

# CONTENTS IN DETAIL

<b>ACKNOWLEDGMENTS</b>	<b>xix</b>
------------------------	------------

<b>INTRODUCTION</b>	<b>xxi</b>
---------------------	------------

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

<b>1</b>	
<b>GETTING STARTED WITH THE BASICS</b>	<b>1</b>

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

Renaming a File . . . . .	15
Removing a File . . . . .	16
Removing a Directory . . . . .	16
Go Play Now! . . . . .	17
Exercises . . . . .	17

## **2** **TEXT MANIPULATION** **19**

Viewing Files . . . . .	20
Taking the Head . . . . .	20
Grabbing That Tail . . . . .	21
Numbering the Lines . . . . .	22
Filtering Text with grep . . . . .	22
Hacker Challenge: Using grep, nl, tail, and head . . . . .	23
Using sed to Find and Replace . . . . .	23
Viewing Files with more and less . . . . .	24
Controlling the Display with more . . . . .	25
Displaying and Filtering with less . . . . .	25
Summary . . . . .	26
Exercises . . . . .	27

## **3** **ANALYZING AND MANAGING NETWORKS** **29**

Analyzing Networks with ifconfig . . . . .	29
Checking Wireless Network Devices with iwconfig . . . . .	30
Changing Your Network Information . . . . .	31
Changing Your IP Address . . . . .	31
Changing Your Network Mask and Broadcast Address . . . . .	32
Spoofing Your MAC Address . . . . .	32
Assigning New IP Addresses from the DHCP Server . . . . .	32
Manipulating the Domain Name System . . . . .	33
Examining DNS with dig . . . . .	33
Changing Your DNS Server . . . . .	34
Mapping Your Own IP Addresses . . . . .	36
Summary . . . . .	37
Exercises . . . . .	37

## **4** **ADDING AND REMOVING SOFTWARE** **39**

Using apt to Handle Software . . . . .	40
Searching for a Package . . . . .	40
Adding Software . . . . .	40
Removing Software . . . . .	41
Updating Packages . . . . .	42
Upgrading Packages . . . . .	42
Adding Repositories to Your sources.list File . . . . .	43
Using a GUI-based Installer . . . . .	45
Installing Software with git . . . . .	46
Summary . . . . .	47
Exercises . . . . .	47

**5**  
**CONTROLLING FILE AND DIRECTORY PERMISSIONS** **49**

Different Types of Users . . . . . 50  
Granting Permissions . . . . . 50  
    Granting Ownership to an Individual User . . . . . 50  
    Granting Ownership to a Group . . . . . 51  
Checking Permissions . . . . . 51  
Changing Permissions . . . . . 52  
    Changing Permissions with Decimal Notation . . . . . 52  
    Changing Permissions with UGO . . . . . 54  
    Giving Root Execute Permission on a New Tool . . . . . 55  
Setting More Secure Default Permissions with Masks . . . . . 56  
Special Permissions . . . . . 57  
    Granting Temporary Root Permissions with SUID . . . . . 57  
    Granting the Root User’s Group Permissions SGID . . . . . 58  
    The Outmoded Sticky Bit . . . . . 58  
    Special Permissions, Privilege Escalation, and the Hacker . . . . . 58  
Summary . . . . . 60  
Exercises . . . . . 60

**6**  
**PROCESS MANAGEMENT** **61**

Viewing Processes . . . . . 62  
    Filtering by Process Name . . . . . 63  
    Finding the Greediest Processes with top . . . . . 64  
Managing Processes . . . . . 64  
    Changing Process Priority with nice . . . . . 65  
    Killing Processes . . . . . 66  
    Running Processes in the Background . . . . . 68  
    Moving a Process to the Foreground . . . . . 68  
Scheduling Processes . . . . . 69  
Summary . . . . . 70  
Exercises . . . . . 70

