（如果存在）（密钥链接表），字段可能具有的任何默认值，以及最后的任何额外信息，例如注释。

#### *查看数据*

要实际查看表中的数据，我们使用**SELECT**命令。 **SELECT**命令要求您知道以下信息：

* 包含要查看的数据的表
* 该表中包含要查看的数据的列

我们按以下格式列出：

SELECT columns FROM table

作为查看所有列数据的便捷快捷方式，我们可以使用星号作为通配符，而不是键入我们想要查看的每个列名。因此，要查看**cardnumbers**表中所有数据的转储，我们输入以下内容：

mysql >SELECT \* FROM cardnumbers;

+­­­­­­­­­­­+­­­­­­­­­­­­­­­+­­­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­­­­­­+

| customers | address | city | state | cc |

+­­­­­­­­­­­+­­­­­­­­­­­­­­­+­­­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­­­­­­+

| Jones | 1 Wall St | NY | NY | 12345678 |

| Sawyer | 12 Piccadilly | London | UK | 234567890 |

| Doe | 25 Front St | Los Angeles | CA | 4567898877 |

+­­­­­­­­­­­+­­­­­­­­­­­­­­­+­­­­­­­­­­­­­+­­­­­­­­­+­­­­­­­­­­­­­­+

如您所见，MySQL已将**cardnumbers**表中的所有信息显示在屏幕上。 我们找到了黑客的金羊毛！

#### *PostgreSQL与Metasploit*

**PostgreSQL**，或**Postgres**，是另一个开源关系数据库，由于其能够轻松扩展并处理繁重的工作负载，因此常用于非常大的互联网应用程序。它于1996年7月首次发布，由一大批名为PostgreSQL全球开发组的开发人员维护。

默认情况下，PostgreSQL也安装在Kali中，但是如果您使用的是另一个Linux发行版，它可能会在您的存储库中，您可以通过输入以下命令来安装它：

kali >apt-get postgres install

作为一名黑客，你会发现PostgreSQL特别重要，因为它是最广泛使用的渗透测试和攻击框架Metasploit的默认数据库。Metasploit使用PostgreSQL存储其模块，以及扫描和利用的结果，以便于在渗透测试或黑客攻击中使用。出于这个原因，我们将在Metasploit的上下文中使用PostgreSQL。

与Linux中的几乎所有服务一样，我们可以通过输入服务来启动PostgreSQL应用程序启动，如下：

kali >service postgresql start

随着PostgreSQL的启动和运行，让我们启动**Metasploit**：

kali >msfconsole

请注意，当Metasploit完成启动时，您将看到msf>提示符。

教您如何使用Metasploit进行黑客攻击和开发目的超出了本书的范围，但在这里我们将建立Metasploit将其信息存储在其中的数据库。

在Metasploit运行的情况下，我们可以使用以下命令设置PostgreSQL，以便它存储来自系统上任何Metasploit活动的数据：

msf >msfdb init

[\*] exec :msfdb init

Creating database use 'msf'

Enter password for new role

Enter it again:

Creating databases 'msf' and 'msf\_test'

Creating configuration file /usr/share/metasploit­framework/config/database.yml

Creating initial database schema

接下来，我们需要以root身份登录**Postgres**。在这里，我们在命令前加上**su**，即“switch user”命令，以获取root权限：

msf >su postgres

[\*] su postgres

postgres@kali:/root$

登录Postgres时，您会看到提示已更改为**postgres@kali:/root$**，表示应用程序，主机名和用户。

在下一步中，我们需要创建用户和密码，如下所示：

postgres@kali:/root$ createuser msf\_user -P

Enter Password for new role:

Enter it again:

