

# OffSec PEN-200

## 24 Week Learning Plan

Welcome to OffSec PEN-200! We are delighted to offer a customized learning plan designed to support your learning journey and ultimately enhance your preparedness for the Offensive Security Certified Professional (OSCP) certification.

The Learning Plan comprises a week-by-week journey, which includes a recommended studying approach, estimated learning hours, course topics to focus on, topic exercises, capstone exercises, and challenge machines to complete, as well as supplemental materials to reinforce your learning (if you so choose).

## Table of Contents

[Week 1](#)

[Week 2](#)

[Week 3](#)

[Week 4](#)

[Week 5](#)

[Week 6](#)

[Week 7](#)

[Week 8](#)

[Week 9](#)

[Week 10](#)

[Week 11](#)

[Week 12](#)

[Week 13](#)

[Week 14](#)

[Week 15](#)

[Week 16](#)

[Week 17](#)

[Week 18](#)

[Week 19-22](#)

[Week 23-24](#)

# Week 1

## Overview and Study Approach

The topics covered this week serve as an introduction to the course material and provide a general approach to the course.

We also recommend learners explore the following OffSec's communication mediums:

- OffSec Help and FAQs: <https://help.offsec.com/hc/en-us>
- Discord: [How may I join the OffSec Community?](#)
- Youtube Channel: [@OffSecTraining](#)
- Twitch Channel: [@offsecofficial](#)
- Twitter: [@OffSecTraining](#)

## Learning Topics

- 1) Penetration Testing with Kali Linux: General Course Information
- 2) Introduction To Cybersecurity
- 3) Report Writing for Penetration Testers

## Exercises

- 3.1.3. On Emulating the Minds of our Opponents
- 3.2.4. Recent Cybersecurity Breaches
- 3.3.4. Balancing the Triad with Organizational Objectives
- 3.4.9. Logging and Chaos Testing
- 3.5.2. Standards and Frameworks
- 3.6.3. Cybersecurity Career Opportunities: Build
- 5.1.6. Tools to Take Screenshots
- 5.2.7. Appendices, Further Information, and References

## Estimate Time (Hours)

10

## Supplemental Learning\*

### Videos:

- Offsec Live Twitch Recordings: [Get to Know the Minds Behind PEN-200 \(2023\)](#).

**Relevant Labs:** N/A

# Week 2

Overview and Study Approach	This week we will focus on getting the learner familiar with different tools and techniques that allow us to perform successful information gathering and vulnerability scanning.
Learning Topics	1) Information Gathering 2) Vulnerability Scanning
Exercises	6.2.1. Whois Enumeration 6.2.2. Google Hacking 6.2.3. Netcraft 6.2.4. Open-Source Code 6.3.1. DNS Enumeration 6.3.2. TCP/UDP Port Scanning Theory 6.3.3. Port Scanning with Nmap 6.3.4. SMB Enumeration 6.3.5. SMTP Enumeration 6.3.6. SNMP Enumeration 7.1.1. How Vulnerability Scanners Work 7.1.2. Types of Vulnerability Scans 7.1.3. Things to consider in a Vulnerability Scan 7.2.1. Installing Nessus 7.2.2. Nessus Components 7.2.3. Performing a Vulnerability Scan 7.2.4. Analyzing the Results 7.2.5. Performing an Authenticated Vulnerability Scan 7.2.6. Working with Nessus Plugins 7.3.1. NSE Vulnerability Scripts 7.3.2. Working with NSE Scripts
Estimate Time (Hours)	10
Supplemental Learning*	<b>Videos:</b> <ul style="list-style-type: none"><li>• OffSec Academy Recordings: <a href="#">OSA - PEN - 200: Week 1A - Active Info. Gathering</a></li></ul> <b>Relevant Labs:</b> N/A

# Week 3

## Overview and Study Approach

This week we will focus on the basic methodology, techniques, and tools required to perform successful enumeration and exploitation of basic web application attacks.

## Learning Topics

1) Introduction to Web Application Attacks

## Exercises

8.2.4. Security Testing with Burp Suite  
8.3.3. Enumerating and Abusing APIs  
8.4.5. Privilege Escalation via XSS

## Estimate Time (Hours)

10

## Supplemental Learning\*

### Videos:

- OffSec Academy Recordings: [OSA - PEN - 200: Week 3A - Web Application Attacks](#)
- OffSec Live Twitch Recordings: [WEB-200: Cross-site Scripting](#)

### Relevant Labs:

- [Proving Ground Practice](#) labs:
  - Key examples: hetemit
  - Additional practice (when ready): N/A

