CompTIA PenTest+ (PT0-001 & PT0-002)

This CompTIA PenTest+ certification training covers the topics on the PT0-002 penetration testing exam objectives. You'll learn how to execute a penetration test and perform vulnerability scans, and be better prepared for more senior security roles.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Understanding the Need for Scope Planning

Introduction to the Importance of Planning

Identifying Target Audience

Specifying the Rules of Engagement

Defining Resources, Requirements, and Budgets

Explaining Timelines and Disclaimers

Defining Technical Constraints

Requesting Support Resources

Explaining Key Legal Concepts

Overview

Legal Concepts Introduction

Identifying Legal Contracts

Considering Environmental and Location Factors

Obtaining Written Authorization

Obeying Corporate Policies

Properly Scoping an Engagement

Overview

Introduction to Properly Scoping an Engagement

Identifying Types of Assessments

Understanding Mergers and Partners

Selecting Targets

Targeting Considerations

Understanding Risk and Tolerance

Identifying Scope Creep and Schedule Impact

Identifying Threat Actors

Explain Compliance-Based Assessments

Overview

Intro to Compliance Assessments

Identifying Various Compliance-based Standards

Using Pre-defined Rules for a Pentesting Engagement

Understanding Password Policies and Key Management

Handling Data Isolation and Limited Access

Standards, Compliance and the Ethical Hacker Mindset

Overview

Regulatory Compliance

Legal Concepts

Standards and Methodologies

MITRE ATT&CK Framework

Ethical Hacker Mindset

WEEK 2

Conduct Information Gathering Using Appropriate Techniques

Overview

Introduction to Information Gathering

Scanning Hosts

Enumerating Hosts for Specific Details

Digging Deeper into Fingerprinting and Cryptography

Eavesdropping for Data

Decompiling and Debugging for Data

Using Open Source Intelligence Gathering

Perform a Vulnerability Scan

Overview

Intro to Vulnerability Scanning

Identifying Types of Scans

Handling Scanning Permissions

Scanning Applications and Containers

Scanning Considerations

Analyze Vulnerability Scan Results

Overview

Intro to Analyzing Scan Results

Categorizing Assets

Adjudicating Scan Results

Prioritizing Vulnerabilities

Identifying Common Themes

Leverage Information for Exploitation

Overview

Intro to Exploitation

Mapping Vulnerabilities to Potential Exploits

Prioritizing Pentest Activities

Implementing Exploits

Learning Password Cracking Methods

Understanding Social Engineering

Explain Weaknesses Inherent to Specialized Systems

Overview

Intro to Specialized Systems

Understanding ICS and SCADA

Considering Mobile Devices

Embedded and Real-Time Devices

Utilizing IoT Devices

Understanding POS Device Weaknesses

Pentesting Reconnaissance

Overview

Introduction to Pentesting Reconnaissance

Pentesting Reconnaissance Tools

WEEK 3

Domain Information Tools

IP and DNS Information Tools

Combination OSINT Tools

Breach Data Tools

Pentesting Reconnaissance Review

Pentest Enumeration and NMAP

Overview

Intro to Pentesting Enumeration

Pentest Enumeration Tools

Basic NMAP Commands

Ping Scans with NMAP

Scanning TCP and UDP with NMAP

Identifying Host Attributes with NMAP

Using NMAP Scripts

Bypassing Firewalls with NMAP

Enumerating Services and Vulnerabilities

Overview

Intro to Enumerating Services and Vulnerabilities

Enumerating with Port Scanners

Enumerating Web Servers

WEEK 4

Enumerating SMB and Shares

Enumerating Vulnerabilities with Nessus

Automating Enumeration

Pentest Enumeration Review

Social Engineering Attacks and Tools

Overview

Social Engineering Anatomy

Social Engineering Attacks

Social Engineering Tools

Social Engineering Toolkit

Using WifiPhisher

Pharming With ShellPhish

Social Engineering Review

Exploits and Payloads

Overview

Exploits and Payloads

Moving Files With PwnDrop

Transferring Files with SMB and SCP

WEEK 5

Working With Exploits

Working With Payloads

Exploits and Payloads Review

Metasploit Framework

Overview

Intro to the Metasploit Framework

Metasploit Startup and Workspaces

Metasploit Modules

Metasploit Options and Payloads

Managing Metasploit Sessions

Using Meterpreter

Metasploit Framework Review

Network-Based Attacks and Tools

Overview

Network Based Attacks and Tools

How Attacks Against ARP Work

ARP Poisoning Attack

How DNS Cache Poisoning Works

DNS Cache Poisoning Attack

WEEK 6

VLAN Hopping Attacks

Bypassing Network Access Control

Network Based Attacks Review

Host Protocol Attacks and Tools

Overview

Host Protocol Attacks and Tools Overview

Server Message Block (SMB) Protocol

Attacking the SMB Protocol

Simple Network Management Protocol (SNMP)

