

CONTENTS IN DETAIL

PREFACE	xix
----------------	------------

ACKNOWLEDGMENTS	xxi
------------------------	------------

INTRODUCTION	xxiii
---------------------	--------------

What's in This Bookxxiv
What Is Ethical Hacking?xxv
Penetration Testing.xxv
Military and Espionagexxvi
Why Hackers Use Linuxxxvi
Linux Is Open Source.xxvi
Linux Is Transparent.xxvi
Linux Offers Granular Control.xxvi
Most Hacking Tools Are Written for Linux.xxvi
The Future Belongs to Linux/Unixxxvii
Downloading Kali Linuxxxvii
Virtual Machinesxxviii
Installing VirtualBox.xxix
Setting Up Your Virtual Machinexxix
Installing Kali on the VMxxxii
Setting Up Kalixxxii
Installing Kali Through the Windows Subsystem for Linuxxxxvii

1	
GETTING STARTED WITH THE BASICS	1

Introductory Terms and Concepts	1
A Tour of Kali	3
The Terminal.	3
The Linux Filesystem.	3
Basic Commands in Linux	4
Finding Yourself with pwd	5
Checking Your Login with whoami.	5
Navigating the Linux Filesystem	6
Getting Help.	7
Referencing Manual Pages with man	8
Finding Stuff	8
Searching with locate	9
Finding Binaries with whereis	9
Finding Binaries in the PATH Variable with which	9
Performing More Powerful Searches with find.	10
Filtering with grep	11
Modifying Files and Directories	12
Creating Files	12
Creating a Directory	14
Copying a File	14
Renaming a File	15

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

2

TEXT MANIPULATION **17**

Viewing Files.	18
Finding the Head	18
Finding the Tail	19
Numbering the Lines	20
Filtering Text with grep	21
Using sed to Find and Replace.	21
Viewing Files with more and less	23
Controlling the Display with more	23
Displaying and Filtering with less	24
Summary	25
Exercises.	25

3

ANALYZING AND MANAGING NETWORKS **27**

Analyzing Networks with ifconfig.	28
Network Statistics with netstat and ss	29
Checking Wireless Network Devices with iwconfig	30
Changing Your Network Information	31
Assigning a New IP Address	31
Changing Your Network Mask and Broadcast Address	31
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	35
Summary	36
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	47
Summary	48
Exercises.	48

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 53
 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 59
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 64
 Killing Processes 66
 Running Processes in the Background 67
 Moving a Process to the Foreground 68
Scheduling Processes 68
Summary 69
Exercises. 70

7
MANAGING USER ENVIRONMENT VARIABLES **71**

Changing the Default Shell to Bash. 72
Viewing and Modifying Environment Variables 74
 Viewing All Environment Variables 74
 Filtering for Particular Variables 75
 Changing Variable Values for a Session. 75
 Making Variable Value Changes Permanent. 76
Changing Your Shell Prompt 76
Changing Your PATH 78
 Adding to the PATH Variable 78
 How Not to Add to the PATH Variable 79
Creating a User-Defined Variable. 79
Summary 80
Exercises. 80

8		
BASH SCRIPTING		81
A Crash Course in Bash		82
Your First Script: "Hello, Hackers-Arise!"		84
Setting Execute Permissions		85
Running HelloHackersArise		85
Adding Functionality with Variables and User Input		86
Your Very First Hacker Script: Scan for Open Ports		87
Our Task		88
A Simple Scanner		89
An Improvement to the MySQL Scanner		90
Common Built-in Bash Commands		92
Summary		93
Exercises.		93

9		
COMPRESSING AND ARCHIVING		95
What Is Compression?		96
Tarring Files Together		96
Compressing Files		98
Compressing with gzip		98
Compressing with bzip2		99
Compressing with compress		99
Creating Bit-by-Bit or Physical Copies of Storage Devices		100
Summary		101
Exercises.		101