# Week 4

Overview and Study Approach	This week, we will focus on the basic methodology, techniques, and tools required to perform successful enumeration and exploitation of common web application attacks.
Learning Topics	1) Common Web Application Attacks (Part 1)
Exercises	9.1.1. Absolute vs Relative Paths 9.1.2. Identifying and Exploiting Directory Traversals 9.1.3. Encoding Special Characters 9.2.1. Local File Inclusion (LFI) 9.2.2. PHP Wrappers
Estimate Time (Hours)	10
Supplemental Learning*	<b>Videos:</b> <ul style="list-style-type: none"><li>OffSec Academy Recordings: <a href="#">OSA - PEN - 200: Week 2A - Web Application Attacks</a></li></ul> <b>Relevant Labs:</b> <ul style="list-style-type: none"><li><a href="#">Proving Ground Practice</a> labs:<ul style="list-style-type: none"><li>Key examples: payday</li><li>Additional practice (when ready): reconstruction, xposedapi, Apex</li></ul></li></ul>

# Week 5

Overview and Study Approach	We will continue to focus on Part 2 of the basic methodology, techniques, and tools required to perform successful enumeration and exploitation of common web application attacks.
Learning Topics	2) Common Web Application Attacks (Part 2)
Exercises	9.2.3. Remote File Inclusion (RFI) 9.3.1. Using Executable Files 9.3.2. Using Non-Executable Files 9.4.1. OS Command Injection
Estimate Time (Hours)	10
Supplemental Learning*	<b>Videos:</b> N/A <b>Relevant Labs:</b> <ul style="list-style-type: none"><li>• <a href="#">Proving Ground Practice</a> labs:<ul style="list-style-type: none"><li>◦ Key examples: uc404</li><li>◦ Additional practice (when ready): slort, Apex</li></ul></li></ul>

# Week 6

## Overview and Study Approach

This week will focus on understanding SQL syntax and exploiting SQL Injection vulnerabilities.

## Learning Topics

1) SQL Injection Attacks

## Exercises

10.1.2. DB Types and Characteristics  
10.2.3. Blind SQL Injections  
10.3.2. Automating the Attack

## Estimate Time (Hours)

10

## Supplemental Learning\*

### Videos

- OffSec Academy Recordings: [OSA - PEN - 200: Week 3A - Web Application Attacks](#)

### Relevant Labs:

- [Proving Ground Practice](#) labs:
  - Key examples: butch, Hepet
  - Additional practice (when ready): hawat, pebbles, megavolt



# Week 7

**Overview and Study Approach** This week will delve into network attacks, password cracking, and attacks against Windows-based authentication implementations.

**Learning Topics** 1) Password Attacks

**Exercises**

- 15.1.1. SSH and RDP
- 15.1.2. HTTP POST Login Form
- 15.2.1. Introduction to Encryption, Hashes and Cracking
- 15.2.2. Mutating Wordlists
- 15.2.3. Cracking Methodology
- 15.2.4. Password Manager
- 15.2.5. SSH Private Key Passphrase
- 15.3.1. Cracking NTLM
- 15.3.2. Passing NTLM
- 15.3.3. Cracking Net-NTLMv2
- 15.3.4. Relaying Net-NTLMv2

**Estimate Time (Hours)** 10

**Videos:** N/A

**Supplemental Learning\***

**Relevant Labs:**

- [Proving Ground Practice](#) labs:
  - Key examples: Authby, nickel
  - Additional practice (when ready): Phobos

# Week 8

## Overview and Study Approach

This week will focus on online resources that provide public known vulnerabilities exploits. Additionally, we will examine offline tools within Kali that contain local-hosted exploits and learn techniques for overcoming any potential obstacles when utilizing these tools.

## Learning Topics

- 1) Locating Public Exploits
- 2) Fixing Exploits

## Exercises

- 12.1.1. A Word of Caution
- 12.2.1. The Exploit Database
- 12.3.1. Exploit Frameworks
- 12.3.2. SearchSploit
- 12.3.3. Nmap NSE Scripts
- 12.4.1. Putting It Together
- 13.1.3. Cross-Compiling Exploit Code
- 13.1.4. Fixing the Exploit
- 13.1.5. Changing the Overflow Buffer
- 13.2.2. Selecting the Vulnerability and Fixing the Code
- 13.2.3. Troubleshooting the "index out of range" Error

## Estimate Time (Hours)

10

## Supplemental Learning\*

**Videos:** N/A

**Relevant Labs:**

- [Proving Ground Practice](#) labs:
  - Key examples: Kevin, shifty
  - Additional practice (when ready): Twiggy

# Week 9

Overview and Study Approach	This week will cover multiple techniques for detecting malicious software, as well as exploring methods to bypass AV software on target machines. Additionally, learners will acquire the skills to conduct target reconnaissance, explore exploitation scenarios using malicious Microsoft Office documents and Windows Library files.
Learning Topics	1) Client-side Attacks 2) Antivirus Evasion
Exercises	11.1.1. Information Gathering 11.1.2. Client Fingerprinting 11.2.1. Preparing the Attack 11.2.2. Installing Microsoft Office 11.2.3. Leveraging Microsoft Word Macros 11.3.1. Obtaining Code Execution via Windows Library Files 14.1.3. Detection Methods 14.2.2. In-Memory Evasion 14.3.2. Evading AV with Thread Injection 14.3.3. Automating the Process
Estimate Time (Hours)	12
Supplemental Learning*	<b>Videos:</b> N/A <b>Relevant Labs:</b> <ul style="list-style-type: none"><li>• <a href="#">Proving Ground Practice</a> labs:<ul style="list-style-type: none"><li>◦ Key examples: Hepet</li><li>◦ Additional practice (when ready): megavolt</li></ul></li></ul>

# Week 10

## Overview and Study Approach

Once we gain access to the target machine, we will need to escalate the privileges in order to perform more advanced actions on the compromised system. This week's topic will focus on techniques and exploits that enable successful privilege escalation on the Windows system.

