

Python Ethical Hacking from Scratch

Think like an ethical hacker, avoid detection, and successfully develop, deploy, detect, and avoid malware

Fahad Ali Sarwar



BIRMINGHAM—MUMBAI

Python Ethical Hacking from Scratch

Copyright © 2021 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Wilson D'souza

Publishing Product Manager: Vijin Boricha

Senior Editor: Rahul D'souza

Content Development Editor: Nihar Kapadia

Technical Editor: Nithik Cheruvakodan

Copy Editor: Safis Editing

Project Coordinator: Shagun Saini

Proofreader: Safis Editing

Indexer: Manju Arasan

Production Designer: Jyoti Chauhan

First published: July 2021

Production reference: 1270521

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

ISBN 978-1-83882-950-6

www.packt.com

Contributors

About the author

Fahad Ali Sarwar teaches ethical hacking and penetration testing on different online platforms with a solid student base. He's passionate about cybersecurity and ethical hacking tool development.

Fahad is particularly enthusiastic about Python for its simplicity and ease of use, and in this book, he chose to focus on it due to the features it offers.

About the reviewers

Omar Ahmed specializes in application and network penetration testing. He has performed dozens of ethical hacking engagements for clients in a wide variety of industries, including government, finance, retail, and manufacturing. Omar has had unique opportunities to assess the security of new applications and technologies ranging from web-enabled e-business applications to proprietary applications.

His security career started in 2012, concentrating on network and application security. Omar has excelled in penetration testing, application assessments, social engineering (both physical and virtual), vulnerability assessments, and log analysis. You can reach out to him on Twitter at @mistspark.

Marquel Waites is a cyber analyst and military veteran, with 21 years of leadership experience in the United States Army and a future career goal of becoming a director of IT security (CISO). He has achieved measurable results while leading organizations of more than 100 people in dynamic, fast-paced environments. He possesses a comprehensive background in financial management operations, cybersecurity operations, incident response coordination, security analytics and monitoring, cybersecurity policy and technical compliance, and cybersecurity risk and vulnerability management. Marquel has managed risk on multiple lines to protect assets, property, and equipment valued at more than \$256M while exceeding the expectations of senior executive stakeholders. He is the recipient of multiple awards for outstanding performance and professionalism. His career is supported by a Bachelor of Science degree in information technology management from Trident University, a Master of Science degree in cybersecurity policy from Colorado Technical University, and a Master of Science in cybersecurity and cloud security architecture from EC Council University. He holds numerous certifications, including Certified Ethical Hacker, Certified Network Defense Architect, and Security+.

I would like to thank Packt for giving me the opportunity to review this book, and I hope this book helps everyone professionally. I would like to thank all the professors at EC Council University and the Coalfire team for continually inspiring me to become a better cybersecurity professional.

Table of Contents

Preface

Section 1: The Nuts and Bolts of Ethical Hacking – The Basics

1

Introduction to Hacking

What's all the fuss about hackers?	4	methodology	18
What is hacking?	5	Planning	19
Confidentiality	6	Reconnaissance	19
Integrity	8	Scanning	21
Availability	9	Identifying weaknesses	22
Becoming a successful hacker	10	Attacking and gaining access	22
Legality	12	Maintaining access	23
Types of hackers	12	Post exploitation	23
White hat hackers	12	Covering tracks	24
Black hat hackers	13	Reporting	24
Gray hat hackers	13	Careers in cybersecurity	26
Nation-state hackers	14	Systems security administration	26
Corporate spies	15	Security architect	26
Hacktivists	16	Penetration tester	26
Script kiddies	17	Forensic analyst	26
Hacking phases and		Chief information security officer	27
		Types of attacks	27
		System control	27

Social engineering	27	Phishing	28
Baiting	28	Summary	28

2

Getting Started – Setting Up a Lab Environment

Technical requirements	30	Integrated development environment	38
Setting up VirtualBox	30	Setting up networking	39
Installing virtual OSes	31	Updating Kali	40
Attack machine OS	31	Using virtual environments	40
Installing Python	36	Summary	43
Installing Python on Windows	36		
Installing Python on Kali Linux	37		

Section 2:
Thinking Like a Hacker – Network
Information Gathering and Attacks

3

Reconnaissance and Information Gathering

What is a computer network?	48	Local area network	53
Components of a basic computer network	50	Personal area network	54
Node	50	Metropolitan area networks	54
Server	50	Wide area network	55
Transmission media	50	Internet	55
Network interface card	50	Network stack	55
Hub	51	Introduction to OSI model	56
Switch	51	Complete cycle	58
Router	51	TCP/IP model	58
Gateway	51	Mapping the OSI and TCP/IP stack	59
Firewall	52	Network entities	60
Classifying network	53	Private IP address	60
		IPv4 versus IPv6	62

MAC address	62	Changing our MAC address	64
Ports	63	Creating a Python script	67
Protection	63	Summary	69

4

Network Scanning

Introduction to networking	71	Understanding how Scapy works	78
Data representation in digital systems	72	Network scanner using Scapy	86
Data encapsulation	73	Address Resolution Protocol	86
The packet delivery process	74	ARP scanner using Scapy	87
Introduction to Scapy	77	Summary	91
Installing Scapy	77		

5

Man in the Middle Attacks

Why do we need ARP?	94	Restoring ARP tables manually	106
ARP poisoning	94	Decrypting the network traffic	107
Building an ARP spoof program	98	HTTPS versus HTTP	107
Arp spoof project	99	Bypassing HTTPS	109
Monitoring traffic	105	Summary	114
Encrypted traffic	105		

Section 3: Malware Development

6

Malware Development

Understanding RATs	118	Socket programming in Python	119
Forward shell	118	Sockets	119
Reverse shell	119	Creating a socket in Python	120
		socket.socket() API	120

socket.bind() API	121	Creating malware	124
socket.listen() API	121	Hacker server	124
socket.accept() API	121	Victim's client	126
socket.connect()	122		
socket.send()	122	Running commands remotely	
Socket.recv()	122	on the victim's machine	129
socket.close()	122	Navigating directories	137
Fitting it altogether	123	Summary	139

7

Advanced Malware

Building a keylogger file		Uploading files to the victim	148
transfer	141	Taking screenshots	149
Downloading the victim file to the		Keylogger	151
hacker	142	Summary	156

8

Post Exploitation

Packaging the malware	157	Attack over a public IP	169
Understanding the pyinstaller library	158	Cracking passwords	170
Understanding trojans	162	Stealing passwords	172
Adding an icon to an executable	163	Creating botnets	174
Creating your own trojan	164	Summary	178

9

System Protection and Perseverance

Persistence system protection	180	Persistence	187
Intrusion detection systems	180	Summary	190
IDS detection mechanisms	181	Why subscribe?	191
Bypassing an IDS	183		

Other Books You May Enjoy

Index