我们使用带有**createuser**命令的**-P**选项创建用户名msf\_user。

然后输入所需的密码两次。接下来，您需要创建数据库并为msf\_user授予权限。将数据库命名为hackers\_arise\_db，如下所示：

postgres@kali:/root$ createdb - owner=msf\_user hackers\_arise\_db

postgres@kali:/root$ exit

当您使用exit命令退出Postgres时，终端将回退到msf>提示符。

接下来，我们必须通过定义以下内容将我们的Metasploit控制台msfconsole连接到PostgreSQL数据库：

* **user**
* **password**
* **host**
* **database name**

在我们的例子中，我们可以使用以下命令将msfconsole连接到我们的数据库：

msf >db\_connect msf\_user:password@127.0.0.1/hackers\_arise\_db

当然，您需要提供之前使用的密码。IP地址是本地系统（localhost）的IP地址，因此除非在远程系统上构建此数据库，否则可以使用127.0.0.1。

最后，我们可以检查PostgreSQL数据库的状态以确保它已连接：

msf >db\_status

[\*] postgresql connected to msf

如您所见，Metasploit响应返回PostgreSQL数据库已连接并可以使用。现在，当我们使用Metasploit进行系统扫描或运行漏洞时，结果将存储在PostgreSQL数据库中。此外，Metasploit现在将其模块存储在Postgres数据库中，使得搜索正确的模块变得更加容易和快捷！

### 总结

Linux有许多服务在后台运行，直到用户需要它们 Apache Web Server是使用最广泛的，但是黑客也应该熟悉MySQL，SSH和PostgreSQL来完成各种任务。在本章中，我们介绍了开始使用这些服务的绝对基础知识。一旦您对Linux系统感到满意，我建议您进一步探索这些服务。

**练习**

在继续学习第13章之前，通过完成以下练习来尝试你从这一章中学到的技能:

1.通过命令行启动**apache2**服务。

2.使用index.html文件，创建一个简单的网站，宣布您进入令人兴奋的黑客攻击世界。

3.通过命令行启动**SSH**服务。现在从LAN上的另一个系统连接到Kali系统。

4.启动MySQL数据库服务并将**root**用户密码更改为hackers-aris。切换到mysql数据库。

5.启动PostgreSQL数据库服务。按照本章所述进行设置，以供Metasploit使用。

## 13

**BECOMING SECURE AND ANONYMOUS**

**安全和匿名**



今天，几乎我们在互联网上做的一切都被跟踪。无论是谷歌跟踪我们的在线搜索、网站访问和电子邮件，还是美国国家安全局(NSA)对我们的所有活动进行编目，无论谁在跟踪我们，我们的每一次在线活动都会被记录、编入索引，然后被挖掘出来，以造福他人。普通个人，尤其是黑客，需要了解如何限制这种跟踪，并在网上保持相对匿名，以限制这种无处不在的监视。

在本章中，我们将介绍如何使用以下四种方法匿名(或尽可能接近)浏览万维网：

* The Onion Network
* 洋葱网络
* 代理服务器
* 虚拟专用网络
* 私有加密的电子邮件

没有一种方法能保证你的活动不被窥探，如果有足够的时间和资源，任何事情都能被追踪。然而，这些方法可能会使跟踪器的工作更加困难。

### 互联网是如何出卖我们的

首先，让我们从更高的层次来讨论我们在互联网上的活动是如何被跟踪的。我们不会讨论所有的跟踪方法，也不会过多地讨论任何一种方法的细节，因为这超出了本书的范围。事实上，这样的讨论可能会占用一整本书的篇幅。

首先，您的IP地址标识您在互联网上的身份。从您的机器发送的数据通常会被标记为您的IP地址，从而使您的活动易于跟踪。其次，谷歌和其他电子邮件服务将“阅读”您的电子邮件，寻找关键词，以更有效地为您服务广告。让我们先来看看IP地址是如何在互联网上泄露信息的。

当您通过互联网发送数据包时，它包含数据的源和目标的IP地址。通过这种方式，数据包知道它要去哪里以及在哪里返回响应。每个数据包通过多个互联网路由器跳转，直到找到它的目的地，然后跳转回发送方。对于一般的互联网冲浪，每一跳都是数据包通过路由器到达目的地。发送方和目的地之间可以有多达20-30跳，但通常任何数据包在不到15跳的时间内就能找到到达目的地的路径。

当数据包在互联网上传播时，任何截获数据包的人都可以看到是谁发送了数据包，它到过哪里，它要去哪里。这是网站可以告诉您到达目的地并自动登录的一种方式，也是有人可以跟踪您在互联网上的位置的方式。