**7**  
**MANAGING USER ENVIRONMENT VARIABLES** **71**

Viewing and Modifying Environment Variables . . . . . 72  
    Viewing All Environment Variables . . . . . 72  
    Filtering for Particular Variables . . . . . 73  
    Changing Variable Values for a Session . . . . . 73  
    Making Variable Value Changes Permanent . . . . . 74  
Changing Your Shell Prompt . . . . . 75  
Changing Your PATH . . . . . 76  
    Adding to the PATH Variable . . . . . 76  
    How Not to Add to the PATH Variable . . . . . 77  
Creating a User-Defined Variable . . . . . 77  
Summary . . . . . 78  
Exercises . . . . . 79

<b>8</b>		
<b>BASH SCRIPTING</b>		<b>81</b>
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

<b>9</b>		
<b>COMPRESSING AND ARCHIVING</b>		<b>93</b>
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

<b>10</b>		
<b>FILESYSTEM AND STORAGE DEVICE MANAGEMENT</b>		<b>101</b>
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

<b>11</b>		
<b>THE LOGGING SYSTEM</b>		<b>111</b>
The rsyslog Logging Daemon . . . . .		112
The rsyslog Configuration File . . . . .		112
The rsyslog Logging Rules . . . . .		113

Automatically Cleaning Up Logs with logrotate . . . . .	115
Remaining Stealthy. . . . .	117
Removing Evidence . . . . .	117
Disabling Logging . . . . .	118
Summary . . . . .	119
Exercises . . . . .	119

## **12 USING AND ABUSING SERVICES 121**

Starting, Stopping, and Restarting Services . . . . .	122
Creating an HTTP Web Server with the Apache Web Server . . . . .	122
Starting with Apache . . . . .	123
Editing the index.html File . . . . .	124
Adding Some HTML . . . . .	124
Seeing What Happens . . . . .	125
OpenSSH and the Raspberry Spy Pi . . . . .	125
Setting Up the Raspberry Pi . . . . .	126
Building the Raspberry Spy Pi . . . . .	126
Configuring the Camera . . . . .	127
Starting to Spy . . . . .	129
Extracting Information from MySQL . . . . .	130
Starting MySQL . . . . .	130
Interacting with MySQL . . . . .	131
Setting a MySQL Password . . . . .	131
Accessing a Remote Database . . . . .	132
Connecting to a Database . . . . .	133
Database Tables . . . . .	134
Examining the Data . . . . .	135
PostgreSQL with Metasploit . . . . .	135
Summary . . . . .	137
Exercises . . . . .	138

## **13 BECOMING SECURE AND ANONYMOUS 139**

How the Internet Gives Us Away . . . . .	140
The Onion Router System . . . . .	141
How Tor Works . . . . .	141
Security Concerns . . . . .	142
Proxy Servers . . . . .	143
Setting Proxies in the Config File . . . . .	144
Some More Interesting Options . . . . .	146
Security Concerns . . . . .	148
Virtual Private Networks . . . . .	148
Encrypted Email . . . . .	150
Summary . . . . .	151
Exercises . . . . .	151

<b>14</b>	<b>UNDERSTANDING AND INSPECTING WIRELESS NETWORKS</b>	<b>153</b>
Wi-Fi Networks . . . . .		154
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
<b>15</b>	<b>MANAGING THE LINUX KERNEL AND LOADABLE KERNEL MODULES</b>	<b>165</b>
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
<b>16</b>	<b>AUTOMATING TASKS WITH JOB SCHEDULING</b>	<b>173</b>
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
<b>17</b>	<b>PYTHON SCRIPTING BASICS FOR HACKERS</b>	<b>183</b>
Adding Python Modules . . . . .		184
Using pip . . . . .		184
Installing Third-Party Modules . . . . .		185
Getting Started Scripting with Python . . . . .		186
Variables . . . . .		187
Comments . . . . .		190
Functions . . . . .		190

Lists . . . . .	191
Modules . . . . .	192
Object-Oriented Programming (OOP) . . . . .	192
Network Communications in Python . . . . .	194
Building a TCP Client . . . . .	194
Creating a TCP Listener . . . . .	195
Dictionaries, Loops, and Control Statements . . . . .	197
Dictionaries . . . . .	197
Control Statements . . . . .	197
Loops . . . . .	198
Improving Our Hacking Scripts . . . . .	199
Exceptions and Password Crackers . . . . .	201
Summary . . . . .	203
Exercises . . . . .	203

**INDEX**