Hands-On Ethical Hacking Tactics : Strategies, Tools, and Techniques for Effective Cyber Defense /

Hartman, Shane,
author

Monografía

Detect and mitigate diverse cyber threats with actionable insights into attacker types, techniques, and efficient cyber threat hunting Key Features Explore essential tools and techniques to ethically penetrate and safeguard digital environments Set up a malware lab and learn how to detect malicious code running on the network Understand different attacker types, their profiles, and mindset, to enhance your cyber defense plan Purchase of the print or Kindle book includes a free PDF eBook Book Description If you're an ethical hacker looking to boost your digital defenses and stay up to date with the evolving cybersecurity landscape, then this book is for you. Hands-On Ethical Hacking Tactics is a comprehensive guide that will take you from fundamental to advanced levels of ethical hacking, offering insights into both offensive and defensive techniques. Written by a seasoned professional with 20+ years of experience, this book covers attack tools, methodologies, and procedures, helping you enhance your skills in securing and defending networks. The book starts with foundational concepts such as footprinting, reconnaissance, scanning, enumeration, vulnerability assessment, and threat modeling. Next, you'll progress to using specific tools and procedures for hacking Windows, Unix, web servers, applications, and databases. The book also gets you up to speed with malware analysis. Throughout the book, you'll experience a smooth transition from theoretical concepts to hands-on techniques using various platforms. Finally, you'll explore incident response, threat hunting, social engineering, IoT hacking, and cloud exploitation, which will help you address the complex aspects of ethical hacking. By the end of this book, you'll have gained the skills you need to navigate the ever-changing world of cybersecurity. What you will learn Understand the core concepts and principles of ethical hacking Gain hands-on experience through dedicated labs Explore how attackers leverage computer systems in the digital landscape Discover essential defensive technologies to detect and mitigate cyber threats Master the use of scanning and enumeration tools Understand how to hunt and use search information to identify attacks Who this book is for Hands-On Ethical Hacking Tactics is for penetration testers, ethical hackers, and cybersecurity enthusiasts looking to explore attack tools, methodologies, and procedures relevant to today's cybersecurity landscape. This ethical hacking book is suitable for a broad audience with varying levels of expertise in cybersecurity, whether you're a student or a professional looking for job opportunities, or just someone curious about the field

Título: Hands-On Ethical Hacking Tactics Strategies, Tools, and Techniques for Effective Cyber Defense Shane Hartman ; foreword by Ken Dunham

Edición: First edition

Editorial: Birmingham, England Packt Publishing Ltd. [2024] 2024

Descripción física: 1 online resource (464 pages)