要查看数据包在您和目的地之间的跳转情况，可以使用traceroute命令，如下所示。只需输入traceroute和目标IP地址或域，该命令将向目标发送数据包并跟踪这些数据包的路由。

kali >traceroute google.com

traceroute to google.com (172.217.1.78), 30 hops max, 60 bytes packets

1 192.168.1.1 (192.168.1.1) 4.152 ms 3.834 ms 32.964 ms

2 10.0.0.1 (10.0.0.1) 5.797 ms 6.995 ms 7.679 ms

3 96.120.96.45 (96.120.96.45) 27.952 ms 30.377 ms 32.964 ms

­­snip­­

18 lgal15s44­in­f14.le100.net (172.217.1.78) 94.666 ms 42.990 ms 41.564 ms

如你所见，ww.google.com与我的互联网距离是18跳。您的结果可能会不同，因为您的请求来自不同的位置，而且谷歌在全球有许多服务器。此外，数据包在互联网上并不总是采用相同的路由，因此您可能会将另一个信息包从您的地址发送到相同的站点，并接收不同的路由。让我们看看如何用Tor网络来掩饰这一切。

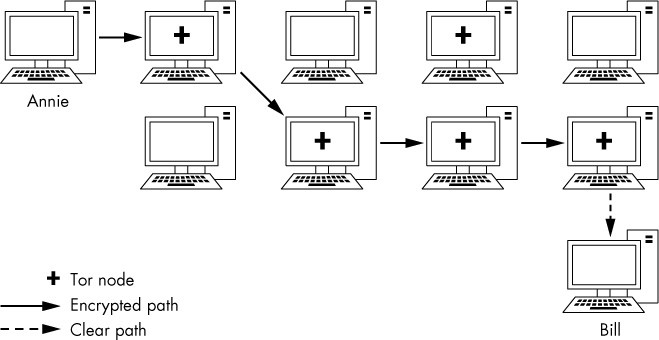
### 洋葱路由系统

上世纪90年代，美国海军研究办公室(ONR)着手开发一种匿名浏览互联网进行间谍活动的方法。该计划是建立一个路由器网络，它与互联网的路由器是分开的，可以加密流量，并且只存储前一个路由器的未加密IP地址-这意味着一路上所有其他路由器地址都加密了。他们的想法是，任何观察流量的人都无法确定数据的来源或目的地。

这项研究在2002年被称为“洋葱路由器(Tor)项目”，现在任何人都可以使用它在web上进行相对安全且匿名的导航。

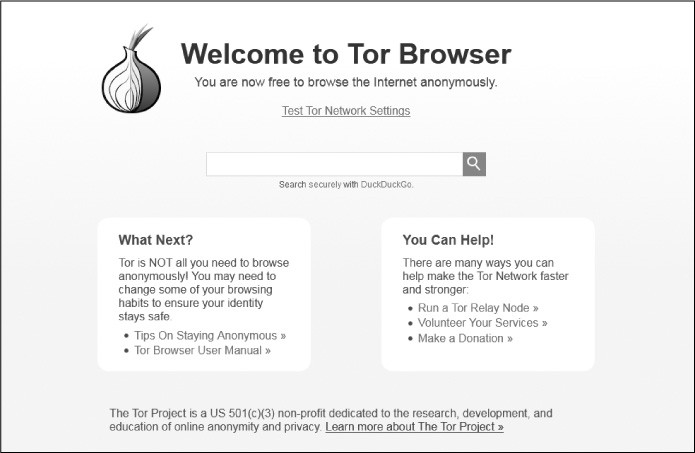
#### *Tor是如何工作的*

通过Tor发送的数据包不是通过常规路由器发送的，而是通过全世界7000多台路由器组成的网络发送的，这要感谢志愿者们允许Tor使用他们的计算机。在使用完全独立的路由器网络的基础上，Tor加密每个数据包的数据、目的地和发送方IP地址。在每一跳，接收到的信息被加密，然后在下一跳被解密。这样，每个包只包含关于路径上的前一跳的信息，而不包含源的IP地址。如果有人拦截流量，他们只能看到上一跳的IP地址，网站所有者只能看到发送流量的最后一个路由器的IP地址(参见图13-1)，这确保在互联网上的相对匿名性。



*图13-1：Tor如何使用加密流量数据*

要启用Tor，只需从https://www.torproject.org/安装Tor浏览器。一旦安装完毕，它将如图13 -2所示，您可以像使用任何老式互联网浏览器一样使用它。通过使用这个浏览器，您将通过一组单独的路由器来浏览互联网，并且能够在不被“老大哥”（隐喻某超级大国）跟踪的情况下访问站点。不幸的是，权衡的结果是通过Tor浏览器浏览会慢得多，因为没有那么多路由器，网络带宽有限。