Exploiting the SNMP Protocol

Denial of Service Attacks

Analyzing the LLMNR Protocol

Attacking the LLMNR Protocol

Host Protocol Attacks and Tools Review

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

WEEK 7

Web Application Vulnerabilities

Overview

OWASP Top 10 (1 thru 3)

OWASP Top 10 (4 thru 6)

OWASP Top 10 (7 thru 10)

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

SQL Injection Attacks

File Inclusion Vulnerabilities

Additional Web App Vulnerabilities and Attacks

Web Application Pentesting

Overview

Web Application Pentesting

OWASP ZAP

Attack Scans Using OWASP ZAP

Brute Force Attack Using OWASP ZAP

SQL Injection Using SQLmap

Local and Remote File Inclusion Attacks

Cross Site Scripting (XSS) Attacks

All About Shells

Overview

Bind and Reverse Shells

The Power of Web Shells

WEEK 8

Working With Bind and Reverse Shells

Shell One-Liners

Spawning Meterpreter Shells

Log Poisoning for a Shell

Windows Localhost Vulnerabilities, Attacks, and Tools

Overview

Windows Privilege Escalation Pt.1

Windows Privilege Escalation Pt.2

Getting a Windows Shell

Windows Local Host Enumeration

Windows Unquoted Service Path Vulnerability

Windows Local Exploit Privilege Escalation

Linux Localhost Vulnerabilities, Attacks, and Tools

Overview

Introduction to Privilege Escalation

Linux Privilege Escalation Pt.1

Linux Privilege Escalation Pt.2

WEEK 9

Linux Shell Escalation

Linux Local Host Enumeration

Linux Privilege Escalation Via Cron Jobs

Linux SUID and SUDO privilege escalation

Linux Local Exploit Privilege Escalation

Physical Penetration Testing

Overview

Physical Pentest Documents

Reconnaissance and Planning

Physical Pentest Tools

Getting Inside

Continuing From the Inside

Physical Pentest Report

Credential Attacks

Overview

Credential Attacks Pt.1

Credential Attacks Pt.2

Creating Custom Wordlists

WEEK 10

Performing a Brute Force Attack

Cracking Hashed Passwords

Executing a Pass the Hash Attack

Performing Attacks on Cloud Technologies

Overview

Credential Harvesting and PrivEsc in the Cloud

Running PACU

Misconfigured Cloud Assets

Running CloudSploit

Resource Exhaustion, Malware Injection and API Attacks

Side Channel and Direct-To-Origin Attacks

Additional Cloud Pentesting Tools

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

WEEK 11

Attacks Against Artificial Intelligence (AI)

Post Exploit Activities

Overview

Establishing Persistence

Lateral Movement

Data Exfiltration

Covering Your Tracks

Linux Post Exploit Activities

Windows Post Exploit Activities

Scripting Basics

Overview

Analyze a Basic Script

Scripting Basics

Assigning Values to Variables

Operating on Variables with Operators

Branching Code with Conditionals

Repeating Code with Loops

Handling Errors in Code

Analyzing Scripts

Overview

Intro

Analyzing PING Scripts

Downloading Files with Scripts

WEEK 12

Automation with Scripts

Updating IP Settings with a Script

NMAP Reports in HTML

Security Controls and Control Frameworks

Overview

Security Controls

Security Control Categories

Security Control Functions

Testing Security Controls

Control Objectives and Frameworks

Designing Controls

Security Control Review

Pentest Reporting and Communications

Overview

Writing and Handling a Pentest Report

Reviewing an Example Pentest Report

Post-Report Delivery Activities

Providing Recommendations

The Importance of Communicaitons

Last updated 1.12.2026