PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CEH

Certified Ethical Hacker

MICHAEL GREGG
OMAR SANTOS

Special Offer

Save 80% on Premium Edition eBook and Practice Test

The *CEH Certified Ethical Hacker Cert Guide Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.

CEH Certified Ethical Hacker Cert Guide

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Table of Contents

Introduction

Chapter 1 An Introduction to Ethical Hacking

- Do I Know This Already? Quiz
- Foundation Topics
- Security Fundamentals
  - Goals of Security
  - Risk, Assets, Threats, and Vulnerabilities
  - Backing Up Data to Reduce Risk
  - Defining an Exploit
  - Risk Assessment
- Security Testing
  - No-Knowledge Tests (Black Box)
  - Full-Knowledge Testing (White Box)
  - Partial-Knowledge Testing (Gray Box)
  - Types of Security Tests
  - Incident Response
- Cyber Kill Chain
- Hacker and Cracker Descriptions

Table of Contents

Who Attackers Are

Ethical Hackers

Required Skills of an Ethical Hacker

Modes of Ethical Hacking

Test PlansKeeping It Legal

Test Phases

Establishing Goals

Getting Approval

Ethical Hacking Report

Vulnerability Research and Bug BountiesKeeping Up with Changes

Ethics and Legality

Overview of U.S. Federal Laws

Compliance Regulations

Payment Card Industry Data Security Standard (PCI-DSS)

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Exercises

1-1 Searching for Exposed Passwords

1-2 Examining Security Policies

Review Questions

Suggested Reading and Resources

Chapter 2 The Technical Foundations of Hacking

Do I Know This Already? Quiz

Foundation Topics

The Hacking Process

Performing Reconnaissance and Footprinting

Table of Contents

- Scanning and Enumeration
- Gaining Access
- Escalating Privilege
- Maintaining Access
- Covering Tracks and Planting Backdoors

The Ethical Hackers Process

- NIST SP 800-115
- Operationally Critical Threat, Asset, and Vulnerability Evaluation
- Open Source Security Testing Methodology Manual

Information Security Systems and the Stack

- The OSI Model
- Anatomy of TCP/IP Protocols
- The Application Layer
- The Transport Layer
- Transmission Control Protocol
- User Datagram Protocol
- The Internet Layer
- Traceroute
- The Network Access Layer

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Exercises

- 2-1 Install a Sniffer and Perform Packet Captures
- 2-2 Using Traceroute for Network Troubleshooting

Review Questions

Suggested Reading and Resources

Table of Contents

Chapter 3 Footprinting, Reconnaissance, and Scanning

- Do I Know This Already? Quiz
- Foundation Topics
- Footprinting
  - Footprinting Methodology
  - Documentation
  - Footprinting Through Search Engines
  - Footprinting Through Social Networking Sites
  - Footprinting Through Web Services and Websites
  - Email Footprinting
  - Whois Footprinting
  - DNS Footprinting
  - Network Footprinting
  - Subnettings Role in Mapping Networks
  - Traceroute
  - Footprinting Through Social Engineering
  - Footprinting Countermeasures
- Scanning
  - Host Discovery
  - Port and Service Discovery
  - Nmap
  - SuperScan
  - THC-Amap
  - Hping
  - Port Knocking
  - OS Discovery (Banner Grabbing/OS Fingerprinting) and Scanning Beyond IDS and Firewall
  - Active Fingerprinting Tools
  - Fingerprinting Services

Table of Contents

Default Ports and Services

Finding Open Services

Draw Network Diagrams

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Exercises

3-1 Performing Passive Reconnaissance

3-2 Performing Active Reconnaissance

Review Questions

Suggested Reading and Resources

Chapter 4 Enumeration and System Hacking

Do I Know This Already? Quiz

Foundation Topics

Enumeration

Windows Enumeration

Windows Security

NetBIOS and LDAP Enumeration

NetBIOS Enumeration Tools

SNMP Enumeration

Linux/UNIX Enumeration

NTP Enumeration

SMTP Enumeration

Additional Enumeration Techniques

DNS Enumeration

Enumeration Countermeasures

System Hacking

Table of Contents

Nontechnical Password Attacks

Technical Password Attacks

Password Guessing

Automated Password Guessing

Password Sniffing

Keylogging

Escalating Privilege and Exploiting Vulnerabilities

Exploiting an Application

Exploiting a Buffer Overflow

Owning the Box

Windows Authentication Types

Cracking Windows Passwords

Linux Authentication and Passwords

Cracking Linux Passwords

Hiding Files and Covering Tracks

Rootkits

File Hiding

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Exercise

4-1 NTFS File Streaming

Review Questions

Suggested Reading and Resources

Chapter 5 Social Engineering, Malware Threats, and Vulnerability Analysis

Do I Know This Already? Quiz

Table of Contents

Foundation Topics

Social Engineering

- Phishing
- Pharming
- Malvertising
- Spear Phishing
- SMS Phishing
- Voice Phishing
- Whaling
- Elicitation, Interrogation, and Impersonation (Pretexting)
- Social Engineering Motivation Techniques
- Shoulder Surfing and USB Baiting