10		
FILESYSTEM AND STORAGE DEVICE MANAGEMENT		103
The Device Directory /dev		104
How Linux Represents Storage Devices		105
Drive Partitions		105
Character and Block Devices		107
List Block Devices and Information with lsblk and lsusb.		107
Mounting and Unmounting		108
Mounting Storage Devices Manually		109
Unmounting with umount		109
Monitoring Filesystems		109
Getting Information on Mounted Disks		109
Checking for Errors		110
Summary		111
Exercises.		111

11		
THE LOGGING SYSTEM		113
The journalctl Utility		114
Log Priorities and Facilities		115
journalctl Queries.		116
Using journalctl to Cover Your Tracks		118
Disabling Logging		120

Summary	121
Exercises	121

12 USING AND ABUSING SERVICES 123

Starting, Stopping, and Restarting Services	124
Creating an HTTP Server with the Apache Web Server	124
Starting with Apache	124
Editing the index.html File	125
Adding Some HTML	126
Seeing What Happens	126
OpenSSH and the Raspberry Spy Pi	127
Setting Up the Raspberry Pi	128
Building the Raspberry Spy Pi	128
Configuring the Camera	129
Starting to Spy	129
Extracting Information from MySQL/MariaDB	130
Starting MySQL or MariaDB	130
Interacting with SQL	131
Setting a Password	131
Accessing a Remote Database	133
Connecting to a Database	133
Exploring Database Tables	134
Examining the Data	135
Summary	135
Exercises	136

13 BECOMING SECURE AND ANONYMOUS 137

How the Internet Gives Us Away	138
The Onion Router System	139
How Tor Works	139
Security Concerns	141
Proxy Servers	141
Setting Proxies in the Config File	142
Configuring Some More Interesting Options	145
Concerning Security	147
Virtual Private Networks	147
Encrypted Email	148
Summary	149
Exercises	150

14 UNDERSTANDING AND INSPECTING WIRELESS NETWORKS 151

Wi-Fi Networks	152
Basic Wireless Commands	152
Wi-Fi Recon with aircrack-ng	155
Detecting and Connecting to Bluetooth	158
How Bluetooth Works	158
Bluetooth Scanning and Reconnaissance	158

Summary	162
Exercises.	162
15	
MANAGING THE LINUX KERNEL AND	
LOADABLE KERNEL MODULES	163
What Is a Kernel Module?	164
Checking the Kernel Version	165
Kernel Tuning with sysctl	165
Managing Kernel Modules	167
Finding More Information with modinfo	168
Adding and Removing Modules with modprobe	168
Inserting and Removing a Kernel Module	169
Summary	170
Exercises.	170
16	
AUTOMATING TASKS WITH JOB SCHEDULING	171
Scheduling an Event or Job to Run on an Automatic Basis	172
Scheduling a Backup Task	174
Using crontab to Schedule Your MySQLscanner	175
crontab Shortcuts	176
Using rc Scripts to Run Jobs at Startup	176
Linux Runlevels	177
Adding Services to rc.d	177
Adding Services to Your Bootup via a GUI	178
Summary	179
Exercises.	179
17	
PYTHON SCRIPTING BASICS FOR HACKERS	181
Adding Python Modules	182
Getting Started Scripting with Python	183
Variables	184
Comments	186
Functions	187
Lists	188
Modules	189
Object-Oriented Programming (OOP)	189
Network Communications in Python	190
Building a TCP Client.	190
Creating a TCP Listener	192
Dictionaries, Control Statements, and Loops	193
Dictionaries	193
Control Statements	194
Loops.	195
Improving Our Hacking Scripts	196
Exceptions and Password Crackers	197
Summary	199
Exercises.	200

18	
ARTIFICIAL INTELLIGENCE FOR HACKERS	201
Collaboration Is Key	202
Major Players in AI	203
Using AI in Cybersecurity	203
Social Engineering Attacks with AI	205
Using AI to Write a Bash Script	206
Summary	207
Exercises	207
INDEX	209