O'REILLY

BOOK

Malware Development for Ethical Hackers

Write the first review

By **Zhassulan Zhussupov**

‹packt›
1ST EDITION
Malware Development for Ethical Hackers
Learn how to develop various types of malware to strengthen cybersecurity
ZHASSULAN ZHUSSUPOV

Start

TIME TO COMPLETE:
8h 8m

LEVEL:
Beginner

SKILLS:
Malware

PUBLISHED BY:

390 pages

+ Add to playlist

Packed with real-world examples, this book simplifies cybersecurity, delves into malware development, and serves as a must-read for advanced ethical hackers

Key Features

- Learn how to develop and program Windows malware applications using hands-on examples
- Explore methods to bypass security mechanisms and make malware undetectable on compromised systems
- Understand the tactics and tricks of real adversaries and APTs and apply their experience in your operations
- Purchase of the print or Kindle book includes a free PDF eBook

Book Description

Malware Development for Ethical Hackers is a comprehensive guide to the dark side of cybersecurity within an ethical context.

This book takes you on a journey through the intricate world of malware development, shedding light on the techniques and strategies employed by cybercriminals. As you progress, you'll focus on the ethical considerations that ethical hackers must uphold. You'll also gain practical experience in creating and implementing popular techniques encountered in real-world malicious applications, such as Carbanak, Carberp, Stuxnet, Conti, Babuk, and BlackCat ransomware. This book will also equip you with the knowledge and skills you need to understand and details of programming, evasion techniques, persistence mechanisms, and more.

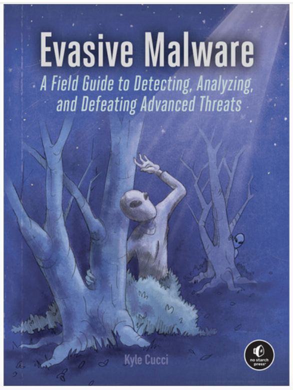
What you will learn

- Familiarize yourself with the logic of real malware developers for cybersecurity
- Get to grips with the development of malware over the years using examples
- Understand the process of reconstructing APT attacks and their techniques
- Design methods to bypass security mechanisms for your red team scenarios
- Explore over 80 working examples of malware
- Get to grips with the close relationship between mathematics and modern malware

Who this book is for

This book is for penetration testers, exploit developers, ethical hackers, red teamers, and offensive security researchers. Anyone interested in cybersecurity and ethical hacking will also find this book helpful. Familiarity with core ethical hacking and cybersecurity concepts will help you understand the topics discussed in this book more easily.

You might also like


Evasive Malware
A Field Guide to Detecting, Analyzing, and Defeating Advanced Threats
Kyle Cucci

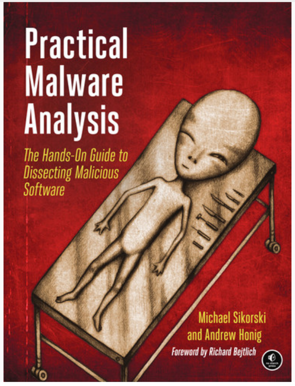
With ACI Learning, Daniel Lowrie and Sophie Goodwin

The course begins with fundamental cybersecurity con-... cepts, paving the way for an extensive

the skills to manage cyber threats efficiently. The course shifts its focus to advanced concepts such as the MITRE ATT&CK Framework, the Diamond Model and the CEH Hacking Methodol

We're all aware of Stuxnet, ShadowHammer,... Sunburst, and similar attacks that use evasion to remain hidden while defending themselves from

static and dynamic code analysis to uncover malware's true intentions, you'll learn how malware weaponizes context awareness to detect and skirt virtual machines and sandboxes, plus the vari-

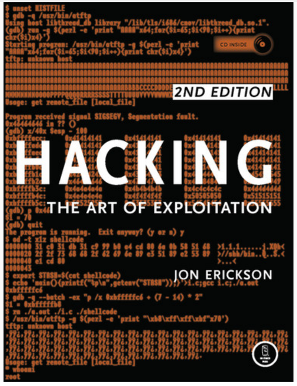

Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich

BOOK

Practical Malware Analysis

By Michael Sikorski and Andrew Honig

For those who want to stay ahead of the latest malware,... Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way.