*图13-2：Tor浏览器的登录页面*

除了能够访问传统互联网上几乎任何网站外，Tor浏览器还能够访问暗网。构成暗网的网站需要匿名，因此它们只允许通过Tor浏览器访问，并且它们的地址以.onion结尾用于其顶级域名（TLD）。暗网因非法活动而臭名昭着，但也有一些合法的服务。但请注意：在访问暗网时，您可能会遇到很多人会觉得冒犯的内容。

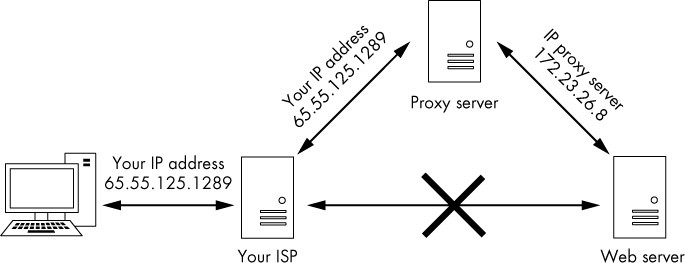
#### *安全问题*

美国和其他国家的情报和间谍机构认为Tor网络是对国家安全的威胁，认为这样一个匿名网络可以让外国政府和恐怖分子在不被监视的情况下进行交流。因此，许多强大的、雄心勃勃的研究项目正在努力打破Tor的匿名性。

Tor的匿名曾经被这些当局破坏过，而且很可能会再次被破坏。例如，NSA运行自己的Tor路由器，这意味着当您使用Tor时，您的流量可能正在通过NSA的路由器。如果您的流量正在退出NSA的路由器，那就更糟了，因为退出路由器总是知道您的目的地。NSA还有一种被称为“流量关联”(traffic correlation)的方法，该方法涉及寻找进出流量的模式，能够打破Tor的匿名性。虽然这些破解Tor的尝试不会影响Tor在商业服务(如Google)中隐藏您身份的有效性，但它们可能会限制浏览器在间谍机构中保持匿名的有效性。

### 代理服务器

在互联网上实现匿名的另一种策略是使用代理，代理是充当流量中间商的中间系统：用户连接到代理，并在传递代理之前向其提供流量的IP地址(参见图13-3)。当流量从目标返回时，代理将流量发送回源IP。通过这种方式，流量似乎来自代理，而不是原始IP地址。



*图13-3:通过代理服务器运行流量*

当然，代理可能会记录您的流量，但调查人员必须获得传票或搜查令才能获得这些日志。为了使您的流量更加难以跟踪，您可以在称为代理链的策略中使用多个代理，这一策略我们将在本章稍后讨论。

Kali Linux有一个优秀的代理工具，称为proxychain，您可以设置它来隐藏您的流量。proxychain命令的语法很简单，如下所示:

kali >proxychains <the command you want proxied> <arguments>

您提供的参数可能包括一个IP地址。例如，如果您想使用命令nmap以通过代理链匿名方式扫描一个站点，则应输入以下内容：

kali >proxychains nmap -sT - Pn <IP address>

这将通过代理将nmap -sS扫描命令隐身发送到给定的IP地址。然后，该工具自己构建代理链，因此您不必担心它。

#### *在配置文件中设置代理*

在本节中，我们为要使用的proxychain命令设置了一个代理。与Linux/Unix中的几乎所有应用程序一样，proxychain的配置是由配置文件管理的，即是/etc/proxychain .conf。使用以下命令在您选择的文本编辑器中打开配置文件(如果需要，用您选择的编辑器替换leafpad):

kali >leafpad /etc/proxychains.conf

您应该看到类似于代码清单13-1中所示的文件。

# proxychains.conf VER 3.1

# HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.

# The option below identifies how the ProxyList is treated.

# only one option should be uncommented at time,

# otherwise the last appearing option will be accepted

#

# dynamic\_chain

#

# Dynamic ­ Each connection will be done via chained proxies

# all proxies chained in the order as they appear in the list

# at least one proxy must be online to play in chain

# (dead proxies are skipped)

# otherwise EINTR is returned to the app strict chain

# Strict ­ Each connection will be done via chained proxies

# all proxies chained in the order as they appear in the list

# all proxies must be online to play in chain

# otherwise EINTR is returned to the app M

­­snip­­

*清单13-1：proxychains.conf文件*

将此文件向下滚动到第61行，您应该看到ProxyList部分，如清单13-2所示。

[ProxyList]