Nota general: Description based upon print version of record

Bibliografía: Includes bibliographical references and index

Contenido: Cover -- Title Page -- Copyright and Credits -- Dedication -- Foreword -- Contributors -- Table of Contents -- Preface -- Part 1: Information Gathering and Reconnaissance -- Chapter 1: Ethical Hacking Concepts -- Technical requirements -- What is ethical hacking? -- Elements of information security -- Why do intrusions and attacks happen? -- Motive -- Means -- Opportunity -- Types and profiles of attackers and defenders -- Black hat hackers -- Script kiddies -- Hacktivists -- Cyber terrorists/cyber warriors -- Cyber criminals -- White hat hackers -- Attack targets and types -- Network -- Application -- Host -- The anatomy of an attack -- Reconnaissance -- Weaponization -- Delivery -- Exploitation -- Installation -- Command and control -- Actions on objectives -- Ethical hacking and penetration testing -- Defensive technologies -- Lab - setting up the testing lab -- Setting up VirtualBox -- Setting up Kali Linux -- Setting up vulnerable hosts -- Configuring the vulnerable Windows host -- Setting up the vulnerable Linux host -- Final checks -- Summary -- Assessment -- Answers -- Chapter 2: Ethical Hacking Footprinting and Reconnaissance -- Technical requirements -- What is footprinting and reconnaissance? -- Keeping inventory -- Web searches and Google hacks -- Exploring some useful Google hacks -- Preventing exploitation through Google searches -- WHOIS database records -- Accessing WHOIS information -- Understanding the name server entry -- Third-party sources of intel -- Sources for collecting intelligence -- Accessing hidden information -- Maltego -- GitHub and online forums -- SpiderFoot tool -- Dmitry -- Shodan -- Archived information -- Lab - Reconnaissance -- Summary -- Assessment -- Answer -- Chapter 3: Ethical Hacking Scanning and Enumeration -- Comparing scanning and enumeration -- Exploring scanning techniques -- Ping Ping at scale -- Traceroute -- Understanding service enumeration -- Introducing ports -- How do port scans work? -- Port scanning issues -- Scanning countermeasures -- Introducing the Nmap network scanning tool -- Controlling Nmap scan speeds -- Outputting results -- The NSE -- The Nmap GUI -- Mapping the network -- Lab - Scanning and enumeration -- Summary -- Assessment -- Answer -- Chapter 4: Ethical Hacking Vulnerability Assessments and Threat Modeling -- Vulnerability assessment concepts -- Explaining vulnerability assessments -- Types of vulnerability assessments -- Vulnerability assessment life cycle -- Vulnerability scanning tools -- Introducing the Nessus vulnerability scanner -- Best practices for vulnerability assessments -- Vulnerability assessment reports -- The elements of threat modeling -- The finding -- The kill chain -- The single asset value -- The organizational asset value -- The estimated risk -- Threat modeling frameworks -- STRIDE -- PASTA -- VAST -- Attack trees -- CVSS -- Threat modeling tools -- Threat forecasting -- Phase 1 - Research -- Phase 2 - Implementation and analysis -- Phase 3 - Information sharing and building -- Threat model lab - personal computer security -- Summary -- Assessment -- Answer -- Part 2: Hacking Tools and Techniques -- Chapter 5: Hacking the Windows Operating System -- Technical requirements -- Exploiting the Windows OS -- Exploiting Windows device drivers -- Exploiting Windows networking -- Address Resolution Protocol -- Simple network management protocol -- Server Message Block -- NetBIOS -- Exploiting Windows authentication -- User authentication and movement -- Obtaining and extracting passwords -- Exploring password-cracking techniques -- Authentication spoofing -- Pulling Windows account names via null sessions -- Tools for pulling account names via null sessions -- Privilege elevation Exploiting Windows services and applications -- Server-side exploits -- Client-side exploits -- Exploring the Windows Registry -- Windows Registry exploitation -- Exploiting the Windows logs -- Summary -- Lab -- Brute force password crack -- Rainbow table crack -- Assessment -- Answers -- Chapter 6: Hacking the Linux Operating System -- Exploiting the Linux operating system -- Exploring the Linux filesystem -- Exploiting the filesystem -- Linux hidden files -- Important files -- Exploiting Linux networking -- Exploiting Linux authentication -- Cracking passwords -- Linux updates and patching -- The Linux logging system -- Exploiting the Linux kernel -- Checking your kernel version -- Exploiting the kernel -- Lab -- Summary -- Assessment -- Answers -- Chapter 7: Ethical Hacking of Web Servers -- Web servers' architecture, configuration, and vulnerabilities -- Adding processing logic -- Threats, vulnerabilities, and exploits to web services -- Web server authentication --