BOOK

Hacking: The Art of Exploitation, 2nd... Edition

By Jon Erickson

Hacking is the art of creative problem solving, whether th... means finding an unconventional solution to a difficult problem or exploiting holes in sloppy programming. Many people call themselves hackers, but few have the strong technical foundation needed to really push the envelope. Rather than merely showing how

About the Publisher

Packt helps real-world developers put software to work in new ways with over 7,500 practical books and videos covering over 1,000 technologies. With coverage ranging from introductory programming to new and emerging technologies, as well as expert advice from

More about Packt Publishing

ances of threat hunting, incident handling, and the role of machine learning and AI in cybersecurity. The course also addresses critical aspects of network and web security, including various scanning and enumeration techniques, vulnerability assessments, and countermeasures against common cyber threats. You'll also delve into specialized areas like mobile, IoT, and cloud security. The course concludes with an emphasis on the latest standards and regulations in cybersecurity, preparing you for the CEH certification and real-world cybersecurity challenges. What you will learn Navigate ethical hacking methodologies and frameworks Conduct comprehensive network and web security assessments Develop skills in mobile, IoT, and

sembly methods and debugging interference to covert code execution and misdirection tactics. You'll also delve into defense evasion, from process injection and rootkits to fileless malware. Finally, you'll dissect encoding, encryption, and the complexities of malware obfuscators and packers to uncover the evil within. You'll learn how malware: Abuses legitimate components of Windows, like the Windows API and LOLBins, to run undetected Uses environmental quirks and context awareness, like CPU timing and hypervisor enumeration, to detect attempts at analysis Bypasses network and endpoint defenses using passive circumvention techniques, like obfuscation and mutation, and active techniques, like unhooking and tampering

work. To share the art and science of hacking in a way that is accessible to everyone, Hacking: The Art of Exploitation, 2nd Edition introduces the fundamentals of C programming from a hacker's perspective. The included LiveCD provides a complete Linux programming and debugging environment-all without modifying your current operating system. Use it to follow along with the book's examples as you fill gaps in your knowledge and explore hacking techniques on your own. Get your hands dirty debugging code, overflowing buffers, hijacking network communications, bypassing protections, exploiting cryptographic weaknesses, and perhaps even inventing new exploits. This book will teach you how to: Program computers and analyze various cyber-attack classifications Implement effective threat hunting and incident management Audience This Certified Ethical Hacker course is designed to strengthen the practical knowledge of security officers, auditors, site administrators, and any professional focused on network security. It's an excellent fit for those responsible for safeguarding network infrastructure and keen to deepen their understanding of ethical hacking. About the Authors ACI Learning: ACI Learning trains leaders in Cybersecurity, Audit, and Information Technology. Whether starting an IT career, mastering a profession, or developing a team, they provide essential support at every step. Daniel Lowrie: Daniel

building a malware analysis lab and tuning it to better counter anti-analysis techniques in malware. Whether you're a frontline defender, a forensic analyst, a detection engineer, or a researcher, Evasive Malware will arm you with the knowledge and skills you need to outmaneuver the stealthiest of today's cyber adversaries.

buffer overflows and format strings Inspect processor registers and system memory with a debugger to gain a real understanding of what is happening Outsmart common security measures like nonexecutable stacks and intrusion detection systems Gain access to a remote server using port-binding or connect-back shellcode, and alter a server's logging behavior to hide your presence Redirect network traffic, conceal open ports, and hijack TCP connections Crack encrypted wireless traffic using the FMS attack, and speed up brute-force attacks using a password probability matrix Hackers are always pushing the boundaries, investigating the unknown, and evolving their art. Even if you don't already know how to program, Hacking:

tal in North-Central Florida. His journey led him to become an in-classroom trainer and Mentored Learning Instructor, specializing in courses covering Microsoft Windows Desktops and Servers, Active Directory, Networking, CCNA, and Linux. He then transitioned to becoming a Systems and Network administrator for a large insurance company before joining ACI Learning as an Edutainer. Certifications: CompTIA A+, Network+, Linux+, CySA+, and PenTest+; CEH; MCSA; CFR; eJPT Sophie Goodwin: Sophie Goodwin is a Voice-Over talent. Her background spans over eight years as a film and voice talent, with experience in eLearning content, independent films, TV & web commercials,

chine architecture, network communications, and existing hacking techniques. Combine this knowledge with the included Linux environment, and all you need is your own creativity.

at the University of Florida. Apart from her work as an Edutainer, Sophie is also involved in other aspects of the entertainment industry. She is certified in (ISC)_ CC: Certified in Cybersecurity.