Malware Threats

- Viruses and Worms
- Types and Transmission Methods of Viruses and Malware
- Virus Payloads
- History of Viruses
- Well-Known Viruses and Worms
- Virus Creation Tools
- Trojans
- Trojan Types
- Trojan Ports and Communication Methods
- Trojan Goals
- Trojan Infection Mechanisms
- Effects of Trojans
- Trojan Tools
- Distributing Trojans
- Wrappers
- Packers

Table of Contents

- Droppers
- Crypters
- Ransomware
- Covert Communications
- Tunneling via the Internet Layer
- Tunneling via the Transport Layer
- Tunneling via the Application Layer
- Port Redirection
- Keystroke Logging and Spyware
- Hardware Keyloggers
- Software Keyloggers
- Spyware
- Malware Countermeasures
- Detecting Malware
- Antivirus
- Analyzing Malware
- Static Analysis
- Dynamic Analysis

Vulnerability Analysis

- Passive vs. Active Assessments
- External vs. Internal Assessments
- Vulnerability Assessment Solutions
- Tree-Based vs. Inference-Based Assessments
- Vulnerability Scoring Systems
- Vulnerability Scanning Tools

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Table of Contents

Command Reference to Check Your Memory

Exercises

- 5-1 Finding Malicious Programs
- 5-2 Using Process Explorer

Review Questions

Suggested Reading and Resources

Chapter 6 Sniffers, Session Hijacking, and Denial of Service

Do I Know This Already? Quiz

Foundation Topics

Sniffers

- Passive Sniffing
- Active Sniffing
- Address Resolution Protocol
- ARP Poisoning and MAC Flooding
- Tools for Sniffing and Packet Capturing
- Wireshark
- Other Sniffing Tools
- Sniffing and Spoofing Countermeasures

Session Hijacking

- Transport Layer Hijacking
- Identify and Find an Active Session
- Predict the Sequence Number
- Take One of the Parties Offline
- Take Control of the Session
- Application Layer Hijacking
- Session Sniffing
- Predictable Session Token ID
- On-Path Attacks
- Client-Side Attacks

Table of Contents

        - Browser-Based On-Path Attacks
        - Session Replay Attacks
        - Session Fixation Attacks
        - Session Hijacking Tools
        - Preventing Session Hijacking
    - Denial of Service and Distributed Denial of Service
        - DoS Attack Techniques
        - Volumetric Attacks
        - SYN Flood Attacks
        - ICMP Attacks
        - Peer-to-Peer Attacks
        - Application-Level Attacks
        - Permanent DoS Attacks
        - Distributed Denial of Service
        - DDoS Tools
        - DoS and DDoS Countermeasures
    - Summary
    - Exam Preparation Tasks
    - Review All Key Topics
    - Define Key Terms
    - Exercises
        - 6-1 Scanning for DDoS Programs
        - 6-2 Spoofing Your MAC Address in Linux
        - 6-3 Using the KnowBe4 SMAC to Spoof Your MAC Address
    - Review Questions
    - Suggested Reading and Resources
- Chapter 7 Web Server Hacking, Web Applications, and Database Attacks

Table of Contents

Do I Know This Already? Quiz

Foundation Topics

Web Server Hacking

- The HTTP Protocol
- Scanning Web Servers
- Banner Grabbing and Enumeration
- Web Server Vulnerability Identification
- Attacking the Web Server
- DoS/DDoS Attacks
- DNS Server Hijacking and DNS Amplification Attacks
- Directory Traversal
- On-Path Attacks
- Website Defacement
- Web Server Misconfiguration
- HTTP Response Splitting
- Understanding Cookie Manipulation Attacks
- Web Server Password Cracking
- Web ServerSpecific Vulnerabilities
- Comments in Source Code
- Lack of Error Handling and Overly Verbose Error Handling
- Hard-Coded Credentials
- Race Conditions
- Unprotected APIs
- Hidden Elements
- Lack of Code Signing
- Automated Exploit Tools
- Securing Web Servers
- Harden Before Deploying
- Patch Management
- Disable Unneeded Services

Table of Contents

Lock Down the File System
Log and Audit
Provide Ongoing Vulnerability Scans
Web Application Hacking
Unvalidated Input
Parameter/Form Tampering
Injection Flaws
Cross-Site Scripting (XSS) Vulnerabilities
Reflected XSS Attacks
Stored XSS Attacks
DOM-Based XSS Attacks
XSS Evasion Techniques
XSS Mitigations
Understanding Cross-Site Request Forgery Vulnerabilities and Related Attacks
Understanding Clickjacking
Other Web Application Attacks
Exploiting Web-Based Cryptographic Vulnerabilities and Insecure Configurations
Web-Based Password Cracking and Authentication Attacks
Understanding What Cookies Are and Their Use
URL Obfuscation
Intercepting Web Traffic
Securing Web Applications
Lack of Code Signing
Database Hacking
A Brief Introduction to SQL and SQL Injection
SQL Injection Categories
Fingerprinting the Database
Surveying the UNION Exploitation Technique
Using Boolean in SQL Injection Attacks

