

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。



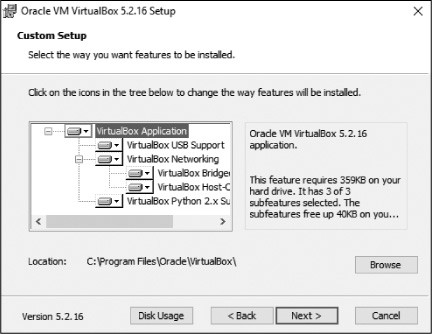
*图1:VirtualBox主页*

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**。

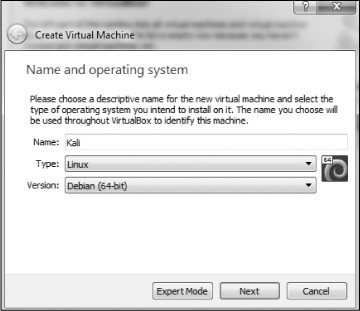
***设置虚拟机***

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。



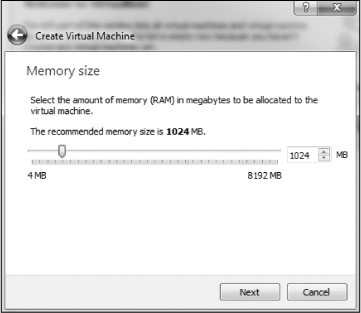
*图4: VirtualBox Manager*

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*

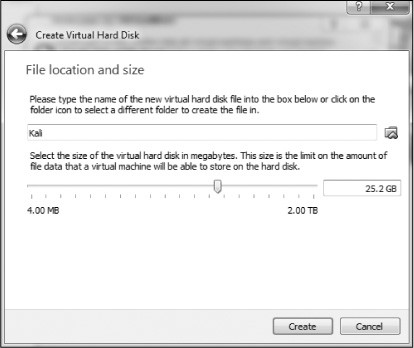
在这里，您需要选择要为此新虚拟机分配多少RAM。

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）。



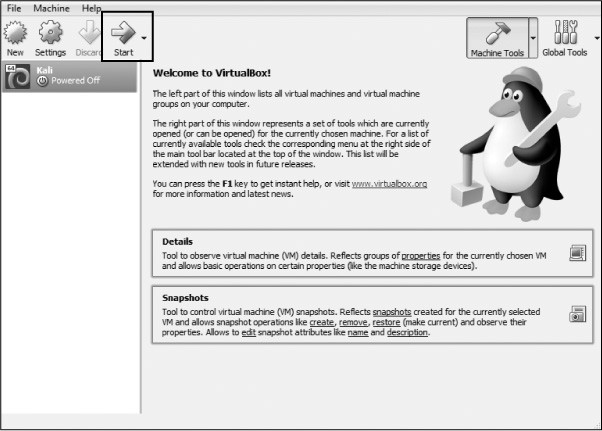
*图7: 分配硬盘空间*

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!

