Python Ethical Hacking from Scratch

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

Fahad Ali Sarwar

Packt

BIRMINGHAM—MUMBAI

Python Ethical Hacking from Scratch

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

2
Getting Started – Setting Up a Lab Environment

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

3
Reconnaissance and Information Gathering

4
Network Scanning

5
Man in the Middle Attacks

Section 3: Malware Development

6
Malware Development