Table of Contents

    - Understanding Out-of-Band Exploitation
    - Exploring the Time-Delay SQL Injection Technique
    - Surveying Stored Procedure SQL Injection
    - Understanding SQL Injection Mitigations
    - SQL Injection Hacking Tools
  - Summary
  - Exam Preparation Tasks
  - Review All Key Topics
  - Exercise
    - 7-1 Complete the Exercises in WebGoat
  - Review Questions
  - Suggested Reading and Resources
- Chapter 8 Wireless Technologies, Mobile Security, and Attacks
  - Do I Know This Already? Quiz
  - Foundation Topics
  - Wireless and Mobile Device Technologies
    - Mobile Device Concerns
    - Mobile Device Platforms
    - Android
    - iOS
    - Windows Mobile Operating System
    - BlackBerry
    - Mobile Device Management and Protection
    - Bluetooth
    - Radio Frequency Identification (RFID) Attacks
  - Wi-Fi
    - Wireless LAN Basics
    - Wireless LAN Frequencies and Signaling

Table of Contents

- Wireless LAN Security
- Installing Rogue Access Points
- Evil Twin Attacks
- Deauthentication Attacks
- Attacking the Preferred Network Lists
- Jamming Wireless Signals and Causing Interference
- War Driving
- Attacking WEP
- Attacking WPA
- Wireless Networks Configured with Open Authentication
- KRACK Attacks
- Attacks Against WPA3
- Attacking Wi-Fi Protected Setup (WPS)
- KARMA Attack
- Fragmentation Attacks
- Additional Wireless Hacking Tools
- Performing GPS Mapping
- Wireless Traffic Analysis
- Launch Wireless Attacks
- Crack and Compromise the Wi-Fi Network
- Securing Wireless Networks
- Site Survey
- Robust Wireless Authentication
- Misuse Detection

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Table of Contents

Suggested Reading and Resources

Chapter 9 Evading IDS, Firewalls, and Honeypots

Do I Know This Already? Quiz

Foundation Topics

Intrusion Detection and Prevention Systems

IDS Types and Components

Pattern Matching

Protocol Analysis

Heuristic-Based Analysis

Anomaly-Based Analysis

Global Threat Correlation Capabilities

Snort

IDS Evasion

Flooding

Insertion and Evasion

Session Splicing

Shellcode Attacks

Other IDS Evasion Techniques

IDS Evasion Tools

Firewalls

Firewall Types

Network Address Translation

Packet Filters

Application and Circuit-Level Gateways

Stateful Inspection

Identifying Firewalls

Bypassing Firewalls

Honeypots

Types of Honeypots

Table of Contents

Detecting Honeypots

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Suggested Reading and Resources

Chapter 10 Cryptographic Attacks and Defenses

Do I Know This Already? Quiz

Foundation Topics

Cryptography History and Concepts

Encryption Algorithms

Symmetric Encryption

Data Encryption Standard (DES)

Advanced Encryption Standard (AES)

Rivest Cipher

Asymmetric Encryption (Public Key Encryption)

RSA

Diffie-Hellman

ElGamal

Elliptic-Curve Cryptography (ECC)

Digital Certificates

Public Key Infrastructure

Trust Models

Single-Authority Trust

Hierarchical Trust

Web of Trust

Email and Disk Encryption

Table of Contents

- Cryptoanalysis and Attacks
  - Weak Encryption
  - Encryption-Cracking Tools
- Security Protocols and Countermeasures
  - Steganography
  - Steganography Operation
  - Steganographic Tools
  - Digital Watermark
  - Hashing
  - Digital Signature
- Summary
- Exam Preparation Tasks
- Review All Key Topics
- Define Key Terms
- Exercises
  - 10-1 Examining an SSL Certificate
  - 10-2 Using PGP
  - 10-3 Using a Steganographic Tool to Hide a Message
- Review Questions
- Suggested Reading and Resources

Chapter 11 Cloud Computing, IoT, and Botnets

- Do I Know This Already? Quiz
- Foundation Topics
- Cloud Computing
  - Cloud Computing Issues and Concerns
  - Cloud Computing Attacks
  - Cloud Computing Security
  - DevOps, Continuous Integration (CI), Continuous Delivery (CD), and DevSecOps

Table of Contents

CI/CD Pipelines

Serverless Computing

Containers and Container Orchestration

How to Scan Containers to Find Security Vulnerabilities

IoT

IoT Protocols

IoT Implementation Hacking

Botnets

Botnet Countermeasures

Summary

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Suggested Reading and Resources

Chapter 12 Final Preparation

Hands-on Activities

Suggested Plan for Final Review and Study

Summary

Glossary of Key Terms

A

B

C

D

E

F

G

Table of Contents

H

I

J-K

L

M

N

O

P

Q

R

S

T

U

V

W-Z

Appendix A: Answers to the Do I Know This Already? Quizzes and Review Questions

Appendix B: CEH Certified Ethical Hacker Cert Guide Exam Updates

Appendix C: Study Planner

Index

Pearson