CompTIA PenTest+ (PT0-001)

Security concepts, tools, and best-practice frameworks

A practical, student-friendly outline covering the Pen Test Engagement, passive Reconnaissance, active Reconnaissance, physical Security, and social Engineering.

MODULES
21

LESSONS
215

FORMAT
Self-paced

Module Breakdown

MODULE 1

The Pen Test Engagement

1.0 PenTest Plus Introduction
1.1 PenTest Plus Topics
1.2 PenTest Engagement
1.3 Threat Modeling
1.4 Technical Constraints
1.5 PenTest Engagement Review
1.6 Examining PenTest Engagement Documents Act

MODULE 2

Passive Reconnaissance

2.1 Passive Reconnaissance part1
2.2 WHOIS Act
2.3 Passive Reconnaissance part2
2.4 Google Hacking Act
2.5 Passive Reconnaissance part3
2.6 DNS Querying Act
2.7 Passive Reconnaissance part4
2.8 Email Server Querying Act
2.9 SSL-TLS Cerfificates
2.10 Shodan Act
2.11 The Havester
2.12 TheHarvester Act
2.13 Recon-ng
2.14 Recon-g Act
2.14 Recon-ng-Part-2-API-key Act
2.15 Maltego
2.16 Have I been Pwned
2.17 Punked and Owned Pwned Act

Module Breakdown (continued)

MODULE 2

Passive Reconnaissance (continued)

2.18 Fingerprinting Organization with Collected Archives
2.19 FOCA Act
2.20 Findings Analysis Weaponization
2.21 Chp 2 Review

MODULE 3

Active Reconnaissance

3.1 Active Reconnaissannce
3.2 Discovery Scans Act
3.3 Nmap
3.4 Nmap Scans Types Act
3.5 Nmap Options
3.6 Nmap Options Act
3.7 Stealth Scans
3.8 Nmap Stealth Scans Act
3.9 Full Scans
3.10 Full Scans Act
3.11 Packet Crafting
3.12 Packet Crafting Act
3.13 Network Mapping
3.14 Metasploit
3.15 Scanning with Metasploit Act
3.16 Enumeration
3.17 Banner Grabbing Act
3.18 Windows Host Enumeration

MODULE 3

Active Reconnaissance (continued)

3.19 Winddows Host Enumeration Act
3.20 Linux Host Enumeration
3.21 Linux Host Enumeration Act
3.22 Service Enumeration
3.23 Service Enumeration Act
3.24 Network Shares
3.25 SMB Share Enumeration Act
3.26 NFS Network Share Enumeration
3.27 NFS Share Enumeration Act
3.28 Null Sessions
3.29 Null Sessions Act
3.30 Website Enumeration
3.31 Website Enumeration Act
3.32 Vulnerability Scans
3.33 Compliance Scans Act
3.34 Credentialed Non-credentialed Scans
3.35 Using Credentials in Scans Act
3.36 Server Service Vulnerability Scan

MODULE 3

Active Reconnaissance (continued)

3.37 Vulnerability Scanning Act
3.38 Web Server Database Vulnerability Scan
3.39 SQL Vulnerability Scanning Act
3.40 Vulnerability Scan Part 2 OpenVAS Act
3.41 Web App Vulnerability Scan
3.42 Web App Vulnerability Scanning Act
3.43 Network Device Vulnerability Scan
3.44 Network Device Vuln Scanning Act
3.45 Nmap Scripts
3.46 Using Nmap Scripts for Vuln Scanning Act
3.47 Packet Crafting for Vulnerbility Scans
3.48 Firewall Vulnerability Scans
3.49 Wireless Access Point Vunerability
3.50 Wireless AP Scans Act
3.51 WAP Vulnerability Scans
3.52 Container Security issues
3.53 How to Update Metasploit Pro Expired Trial License

MODULE 4

Physical Security

4.1 Physical Security
4.2 Badge Cloning Act
4.3 Physical Security Review

MODULE 5

Social Engineering

5.1 Social Engineering
5.2 Using Baited USB Stick Act
5.3 Using Social Enginnering to Assist Attacks
5.4 Phishing Act
5.5 Social Engineering Review

Module Breakdown (continued)

MODULE 6

Vulnerability Scan Analysis

6.1 Vulnerbility Scan Analysis
6.2 Validating Vulnerability Scan Results Act
6.3 Vulnerbility Scan Analysis Review

MODULE 7

Password Cracking

7.1 Password Cracking
7.2 Brute Force Attack Against Network Service Act
7.3 Network Authentication Interception Attack
7.4 Intercepting Network Authentication Act
7.5 Pass the Hash Attacks
7.6 Pass the Hash Act
7.7 Password Cracking Review

