# CONTENTS IN DETAIL

## ACKNOWLEDGMENTS

## INTRODUCTION

<table>
<thead>
<tr>
<th>What's in This Book</th>
<th>xxii</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is Ethical Hacking?</td>
<td>xxiii</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>xxiii</td>
</tr>
<tr>
<td>Military and Espionage</td>
<td>xxiii</td>
</tr>
<tr>
<td>Why Hackers Use Linux</td>
<td>xxiv</td>
</tr>
<tr>
<td>Linux Is Open Source</td>
<td>xxiv</td>
</tr>
<tr>
<td>Linux Is Transparent</td>
<td>xxiv</td>
</tr>
<tr>
<td>Linux Offers Granular Control</td>
<td>xxiv</td>
</tr>
<tr>
<td>Most Hacking Tools Are Written for Linux</td>
<td>xxiv</td>
</tr>
<tr>
<td>The Future Belongs to Linux/Unix</td>
<td>xxiv</td>
</tr>
<tr>
<td>Downloading Kali Linux</td>
<td>xxv</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>xxvi</td>
</tr>
<tr>
<td>Installing VirtualBox</td>
<td>xxvi</td>
</tr>
<tr>
<td>Setting Up Your Virtual Machine</td>
<td>xxvii</td>
</tr>
<tr>
<td>Installing Kali on the VM</td>
<td>xxix</td>
</tr>
<tr>
<td>Setting Up Kali</td>
<td>xxxi</td>
</tr>
</tbody>
</table>

## 1 GETTING STARTED WITH THE BASICS

<table>
<thead>
<tr>
<th>Introductory Terms and Concepts</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Tour of Kali</td>
<td>3</td>
</tr>
<tr>
<td>The Terminal</td>
<td>4</td>
</tr>
<tr>
<td>The Linux Filesystem</td>
<td>4</td>
</tr>
<tr>
<td>Basic Commands in Linux</td>
<td>5</td>
</tr>
<tr>
<td>Finding Yourself with pwd</td>
<td>6</td>
</tr>
<tr>
<td>Checking Your Login with whoami</td>
<td>6</td>
</tr>
<tr>
<td>Navigating the Linux Filesystem</td>
<td>6</td>
</tr>
<tr>
<td>Getting Help</td>
<td>8</td>
</tr>
<tr>
<td>Referencing Manual Pages with man</td>
<td>9</td>
</tr>
<tr>
<td>Finding Stuff</td>
<td>9</td>
</tr>
<tr>
<td>Searching with locate</td>
<td>10</td>
</tr>
<tr>
<td>Finding Binaries with whereis</td>
<td>10</td>
</tr>
<tr>
<td>Finding Binaries in the PATH Variable with which</td>
<td>10</td>
</tr>
<tr>
<td>Performing More Powerful Searches with find</td>
<td>11</td>
</tr>
<tr>
<td>Filtering with grep</td>
<td>12</td>
</tr>
<tr>
<td>Modifying Files and Directories</td>
<td>13</td>
</tr>
<tr>
<td>Creating Files</td>
<td>13</td>
</tr>
<tr>
<td>Creating a Directory</td>
<td>15</td>
</tr>
<tr>
<td>Copying a File</td>
<td>15</td>
</tr>
</tbody>
</table>
2
TEXT MANIPULATION

20
Viewing Files
  Taking the Head
  Grabbing That Tail
  Numbering the Lines
21
Filtering Text with grep
  Hacker Challenge: Using grep, nl, tail, and head
22
Using sed to Find and Replace.
23
Viewing Files with more and less
  Controlling the Display with more
  Displaying and Filtering with less
24
Summary
25
Exercises
26

3
ANALYZING AND MANAGING NETWORKS

29
Analyzing Networks with ifconfig
30
Checking Wireless Network Devices with iwconfig
31
Changing Your Network Information
  Changing Your IP Address
  Changing Your Network Mask and Broadcast Address
  Spoofing Your MAC Address
  Assigning New IP Addresses from the DHCP Server
32
Manipulating the Domain Name System
  Examining DNS with dig
  Changing Your DNS Server
  Mapping Your Own IP Addresses
33
Summary
34
Exercises
37

4
ADDING AND REMOVING SOFTWARE

39
Using apt to Handle Software
  Searching for a Package
  Adding Software
  Removing Software
  Updating Packages
  Upgrading Packages
40
Adding Repositories to Your sources.list File
41
Using a GUI-based Installer
42
Installing Software with git
43
Summary
44
Exercises
47
8
BASH SCRIPTING .................................................. 81
A Crash Course in Bash ........................................... 82
Your First Script: “Hello, Hackers-Arise!” ..................... 82
   Setting Execute Permissions ................................ 83
   Running HelloHackersArise ................................ 84
   Adding Functionality with Variables and User Input...... 84
Your Very First Hacker Script: Scan for Open Ports ........ 86
   Our Task ...................................................... 86
   A Simple Scanner .......................................... 87
   Improving the MySQL Scanner ............................. 88
Common Built-in Bash Commands ............................... 90
Summary .................................................................. 91
Exercises ............................................................ 91

