Network Penetration Testing Essentials (PEN-200)

This is a professional-level OffSec course that prepares penetration testers and red team operators for the OSCP+ certification. Gain deep experience in areas like enumeration, privilege escalation, and Active Directory exploitation as you apply tools like Metasploit, Kali Linux, and tunneling frameworks in real-world scenarios.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Beginning Pen-200

Timestamps

Applying timestamps

Note taking

Note taking in use

Executive Summary

Challenge

Pen Testing Lifecycle with Reconnaissance

Pen Testing Lifecycle

Reconnaissance

Conducting Recon

Other things to consider

Recon using Kali

Challenge

Exploit resources

Exploit resources

Public databases

Zero-Day Vulnerabilities

Automated scripting tools

Physical Access

Challenge

Metasploit fundamentals

Metasploit fundamentals

Metasploit main console

msfvenom

msfconsole

Vulnerability assessment with Metasploit

Challenge

Matasploit Payloads

Metasploit Payloads

Stagers

Singles

Stages

Inline

Nops

Challenge

Scanning with nMap

Finding the right kind of bacon

Need a refresher?

Controlling your speed

Practice Lab

Challenge

Scanning with Nessus (Active)

Scanning with Nessus (Active)

WEEK 2

Installing Nessus

Configuring Nessus

Doing a simple scan

Challenge

Detailed Active Scanning with Nessus

Taking a deeper look at Nessus

Understanding Plugins

Installing offline plugins

Scanning with plugins

Challenge

OpenVAS

OpenVAS

Building our database

Identifying and configuring our scope

Scan results

Challenge

Passive Scanning for Vulnerabilities

Passive scanning for vulnerabilities

Getting ready to passively scan

Listening to the network

Parsing through some of the capture

Challenge

WEEK 3

Deeper into Passive Scanning

Can we look deeper into the passive packet capture?

Etherape

NetworkMiner

Challenge

Web Application Assessment

Web Application Assessment

Beginning to understand web platforms

Now let's look at some tools

Playground introduction

Challenge

Web Application Assessment Tools

Web Application Assessment Tools

Misconfiguration examples

Nikto

Trying to be stealthy

OWASP ZAP

Challenge

Burpsuite

Getting to know burpsuite

Burpsuite proxy

Testing against our dummy site

Challenge

Cross-Site Scripting XSS

Cross-Site Scripting XSS

Reflected XSS (Non-Persistent)

Using reflection to redirect

Stored XSS (Persistent)

Challenge

Directory Traversal

What is directory traversal?

Directory traversal on a website

Directory traversal attacks

Attacking the files

Challenge

File Inclusion Attack

File inclusion attacks

Review and prep work

Uploading our file

Testing the file

Challenge

Command Injection

Command injection

The Good

The Bad

The Ugly

Challenge

SQL Theory and Exploration

What is SQL?

Where is SQL used?

SQL, but lite(er)

Basic SQL Injection tests

Challenge

Exploiting Microsoft Office

Exploiting Microsoft Office

Macro coding

Beginning to exploit with macros

Sending information with macros

Challenge

Windows Library Files

Windows Library Files

Identifying DLLs tied to a program

Shared libraries

Signed or not signed

Challenge

Abusing Windows Library Files

Why would we attack DLL files?

Using Metasploit to craft DLLs

Replacing unsigned DLLs

Rundll32.exe

Challenge

Advanced DLL Injection

Advanced DLL Injection

Getting the target to run things for us

Using DLL Injection with our crafted DLLs

Making use of the injection

Challenge

But wait! That's not all.

Post-Exploitation with Metasploit

Post-Exploitation with Metasploit

Persistence

Hash dumping

Files and critical information

Challenge

Password Attacks - Understanding

Password Attacks

Salt

Knowing the password parameters

Challenge

But wait, there's more!

Password Attacks - Methodology

Beginning to crack passwords

Rainbow Tables

Something more recent

Hashcat

Challenge

Password Attacks - Physical Attack

Physical Pen Testing

Booting into a Live OS

BIOS vs UEFI

Challenge

Password Attacks - Tools

Tools of the trade

WEEK 4

John the Ripper

Hydra

Other passwords

Challenge

Windows Enumeration

Attack on Windows

Triage

System Configuration

Services & Processes

Saved Credentials & Sensitive Files

Challenge

Leveraging Windows Services

Windows Services

Service Examination

Service Permissions

Services for persistence

Challenge

Linux Enumeration

Attack on Linux

Triage

System Configuration

Policies & Services

Challenge

Linux Insecurity

Believe it or not...

Software & Kernel Vulnerabilities

Weak sudo Policy

Remote connections

Challenge

Linux File Insecurity

Insecurity in Linux files

World-Writable Files and Directories

SUID Binaries

Unowned Files and Directories

Challenge

Port Forwarding and Tunneling

Port Forwarding

Port Forwarding with ssh

Dynamic Port Forwarding

socat

Challenge

Deep Packet Inspection

Deep packet inspection

Inspection conditions

Evasion through encryption

Avoiding Deep Packet Inspection

Challenge

Other Tunneling Tools

More Tunneling

chisel

ptunnel

Challenge

Antivirus Evasion

Antivirus Evasion

Is there a difference?

How does it know?

Endpoint detection in action

Challenge

Automating Metasploit

Automation

Scripts

Multi session scripts

Session automation

Challenge

Memory Corruption Exploits

Understanding the architecture

Stack vs Heap

Using memory exploits

How to fix

Challenge

Fixing Web Exploits

Fixing web exploits

Where do we begin?

Directory scanning

Nikto

Challenge

Understanding Active Directory Authentication

Active Directory

Kerberos

NTLM (New Technology LAN Manager)

Monitoring the Authentication Traffic

Challenge

Active Directory Manual Enumeration

Manual Enumeration

Looking for servers and computers

Network information

Challenge

Active Directory Automated Enumeration

Auto Enumerate

Looking at the scripts

Sites and Services

Enumeration with Metasploit

Challenge

Attacks on Active Directory Authentication

Attacking AD

Passive Harvesting

Roasting

Kerberoast

Challenge

Active Directory Persistence

The Golden Ticket

Prerequisites

Gaining a ticket

Using the ticket

Challenge

Lateral Movements and Post-cleanup

Closing out

Looking at the logs

Stopping time!!

Lateral movements

Laterally commanding

Challenge

Last updated 12.17.2025