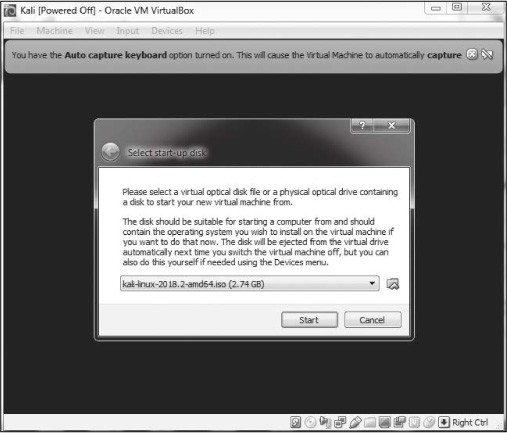
***在VM上安装Kali***

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*

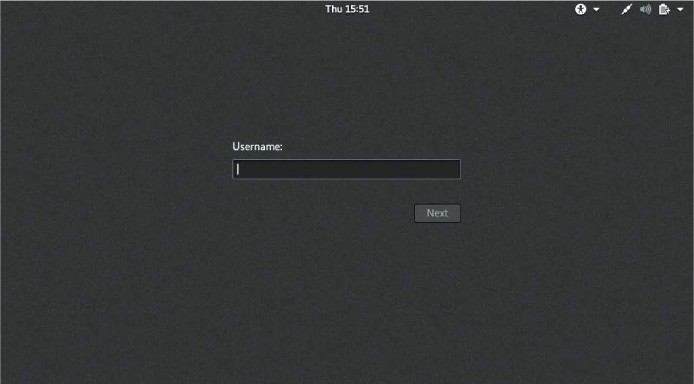
在下一个屏幕上，系统将提示您是自动还是手动安装GRUB引导加载程序。由于原因尚不清楚，如果您选择第二个选项，Kali将倾向于挂起并在安装后显示空白屏幕。选择手动输入设备**Enter device manually**，如图15所示。



*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。

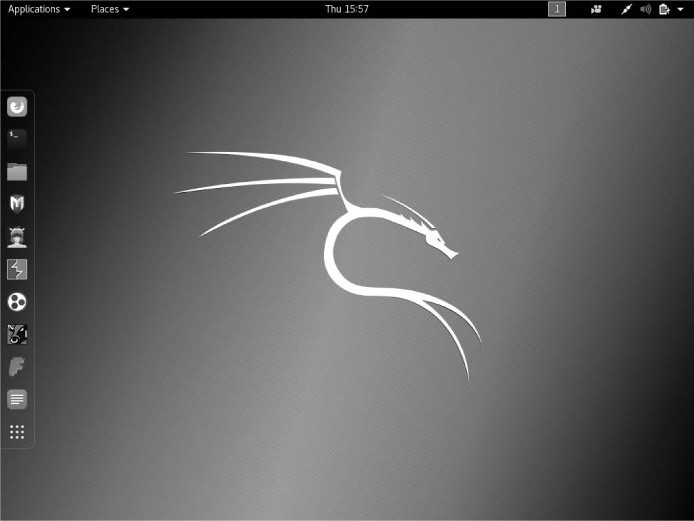
恭喜！你已经安装了Kali。单击**Continue**继续。Kali将尝试重新启动，在您最终遇到Kali 2019的登录屏幕之前，您将看到许多代码行穿过一个空白的黑色屏幕，然后如图16所示。



*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。

**INTRODUCTORY TERMS AND CONCEPTS**

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。

Binaries This term refers to files that can be executed, similar to executables in Windows. Binaries generally reside in the /usr/bin or usr/sbin directory and include utilities such as ps, cat, ls, and cd (we’ll touch on all of four of these in this chapter) as well as applications such as the wireless hacking tool aircrack­ng and the intrusion detection system (IDS) Snort.

**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 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。

Home Each user has their own /home directory, and this is generally where files you create will be saved by default.

Kali Kali Linux is a distribution of Linux specifically designed for penetration testing. It has hundreds of tools preinstalled, saving you the hours it would take to download and install them yourself. I will be using the latest version of Kali at the time of this writing: Kali 2018.2, first released in April 2018.

root Like nearly every operating system, Linux has an administrator or superuser account, designed for use by a trusted person who can do nearly anything on the system. This would include such things as reconfiguring the system, adding users, and changing passwords. In Linux, that account is called root. As a hacker or pentester, you will often use the root account to give yourself control over the system. In fact, many hacker tools require that you use the root account.

Script This is a series of commands run in an interpretive environment that converts each line to source code. Many hacking tools are simply scripts. Scripts can be run with the bash interpreter or any of the other scripting language interpreters, such as Python, Perl, or Ruby. Python is currently the most popular interpreter among hackers.

Shell This is an environment and interpreter for running commands in Linux. The most widely used shell is bash, which stands for Bourne­again shell, but other popular shells include the C shell and Z shell. I will be using the bash shell exclusively in this book.

Terminal This is a command line interface (CLI).

With those basics behind us, we will attempt to methodically develop the essential Linux skills you’ll need to become a hacker or penetration tester. In this first chapter, I’ll walk you through getting started with Kali Linux.

## 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