

# **LINUX BASICS FOR HACKERS**

**Getting Started with  
Networking, Scripting,  
and Security in Kali**

**by OccupyTheWeb**



**no starch  
press**

San Francisco

**LINUX BASICS FOR HACKERS.** Copyright © 2019 by OccupyTheWeb.

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN-10: 1-59327-855-1

ISBN-13: 978-1-59327-855-7

Publisher: William Pollock

Production Editors: Serena Yang and Meg Sneeringer

Cover Illustration: Josh Ellingson

Interior Design: Octopod Studios

Developmental Editor: Liz Chadwick

Technical Reviewer: Cliff Janzen

Copyeditor: Barton D. Reed

Compositors: Serena Yang and Meg Sneeringer

Proofreader: Paula L. Fleming

Indexer: JoAnne Burek

For information on distribution, translations, or bulk sales, please contact No Starch Press, Inc. directly:  
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 Cataloging-in-Publication Data*

Names: OccupyTheWeb, author.

Title: Linux basics for hackers : getting started with networking, scripting,  
and security in Kali / OccupyTheWeb.

Description: First edition. | 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)

Subjects: LCSH: Penetration testing (Computer security) | Kali Linux. |  
Hackers. | Operating systems (Computers)

Classification: LCC QA76.9.A25 (ebook) | LCC QA76.9.A25 O325 2018 (print) |  
DDC 005.8--dc23

LC record available at <https://lcn.loc.gov/2018030544>

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

I dedicate this book to my three incredible daughters.  
You mean the world to me.



## **About the Author**

OccupyTheWeb (OTW) is the pseudonym for the founder and primary writer for the hacker and pentester training website, <https://www.hackers-arise.com/>. He is a former college professor and has over 20 years of experience in the information technology industry. He has trained hackers throughout the US, including branches of the US military (Army, Air Force, and Navy) and the US intelligence community (CIA, NSA, and DNI). He is also an avid mountain biker and snow boarder.

## **About the Technical Reviewer**

Since the early days of Commodore PET and VIC-20, technology has been a constant companion (and sometimes an obsession!) to Cliff Janzen. Cliff discovered his career passion when he moved to information security in 2008 after a decade of IT operations. Since then, Cliff has had the great fortune to work with and learn from some of the best people in the industry including OccupyTheWeb and the fine people at No Starch during the production of this book. He is happily employed as a security consultant, doing everything from policy review to penetration tests. He feels lucky to have a career that is also his favorite hobby and a wife that supports him.



# BRIEF CONTENTS

Acknowledgments . . . . .	xix
Introduction . . . . .	xxi
Chapter 1: Getting Started with the Basics . . . . .	1
Chapter 2: Text Manipulation . . . . .	19
Chapter 3: Analyzing and Managing Networks . . . . .	29
Chapter 4: Adding and Removing Software . . . . .	39
Chapter 5: Controlling File and Directory Permissions. . . . .	49
Chapter 6: Process Management . . . . .	61
Chapter 7: Managing User Environment Variables. . . . .	71
Chapter 8: Bash Scripting . . . . .	81
Chapter 9: Compressing and Archiving . . . . .	93
Chapter 10: Filesystem and Storage Device Management. . . . .	101
Chapter 11: The Logging System . . . . .	111
Chapter 12: Using and Abusing Services . . . . .	121
Chapter 13: Becoming Secure and Anonymous. . . . .	139
Chapter 14: Understanding and Inspecting Wireless Networks . . . . .	153
Chapter 15: Managing the Linux Kernel and Loadable Kernel Modules . . . . .	165
Chapter 16: Automating Tasks with Job Scheduling . . . . .	173
Chapter 17: Python Scripting Basics for Hackers . . . . .	183
Index . . . . .	205





# 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 . . . . .	xxxix

<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

<b>5</b>		
<b>CONTROLLING FILE AND DIRECTORY PERMISSIONS</b>		<b>49</b>
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
<b>6</b>		
<b>PROCESS MANAGEMENT</b>		<b>61</b>
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
<b>7</b>		
<b>MANAGING USER ENVIRONMENT VARIABLES</b>		<b>71</b>
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**