# add proxy here...

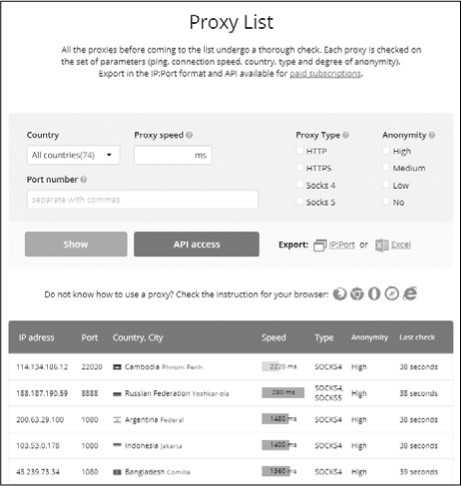
# meanwhile

# defaults set to "tor"

socks4 127.0.0.1 9050

*清单13-2：用于添加代理的配置文件部分*

我们可以通过输入要在此列表中使用的代理的IP地址和端口来添加代理。现在，我们将使用一些免费代理。你可以通过谷歌搜索“免费代理”或使用网站http://www.hidemy.name找到免费代理，如图3-4。 但请注意，在现实黑客活动中使用免费代理并不是一个好主意。我将在本章后面详细介绍这一点。这里使用的示例仅用于教育目的。



*图13-4：http://www.hidemy.name中的免费代理*

填写表单中的详细信息或单击搜索，然后使用以下格式将其中一个生成的代理添加到proxychains.conf文件中：

Type IPaddress Port

这是一个例子：

[ProxyList]

# add proxy here...

socks4 114.134.186.12 22020

# meanwhile

# defaults set to "tor"

# socks4 127.0.0.1 9050

需要注意的是，如果您没有输入自己的代理，那么proxychain默认使用Tor。清单13-2中的最后一行指示代理链首先通过主机127.0.0.1上的9050端口发送流量（默认Tor配置）。如果您没有添加自己的代理，并希望使用Tor，那么请保持现状。如果您不使用Tor，您将需要注释掉这一行(在它之前添加一个#)。

虽然我很喜欢Tor，但它通常很慢。而且，由于NSA已经破解了Tor，我不太可能依赖它的匿名性。因此，我注释掉这一行并添加自己的代理集。

我们来测试一下。在本例中，我将打开浏览器Firefox，通过代理发送流量，让它匿名导航到https://www.hacks-arise.com/。

命令如下:

kali >proxychains firefox [www.hackers-arise.com](http://www.hackers-arise.com/)

这将通过我选择的代理成功地在Firefox中打开https://www.hacks-arise.com/并将结果返回给我。对于任何跟踪此流量的人来说，似乎是我的代理导航到了https://www.hacks-arise.com/，而不是我的IP地址。

#### *一些更有趣的选择*

现在我们已经让proxychain工作了，让我们看看可以通过proxychain.conf文件配置的其他选项。正如我们现在所设置的，我们只是使用一个代理。但是，我们可以放入多个代理并使用它们，我们可以使用列表中的有限数量，或者我们可以让proxychain随机改变顺序。

让我们尝试所有这些选项。

##### 添加更多的代理

首先，让我们向列表中添加更多代理。回到http://www.hidemy.name并找到更多的代理IP地址。然后在proxychain .conf文件中添加更多的代理，如下所示:

[ProxyList]

# add proxy here...

socks4 114.134.186.12 22020

socks4 188.187.190.59 8888

socks4 181.113.121.158 335551

现在保存这个配置文件，并尝试运行以下命令:

kali >proxychains firefox www.hackers-arise.com

您不会注意到任何差异，但是您的数据包现在正在通过几个代理进行传输。

##### 动态链接

在我们的proxychain.conf文件中有多个ip，我们可以设置动态链接（*dynamic chaining*），它通过列表中的每个代理运行我们的流量，如果其中一个代理宕机或没有响应，则自动转到列表中的下一个代理，而不会抛出错误。如果我们不设置这个，则其中一个失败的代理将会破坏我们整个的请求。

回到proxychain配置文件中，找到dynamic\_chain行(第10行)并取消注释，如下所示。还要确保注释掉strict\_chain行(如果还没有的话)。