MODULE 8

Penetrating Wired Networks

8.1 Penetrating Wired Network
8.2 Sniffing Act
8.3 Eavesdropping
8.4 Eavesdropping Act
8.5 ARP Poisoning
8.6 ARP Poisoning Act
8.7 Man In The Middle
8.8 MITM Act
8.9 TCP Session HiJacking
8.10 Server Message Blocks SMB Exploits
8.11 SMB Attack Act
8.12 Web Server Attacks
8.13 FTP Attacks
8.14 Telnet Server Attacks
8.15 SSH Server Attacks
8.16 Simple Network Mgmt Protocol SNMP
8.17 Simple Mail Transfer Protocol SMTP
8.18 Domain Name System DNS Cache Poisoning

MODULE 8

Penetrating Wired Networks (continued)

8.19 Denail of Service Attack DoS-DDoS
8.20 DoS Attack Act
8.21 VLAN Hopping Review

MODULE 9

Penetrating Wireless Networks

9.1 Penetrating Wireless Networks
9.2 Jamming Act
9.3 Wireless Sniffing
9.4 Replay Attacks
9.5 WEP Cracking Act
9.6 WPA-WPA2 Cracking
9.7 WAP Cracking Act
9.8 Evil Twin Attacks
9.9 Evil Twin Attack Act
9.10 WiFi Protected Setup
9.11 Bluetooth Attacks
9.12 Penetrating Wireless Networks

MODULE 10

Windows Exploits

10.1 Windows Exploits
10.2 Dumping Stored Passwords Act
10.3 Dictionary Attacks
10.4 Dictionary Attack Against Windows Act
10.5 Rainbow Table Attacks
10.6 Credential Brute Force Attacks
10.7 Keylogging Attack Act
10.8 Windows Kernel
10.9 Kernel Attack Act
10.10 Windows Components
10.11 Memory Vulnerabilities
10.12 Buffer Overflow Attack Act
10.13 Privilegde Escalation in Windows
10.14 Windows Accounts
10.15 Net and WMIC Commands
10.16 Sandboxes

Module Breakdown (continued)

MODULE 11

Linux Exploits

11.1 Linux Exploits
11.2 Exploiting Common Linux Features Act
11.3 Password Cracking in Linux
11.4 Cracking Linux Passwords Act
11.5 Vulnerability Linux
11.6 Priviledge Escalation Linux
11.7 Linux Accounts
11.8 Linux Exploits Review

MODULE 12

Mobile Devices

12.1 Mobile Devices
12.2 Hacking Android Act
12.3 Apple Exploits
12.4 Moblie Devices Review

MODULE 13

Specialized Systems

13.1 Specialized Systems
13.2 Specialized Systems Review

MODULE 14

Scripts

14.1 Scripts
14.2 Powershell
14.3 Python
14.4 Ruby
14.5 Common Scripting Elements
14.6 Scripts Review
14.7 Better Ping Sweep
14.8 Simple Port Scanner2
14.9 Multitarget Port Scanner
14.10 Port Scanner with Nmap
14.11 Scripts Review

MODULE 15

Application Testing

15.1 Application Testing
15.2 Reverse Engineering

MODULE 16

Web App Exploits

16.1 Webb App Exploits
16.2 Injection Attacks
16.3 HTML Injection
16.4 SQL Hacking - SQLmap Act
16.5 Cross-Site Attacks
16.6 Cross-Site Request Forgery
16.7 Other Web-based Attacks
16.8 File Inclusion Attacks
16.9 Web Shells
16.10 Web Shells Review

Module Breakdown (continued)

MODULE 17

Lateral Movement

17.1 Lateral Movement
17.2 Lateral Movement with Remote Mgmt Services
17.3 Process Migration Act
17.4 Passing Control Act
17.5 Pivoting
17.6 Tools the Enable Pivoting
17.7 Lateral Movement Review

MODULE 18

Persistence

18.1 Persistence
18.2 Breeding RATS Act
18.3 Bind and Reverse Shells
18.4 Bind Shells Act
18.5 Reverse Shells
18.6 Reverse Shells Act
18.7 Netcat
18.8 Netcat Act
18.9 Scheduled Tasks
18.10 Scheduled Tasks Act
18.11 Services and Domains
18.12 Persistence Review

MODULE 19

Cover Your Tracks

19.1 Cover Your Tracks
19.2 Cover Your Tracks - Timestomp Files Act
19.3 Cover Your Tracks - Frame the Administrator Act
19.4 Cover Your Tracks - Clear the Event Log Act
19.5 Cover Your Tracks Review

MODULE 20

The Report

20.1 The Report
20.2 The Report Review

MODULE 21

Post Engagement Cleanup

21.1 Post Engagement Cleanup_1
21.3 Post Engagement Cleanup Review
21.4 PenTest Plus Conclusion.mp4