CompTIA Pentest+ (PT0-003)

Learn how to simulate real-world cyberattacks, uncover network vulnerabilities, and sharpen your ethical hacking skills with this intermediate PenTest+ training. You'll practice modern penetration testing techniques in realistic labs, document findings, and prepare for the CompTIA PenTest+ (PT0-003) exam. Ideal for junior cybersecurity pros ready to level up or seasoned testers looking to validate their skills.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Pre-Engagement Activities

What Is Penetration Testing

The Pentesting Process

Defining A Scope

Defining A Scope - Identifying Targets

Defining A Scope - Rules of Engagement

Types of Agreements

Validation

Communications and Pentesting Methodologies

Introduction

Shared Responsibilities

Legal and Ethical Considerations

The Importance of Communications

Peer Review and Secure Distribution

Calculating Risk and Client Acceptance

Pentesting Standards & Methodologies

Threat Modeling Frameworks

The MITRE ATT&CK Framework

Validation

Pentest Reports and Security Controls

Introduction

Pentest Reports

Viewing A Pentest Report

Reporting Considerations

Providing Recommendations - Technical Controls

Providing Recommendations - Administrative Controls

Providing Recommendations - Operational Controls

WEEK 2

Providing Recommendations - Physical Controls

Validation

Passive Reconnaissance and OSINT

Introduction

Active vs. Passive Reconnaissance and OSINT

Web-Based OSINT Tools

NSLookup/DIG and Maltego

Recon-ng and SpiderFoot

OWASP Amass

DNSenum & DNSrecon

theHarvester

Google Dorking

Validation

Passive Reconnaissance Practice

Introduction

Pre-Engagement Discussion

DNS Enumeration

Email Enumeration

Password Enumeration

Social Media Snooping

Job Posting and Business Information Enumeration

Validation

Active Enumeration In The Lab

Introduction

Active Enumeration of Targets

Active Enumeration Tools

What Are We Looking For?

What Do We Do With Our Findings?

WEEK 3

Port Scanners

Lab Introduction

Validation

NMAP In-Depth

Introduction

The TCP 3-Way Handshake

Ports and Sockets

A Basic NMAP Scan

NMAP and ICMP

Scanning TCP and UDP Ports

Identifying Host Attributes

NMAP Scripting Engine (NSE)

Bypassing Firewalls With NMAP

Validation

Active Enumeration - Network Services Part 1

Introduction

FTP Enumeration

SSH Enumeration

Telnet Enumeration

SMTP Enumeration

DNS Enumeration

SNMP Enumeration

Validation

WEEK 4

Active Enumeration - Network Services Part 2

Introduction

R Services

Java RMI (Remote Method Invocation)

Bind shells

RPC / NFS

MySQL

distccd v1

Postgresql

VNC (Virtual Network Computing)

IRC (Internet Relay Chat)

Validation

Active Enumeration - Network Services Part 3

Introduction

LDAP Enumeration

Server Message Block (SMB) Part 1

Server Message Block (SMB) Part 2

CUPS Enumeration

RDP Enumeration

Validation

Active Enumeration - Web Services Part 1

Introduction

Introduction To Web Communications

HTTP Methods In Action

WEEK 5

Banner Grabbing

Content Management Systems (CMS) and Frameworks

Identifying Web Technologies In Use

Website Enumeration With Fuzzing

Validation

Active Enumeration - Web Services Part 2

Introduction

Detecting Web Application Firewalls (WAFs)

HTML/Web Scraping

Using Burp Suite To Enumerate Web Services

Enumerating Web Services With OWASP ZAP

Validation

Analyzing Scripts

Introduction

Scripting Basics

Working With Scripts

Analyzing PING Scripts - BASH

Analyzing PING Scripts - PowerShell

Analyzing PING Scripts - Python

Downloading Files With Scripts

Using Automation With Scripts

Validation

WEEK 6

Vulnerability Discovery and Analysis Pt.1

Introduction

Security Testing Methodologies - Containers

Security Testing Methodologies - Software

Scanning Methods

Scanning Methods for Industrial Control Systems (ICS)

Web App Vulnerability Scanning With Nikto

Finding Secrets With Trufflehog

Validation

Vulnerability Discovery and Analysis Pt.2

Introduction

Getting To Know Bloodhound

Analyzing Active Directory With BloodHound

Vulnerability Scanning With Nessus

The PowerSploit Framework

Scanning Containers With Trivy

Physical Security Controls

Validation

Metasploit Framework (MSF)

