Penetration Testing Tools

Learn essential penetration testing tools and techniques in this intermediate Penetration Testing training, designed for CompTIA PenTest+ certification. Master industry tools like Kali, network mappers, and password crackers to identify vulnerabilities, exploit targets, and strengthen security. This CompTIA course is ideal for security technicians and IT teams focused on network protection and penetration testing skills.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Pentesting Reconnaissance — 163 min.

Introduction to Pentesting Reconnaissance	5
Pentesting Reconnaissance Tools	9
Domain Information Tools	12
IP and DNS Information Tools	7
Combination OSINT Tools	8
Breach Data Tools	5
Pentesting Reconnaissance Review	3

Pentest Enumeration and NMAP

Overview	1
Intro to Pentesting Enumeration	9
Pentest Enumeration Tools	14
Basic NMAP Commands	10
Ping Scans with NMAP	9
Scanning TCP and UDP with NMAP	11
Identifying Host Attributes with NMAP	13
Using NMAP Scripts	11
Bypassing Firewalls with NMAP	11

Enumerating Services and Vulnerabilities

Overview	1
Intro to Enumerating Services and Vulnerabilities	2
Enumerating with Port Scanners	20

WEEK 2 — **159 min.**

Enumerating Web Servers	17

Enumerating SMB and Shares	14
Enumerating Vulnerabilities with Nessus	21
Automating Enumeration	13
Pentest Enumeration Review	3

Social Engineering Attacks and Tools

Overview	1
Social Engineering Anatomy	9
Social Engineering Attacks	8
Social Engineering Tools	8
Social Engineering Toolkit	5
Using WifiPhisher	4
Pharming With ShellPhish	10
Social Engineering Review	4

Exploits and Payloads

Overview	1
Exploits and Payloads	8
Moving Files With PwnDrop	17
Transferring Files with SMB and SCP	14

WEEK 3

156 min.

Working With Exploits	21
Working With Payloads	14
Exploits and Payloads Review	2

Metasploit Framework

Overview	1
Intro to the Metasploit Framework	4
Metasploit Startup and Workspaces	12
Metasploit Modules	15
Metasploit Options and Payloads	15
Managing Metasploit Sessions	8
Using Meterpreter	15
Metasploit Framework Review	2

Network-Based Attacks and Tools

Overview	1
Network Based Attacks and Tools	11
How Attacks Against ARP Work	6
ARP Poisoning Attack	13
How DNS Cache Poisoning Works	3
DNS Cache Poisoning Attack	11

WEEK 4

152 min.

VLAN Hopping Attacks	4
Bypassing Network Access Control	10
Network Based Attacks Review	6

Host Protocol Attacks and Tools

Overview	1
Host Protocol Attacks and Tools Overview	5
Server Message Block (SMB) Protocol	4
Attacking the SMB Protocol	18
Simple Network Management Protocol (SNMP)	5
Exploiting the SNMP Protocol	18

Denial of Service Attacks	10
Analyzing the LLMNR Protocol	4
Attacking the LLMNR Protocol	11
Host Protocol Attacks and Tools Review	3

Wireless and Mobile Device Attacks and Tools

Overview	1
Wireless and Mobile Device Attacks and Tools	9
Sniffing Wireless Data	6
Wireless Analysis With Kismet	7
Wireless Deauthentication Attacks	4
Cracking WPA2 Preshared Keys	5
Wireless Evil Twin Attack	8
Automated Wifi Attack Tools	7
Section Review	4

WEEK 5

Web Application Vulnerabilities — 166 min.

Overview	1
OWASP Top 10 (1 thru 3)	11
OWASP Top 10 (4 thru 6)	7
OWASP Top 10 (7 thru 10)	10
Cross Site Scripting (XSS) and Cross Site Request Forgery (CSRF)	4
SQL Injection Attacks	4
File Inclusion Vulnerabilities	8
Additional Web App Vulnerabilities and Attacks	6

Web Application Pentesting

Overview	1
Web Application Pentesting	4
OWASP ZAP	17
Attack Scans Using OWASP ZAP	10
Brute Force Attack Using OWASP ZAP	12
SQL Injection Using SQLmap	18
Local and Remote File Inclusion Attacks	13
Cross Site Scripting (XSS) Attacks	11

All About Shells

Overview	1
Bind and Reverse Shells	9
The Power of Web Shells	16

WEEK 6

Working With Bind and Reverse Shells — 156 min.

Working With Bind and Reverse Shells	12
Shell One-Liners	11
Spawning Meterpreter Shells	18
Log Poisoning for a Shell	11

Windows Localhost Vulnerabilities, Attacks, and Tools

Overview	1
Windows Privilege Escalation Pt.1	8
Windows Privilege Escalation Pt.2	7
Getting a Windows Shell	14
Windows Local Host Enumeration	14
Windows Unquoted Service Path Vulnerability	15

Linux Localhost Vulnerabilities, Attacks, and Tools

WEEK 7

161 min.

Physical Penetration Testing

Credential Attacks

WEEK 8

155 min.

Performing Attacks on Cloud Technologies

Attacks and Vulnerabilities of Specialized Systems

WEEK 9

Post Exploit Activities — 160 min.

Overview	1
Establishing Persistence	5
Lateral Movement	9
Data Exfiltration	7
Covering Your Tracks	6
Linux Post Exploit Activities	16
Windows Post Exploit Activities	16

Analyzing Scripts

Overview	1
Intro	1
Analyzing PING Scripts	15
Downloading Files with Scripts	5
Automation with Scripts	11
Updating IP Settings with a Script	6
NMAP Reports in HTML	7

Scripting Basics

Overview	1
Analyze a Basic Script	6
Scripting Basics	9
Assigning Values to Variables	8
Operating on Variables with Operators	7
Branching Code with Conditionals	9
Reapeating Code with Loops	11

WEEK 10

8 min.

Handling Errors in Code	7

Last updated 12.3.2024