9
COMPRESSING AND ARCHIVING ....... 93
What Is Compression? ............................................. 93
Tarring Files Together ............................................ 94
Compressing Files ................................................ 96
   Compressing with gzip ..................................... 96
   Compressing with bzip2 .................................... 97
   Compressing with compress ......................... 97
Creating Bit-by-Bit or Physical Copies of Storage Devices . 98
Summary ............................................................ 99
Exercises ............................................................ 99

10
FILESYSTEM AND STORAGE DEVICE MANAGEMENT ....... 101
The Device Directory /dev ........................................... 102
   How Linux Represents Storage Devices .................. 103
   Drive Partitions ............................................. 103
   Character and Block Devices ............................... 105
   List Block Devices and Information with lsblk ........ 105
Mounting and Unmounting ....................................... 106
   Mounting Storage Devices Yourself ....................... 106
   Unmounting with umount .................................. 107
Monitoring Filesystems ............................................ 107
   Getting Information on Mounted Disks .................. 107
   Checking for Errors ........................................ 108
Summary ............................................................ 109
Exercises ............................................................ 109

11
THE LOGGING SYSTEM 111
The rsyslog Logging Daemon ...................................... 112
   The rsyslog Configuration File ............................. 112
   The rsyslog Logging Rules .................................. 113
## 14 UNDERSTANDING AND INSPECTING WIRELESS NETWORKS

Wi-Fi Networks .................................................. 153
  Basic Wireless Commands .................................. 154
  Wi-Fi Recon with aircrack-ng .............................. 157
Detecting and Connecting to Bluetooth .................... 159
  How Bluetooth Works ........................................ 160
  Bluetooth Scanning and Reconnaissance ................. 160
Summary .......................................................... 164
Exercises ......................................................... 164

## 15 MANAGING THE LINUX KERNEL AND LOADABLE KERNEL MODULES

What Is a Kernel Module? ..................................... 166
Checking the Kernel Version ................................. 167
Kernel Tuning with sysctl .................................... 167
Managing Kernel Modules .................................... 169
  Finding More Information with modinfo ................. 170
  Adding and Removing Modules with modprobe ........... 170
  Inserting and Removing a Kernel Module ................. 171
Summary .......................................................... 171
Exercises ......................................................... 172

## 16 AUTOMATING TASKS WITH JOB SCHEDULING

Scheduling an Event or Job to Run on an Automatic Basis ................................. 174
  Scheduling a Backup Task .................................. 176
  Using crontab to Schedule Your MySQLscanner ........ 177
  crontab Shortcuts ............................................. 178
Using rc Scripts to Run Jobs at Startup .................... 178
  Linux Runlevels .............................................. 179
  Adding Services to rc.d ..................................... 179
Adding Services to Your Bootup via a GUI .................. 180
Summary .......................................................... 181
Exercises ......................................................... 181

## 17 PYTHON SCRIPTING BASICS FOR HACKERS

Adding Python Modules ........................................ 184
  Using pip ....................................................... 184
  Installing Third-Party Modules ............................ 185
Getting Started Scripting with Python ....................... 186
  Variables ....................................................... 187
  Comments ........................................................ 190
  Functions ....................................................... 190
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>191</td>
</tr>
<tr>
<td>Modules</td>
<td>192</td>
</tr>
<tr>
<td>Object-Oriented Programming (OOP)</td>
<td>192</td>
</tr>
<tr>
<td>Network Communications in Python</td>
<td>194</td>
</tr>
<tr>
<td>Building a TCP Client</td>
<td>194</td>
</tr>
<tr>
<td>Creating a TCP Listener</td>
<td>195</td>
</tr>
<tr>
<td>Dictionaries, Loops, and Control Statements</td>
<td>197</td>
</tr>
<tr>
<td>Dictionaries</td>
<td>197</td>
</tr>
<tr>
<td>Control Statements</td>
<td>197</td>
</tr>
<tr>
<td>Loops</td>
<td>198</td>
</tr>
<tr>
<td>Improving Our Hacking Scripts</td>
<td>199</td>
</tr>
<tr>
<td>Exceptions and Password Crackers</td>
<td>201</td>
</tr>
<tr>
<td>Summary</td>
<td>203</td>
</tr>
<tr>
<td>Exercises</td>
<td>203</td>
</tr>
</tbody>
</table>