Basic authentication -- OAuth -- Some real-world web servers and ways to combat attacks -- IIS hardening tasks -- Apache web server hardening tasks -- Types of web server/website attacks -- Website defacement -- DoS/DDoS attack -- HTTP response-splitting attack -- Cross-Site Request Forgery -- Deep linking -- Directory traversal attack -- Man-in-the-Middle/sniffing attack -- Cookie tampering -- Cookie-based session attacks -- Session hijacking -- DNS -- Lab -- Summary -- Assessment -- Answer -- Chapter 8: Hacking Databases -- Finding databases on the network -- Discovering databases on the network -- Mitigating database discovery -- Exploring databases and database structures -- Database threats and vulnerabilities -- Network-based database attacks -- Database engine faults and bugs -- Brute-force attacks on weak or default passwords -- Misconfigurations -- Remote code execution Indirect attacks -- Hidden database servers -- Accessible backups -- Privilege escalation -- Insecure system architecture -- Database server password cracking -- Methods of attacking database servers -- Scanning for vulnerabilities -- Attacking the System Administrator account -- Exploit module attacks -- Google hacks -- Perusing website source code -- SQL replay attack -- Protecting databases -- Hidden or unknown databases -- How insecure databases are created -- Weak auditing and insufficient logging -- Lab - Database hacking -- Setup -- Exercise 1 -- Exercise 2 -- Summary -- Assessment -- Answer -- Chapter 9: Ethical Hacking Protocol Review -- Exploring communication protocols -- Introducing the OSI model -- Introducing IP -- Introducing TCP -- The three-way handshake -- UDP -- ICMP -- Comparing TCP and UDP -- Well-known ports -- Understanding protocol attacks -- TCP attacks -- UDP attacks -- ICMP attacks -- An overview of IPv6 -- The setup and configuration of IPv6 -- Reconnaissance and attack tools -- Defending IPv4 networks -- Defending IPv6 networks -- Lab -- Exercise 1 -- Exercise 2 -- Summary -- Assessment -- Answers -- Chapter 10: Ethical Hacking for Malware Analysis -- Technical requirements -- Why does malware exist and who are its sources? -- Exploring types of malware -- Virus -- Worms -- Trojans -- Ransomware -- Bots/botnets -- Adware -- Spyware -- Malvertising -- Fileless malware -- Backdoors -- Rootkits -- How does malware get onto machines? -- Analyzing a sample -- Setting up a malware analysis lab -- Static analysis -- Dynamic analysis -- Detecting malware and removing it -- Perimeter monitoring -- Malware prevention -- Summary -- Lab -- Assessment -- Answers -- Part 3: Defense, Social Engineering, IoT, and Cloud -- Chapter 11: Incident Response and Threat Hunting -- What is an incident? -- The incident response plan The incident response process -- The preparation phase -- Detection phase -- Analysis phase -- Containment and eradication phase -- Recovery phase -- Post-incident activities (postmortem) -- Information sharing and coordination -- Incident response team structure -- Introducing indicators of incidents -- Types of indicators -- IOC tools -- Introducing threat hunting -- Threat hunting tools -- Getting Started with the Threat hunting process -- Best practices for threat hunting -- Practical aspects of threat hunting -- Lab: Security incident response simulation -- Exercise 2: Threat Hunt -- Summary -- Assessment -- Answers -- Chapter 12: Social Engineering -- Introducing social engineering -- Phases of a social engineering attack -- Social engineering attack techniques -- Physical-based social engineering -- Electronic-based social engineering -- Social engineering tools -- Social-Engineer Toolkit -- Browser Exploitation Framework -- Social engineering defenses -- Protecting businesses' strategies -- Protecting businesses' policies and practices -- Protecting individuals -- The impact of AI on social engineering -- Lab -- Activities -- Summary -- Assessment -- Answers -- Chapter 13: Ethical Hacking of the Internet of Things -- What is IoT? -- Understanding IoT communication -- IoT communication layers -- IoT communication models -- IoT communication protocols -- Attack vectors for IoT devices -- Access control -- Firmware attacks -- Web attacks -- Network service/communication protocol attacks -- Unencrypted local data storage -- Confidentiality and integrity issues -- Cloud computing attacks -- Malicious updates -- Insecure APIs -- Mobile application threats -- Other attacks -- An IoT hacking methodology -- Understanding OT -- An OT hacking methodology -- Best practices for securing IoT/OT -- Lab - discovering IoT devices -- Summary -- Assessment Answers

ISBN: 1-80181-865-7

Materia: Penetration testing (Computer security) Piratas informáticos

Autores: Dunham, Ken, writer of foreword

Enlace a formato físico adicional: 1-80181-008-7

Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid

- (+34) 91 456 03 60
- informa@baratz.es