# dynamic\_chain

#

# Dynamic – Each connection will be done via chained proxies

# all proxies chained in the order as they appear in the list

# at least one proxy must be online to play in chain

­­snip­­

这将实现我们代理的动态链接，从而允许更大的匿名性和无故障的黑客攻击。保存配置文件并随意试用它。

##### 随机链接

最后一个代理技巧是随机链接（*random chaining*）选项，其中proxychain将从列表中随机选择一组IP地址，并使用它们创建代理链。这意味着每次我们使用proxychain时，代理对目标的外观都会有所不同，这使得从源跟踪我们的流量变得更加困难。这个选项也被认为是“动态”的，因为如果一个代理关闭，它将跳到下一个代理。

回到/etc/proxychain.conf文件中，通过在每个行代码的开头添加一个#来注释掉dynamic\_chain和strict\_chain这两行代码，然后取消对random\_chain行代码的注释。我们一次只能使用这三个选项中的一个，所以在使用proxychain之前一定要注释掉其他选项。

接下来，使用chain\_len查找并取消对该行的注释，然后给出一个合理的数字。这一行确定在创建随机代理链时将使用链中的多少IP地址。

# dynamic\_chain

#

# Dynamic – Each connection will be done via chained proxies

# all proxies chained in the order as they appear in the list

# at least one proxy must be online to play in chain

#

# strict\_chain

#

# Strict ­ Each connection will be done via chained proxies

# all proxies chained in the order as they appear in the list

# all proxies must be online to play in chain

# otherwise EINTR is returned to the app

#

random\_chain

# Random ­ Each connection will be done via random proxy

# (or proxy chain, see chain\_len) from the list.

# this option is good to test your IDS :)

# Makes sense only if random\_chain

chain\_len = 3

在这里，我已经取消了chain\_len的注释，并将其赋值为3，这意味着proxychain现在将使用/etc/proxychain .conf文件中我的列表中的三个代理，随机选择它们，并在代理关闭时转移到下一个代理。请注意，虽然这种方法肯定会增强匿名性，但也会增加在线活动的延迟。

现在您已经知道如何使用proxychain，您可以在相对匿名的情况下进行黑客攻击。我说“相对”，是因为在NSA和FSB（美国国家安全局和联邦安全局）监视我们的网络活动的情况下，没有绝对可靠的方法来保持匿名，但我们可以借助proxychain来更有效地进行侦查。

#### *安全问题*

关于代理安全性的最后一个注意事项是，一定要明智地选择您的代理：proxychains只与您使用的代理一样好。如果您希望保持匿名，请不要使用前面提到的免费代理。黑客使用可信任的付费代理。事实上，免费代理很可能会出售你的IP地址和浏览历史。正如著名密码学家和安全专家布鲁斯施奈尔(Bruce Schneier)曾经说过的，“如果有些东西是免费的，那么你就不是客户的产品，你就是它的用户。”换句话说，任何免费产品都有可能收集你的数据并出售。不然他们为什么要免费提供代理呢?

虽然您离开代理的流量的IP地址是匿名的，但是监视机构可以通过其他方式识别您。例如，代理的所有者将知道您的身份，如果受到足够的间谍或有管辖权的执法机构的压力，可能会提供您的身份来保护他们的业务。了解代理作为匿名来源的局限性是很重要的。

### 虚拟专用网络

使用虚拟专用网(VPN)是保持您的web流量相对匿名和安全的有效方法。VPN用于连接到一个中间的互联网设备，例如路由器，它将您的流量发送到其最终目的地，并使用该路由器的IP地址进行标记。

使用VPN当然可以增强您的安全性和隐私，但它不能保证匿名。您所连接的互联网设备必须记录或记录您的IP地址，以便能够正确地将数据发送回您，这样任何能够访问这些记录的人都可以发现关于您的信息。

VPN的优点是简单易用。您可以在VPN提供商那里开户，然后在每次登录计算机时无缝连接VPN。您可以像往常一样使用浏览器来浏览web，但是任何人看到您的流量来自互联网 VPN设备的IP地址和位置，而不是您自己的。另外，您与VPN设备之间的所有通信都是加密的，所以即使您的互联网服务提供商也看不到您的通信。

除此之外，VPN可以有效地规避政府控制的内容和信息审查。例如，如果您的国家政府限制您访问具有特定政治信息的网站，您可以使用您所在国家/地区以外的VPN来访问该内容。 一些媒体公司，如Netflix，Hulu和HBO，将其内容的访问权限限制为源自其本国的IP地址。在这些服务允许的国家/地区使用VPN通常可以帮助您解决这些访问限制。