Introduction

Intro To The Metasploit Framework (MSF)

MSF Startup and Workspaces

Metasploit Modules

Metasploit Options and Payloads

Managing Metasploit Sessions

WEEK 7

Using Post Modules in MSF

The MSF Meterpreter Shell

Validation

Analyze, Prioritize and Prepare Attacks

Introduction

Target Prioritization

Selecting A Strategy

Attack Types and Tools Pt.1

Attack Types and Tools Pt.2

Attack Types and Tools Pt.3

Attack Types and Tools Pt.4

Validation

Authentication Attacks Pt.1

Introduction

MFA Fatigue and Hashes

Hash Attacks, Kerberos Attacks and LDAP Injection

Getting To Know NetExec (Previously CrackMapExec)

Dumping Hashes On Windows

Pass-The-Hash Attacks

Validation

WEEK 8

Authentication Attacks Pt.2

Introduction

Credential Attacks

Creating Custom Wordlists

Brute Force Credential Attacks

Dumping Hashes On Linux

Cracking Hashes

Validation

Host Based Attacks

Introduction

Windows Privilege Escalation (privesc)

Linux Privilege Escalation (privesc)

Host Based Attacks Pt.1

Host Based Attacks Pt.2

Privesc Using SUID/GUID

Validation

Web Application Vulnerabilities

Overview

OWASP Top 10 (1 thru 3)

OWASP Top 10 (4 thru 6)

OWASP Top 10 (7 thru 10)

WEEK 9

Cross Site Scripting (XSS) and Cross Site Request Forgery (CSRF)

SQL Injection Attacks

File Inclusion Vulnerabilities

Additional Web App Vulnerabilities and Attacks

Web Application Attacks

Introduction

Brute Force Attacks Using OWASP ZAP

SQL Injection (SQLi) Attacks Using SQLmap

Local and Remote File Inclusion Attacks

Cross Site Scripting (XSS) Attacks

Validation

All About Shells

Introduction

All About Shells

Bind and Reverse Shells

Web Shells

Shell One-Liners

Creating A Meterpreter Shell

Web Server Log Poisoning For A Shell

Validation

Cloud Based Attacks

Introduction

Attacks On Cloud Services

Exploiting Misconfigurations In AWS S3 Buckets

WEEK 10

Performing An Account Takeover With Pacu

Enumeration With ScoutSuite

Validation

Wireless and Mobile Device Attacks and Tools

Overview

Wireless and Mobile Device Attacks and Tools

Sniffing Wireless Data

Wireless Analysis With Kismet

Wireless Deauthentication Attacks

Cracking WPA2 Preshared Keys

Wireless Evil Twin Attack

Automated Wifi Attack Tools

Section Review

Social Engineering Attacks

Introduction

Social Engineering Attack Anatomy

Social Engineering Attacks

Social Engineering Tools

The Social Engineering Toolkit

WifiPhisher

GoPhish

Validation

Attacks and Vulnerabilities of Specialized Systems

Overview

Mobile Device Attacks

Mobile Device Vulnerabilities

Mobile Security Tools

Internet of Things (IoT) Devices

Data Storage System Vulnerabilities

SCADA, IIoT and ICS Vulnerabilities

Virtual Environment Vulnerabilities

Attacks Against Artificial Intelligence (AI)

Automating Enumeration and Pentesting

Introduction

PowerShell Enumeration and Data Manipulation In BASH

Linux On-Host Enumeration

Scapy and Impacket

Windows Active Directory Enumeration With PowerView

Breach and Attack Simulation (BAS)

Validation

Pivoting and Lateral Movement

Introduction

Pivoting and Lateral Movement

Pivoting With Chisel

Lateral Movement With Chisel and Proxychains

Port Forwarding With Chisel

Pivoting With Metasploit

Port Forwarding With Metasploit

Validation

WEEK 11

WEEK 12

Establishing Persistence

What Is Persistence

Setup Persistence On Linux Using Cron Jobs

Setup Persistence On Windows Using Scheduled Tasks

Setup Persistence On Windows Using An MSF Payload

Validation

Data Exfiltration and Pentest Cleanup

Introduction

Data Exfiltration

Data Exfiltration On Linux

Data Exfiltration On Windows

Cleanup and Restoration Activities

Covering Your Tracks

Validation

Last updated 1.12.2026