根据CNET，一些最好和最受欢迎的商业VPN服务如下：

* IPVanish
* NordVPN
* ExpressVPN
* CyberGhost
* Golden Frog VPN
* Hide My Ass (HMA)
* Private Internet Access
* PureVPN
* TorGuard
* Buffered VPN

大多数VPN服务每年收费50 - 100美元，许多还提供30天免费试用期。要了解如何设置VPN的更多信息，请从列表中选择一个并访问该网站。您应该可以找到非常容易遵循的下载、安装和使用说明。

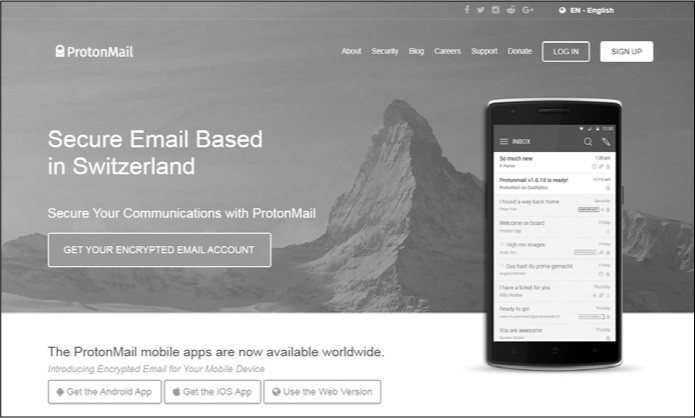
VPN的优点是所有流量在离开计算机时都是加密的，从而保护您不受窥探，当您访问一个站点时，您的IP地址被VPN IP地址所掩盖。与代理服务器一样，VPN的所有者拥有您的原始IP地址(否则他们无法将您的流量发回给您)。如果他们受到间谍机构或执法部门的压力，他们可能会放弃你的身份。防止这种情况的一种方法是只使用承诺不存储或记录任何此类信息的vpn(并希望它们是真实的)。这样，如果有人坚持要求VPN服务提供商将数据交给用户，那么就没有数据。

### 加密的电子邮件

免费的商业电子邮件服务，如Gmail，雅虎!，Outlook Web Mail(前身为Hotmail)的免费是有原因的：它们是追踪你的兴趣和提供广告的工具。如前所述，如果服务是免费的，那么您就是产品，而不是客户。此外，电子邮件提供者的服务器(例如谷歌)可以访问电子邮件的未加密内容，即使您使用HTTPS。

防止窃听你的电子邮件的一个方法是使用加密的电子邮件。ProtonMail，如图13-5所示，从一端加密到另一端或从一个浏览器加密到另一个浏览器。这意味着您的电子邮件是在ProtonMail服务器上加密的，即使是ProtonMail管理员也无法读取您的电子邮件。

ProtonMail是由一群年轻的科学家在瑞士欧洲核子研究中心（CERN）的超级对撞机设施工厂建立的。瑞士在保护机密方面有着悠久而传奇的历史(还记得你经常听说的那些瑞士银行账户吗?) ProtonMail的服务器位于欧盟，该网络在分享个人数据方面有着比美国法律更为严格的法律规定。ProtonMail不收取基本帐户，但提供保费帐户象征性的费用。需要注意的是，在与非protonmail用户交换电子邮件时，可能有部分或全部电子邮件没有加密。有关详细信息，请参见ProtonMail支持知识库。



*图13-5：ProtonMail登录界面*

### 总结

我们不断受到商业公司和国家情报机构的监视。为了保证数据和web传输的安全性，您需要实现本章中讨论的至少一种安全措施。通过组合使用它们，您可以最大限度地减少在Web上的占用空间并使数据更加安全。

**练习**

在你继续学习第14章之前，通过完成以下练习来尝试你从这一章中学到的技能:

1.运行**traceroute**到您最喜欢的网站。你和你最喜欢的网站之间出现了多少跳?

2.下载并安装Tor浏览器。现在，像使用其他浏览器一样匿名浏览web，看看是否注意到了速度上的差异。

3.尝试在Firefox浏览器中使用proxychain来导航到您最喜欢的网站。

4.从本章列出的一些供应商那里探索商业VPN服务。选择一个并测试一个免费试用。

5.打开一个免费的ProtonMail帐户，发送一个安全的问候到ccupytheweb@ protonmail.com。

## 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（http://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