## Learning Topics

1) Windows Privilege Escalation

## Exercises

16.1.1. Understanding Windows Privileges and Access Control Mechanisms  
16.1.2. Situational Awareness  
16.1.3. Hidden in Plain View  
16.1.4. Information Goldmine PowerShell  
16.1.5. Automated Enumeration  
16.2.1. Service Binary Hijacking  
16.2.2. Service DLL Hijacking  
16.2.3. Unquoted Service Paths  
16.3.1. Scheduled Tasks  
16.3.2. Using Exploits

## Estimate Time (Hours)

10

## Supplemental Learning\*

### Videos:

- OffSec Academy Recordings:
  - [OSA - PEN - 200: Week 5A - Privilege Escalation](#)
  - [OSA - PEN - 200: Week 6A Privilege Escalation](#)

**Relevant Labs:** N/A

# Week 11

## Overview and Study Approach

As we continue to focus on privilege escalation, this week we will cover the techniques and exploits that enable successful privilege escalation on the Linux system.

## Learning Topics

1) Linux Privilege Escalation

## Exercises

17.1.2. Manual Enumeration  
17.1.3. Automated Enumeration  
17.2.1. Inspecting User Trails  
17.2.2. Inspecting Service Footprints  
17.3.1. Abusing Cron Jobs  
17.3.2. Abusing Password Authentication  
17.4.1. Abusing Setuid Binaries and Capabilities  
17.4.2. Abusing Sudo  
17.4.3. Exploiting Kernel Vulnerabilities

## Estimate Time (Hours)

12

## Supplemental Learning\*

### Videos:

- OffSec Academy Recordings: [OSA - PEN - 200: Week 4A - Privilege Escalation](#)

### Relevant Labs:

- [Proving Ground Practice](#) labs:
  - Key examples: morbo, Nibbles
  - Additional practice (when ready): billyboss, escape

# Week 12

## Overview and Study Approach

This week will cover port redirection and tunneling techniques using SSH. The topic will begin with simple techniques and gradually progress to more complex ones as we move towards more secure network environments.

## Learning Topics

1) Port Redirection and SSH Tunneling

## Exercises

18.2.3. Port Forwarding with Socat  
18.3.1. SSH Local Port Forwarding  
18.3.2. SSH Dynamic Port Forwarding  
18.3.3. SSH Remote Port Forwarding  
18.3.4. SSH Remote Dynamic Port Forwarding  
18.3.5. Using sshuttle  
18.4.1. ssh.exe  
18.4.2. Plink  
18.4.3. Netsh

## Estimate Time (Hours)

12

## Supplemental Learning\*

### Videos:

- OffSec Academy Recordings:
  - [OSA - PEN - 200: Week 8A - Port Redirection and tunneling](#)
  - [OSA - PEN - 200: Week 8B - Port Redirection and Tunneling](#)

### Relevant Labs:

- [Proving Ground Practice](#) labs:
  - Key examples: N/A
  - Additional practice (when ready): Nukem

# Week 13

Overview and Study Approach	There may be many restrictions implemented on a network. We will focus on learning and leveraging various tunneling tools and strategies to bypass technologies such as deep packet inspection. We will also cover the Metasploit Framework, including its features, usage and its internal workings. By doing this, we can understand how these frameworks can assist us in real penetration tests.
Learning Topics	1) Tunneling Through Deep Packet Inspection 2) The Metasploit Framework
Exercises	19.1.2. HTTP Tunneling with Chisel 19.2.1. DNS Tunneling Fundamentals 19.2.2. DNS Tunneling with dnscat2 20.1.1. Setup and Work with MSF 20.1.2. Auxiliary Modules 20.1.3. Exploit Modules 20.2.1. Staged vs Non-Staged Payloads 20.2.2. Meterpreter Payload 20.2.3. Executable Payloads 20.3.1. Core Meterpreter Post-Exploitation Features 20.3.2. Post-Exploitation Modules 20.3.3. Pivoting with Metasploit 20.4.1. Resource Scripts
Estimate Time (Hours)	12
Supplemental Learning*	<b>Videos:</b> <ul style="list-style-type: none"><li>• OffSec Academy Recordings: <a href="#">OSA - PEN - 200: Week 10A - The Metasploit Framework</a></li></ul> <b>Relevant Labs:</b> <ul style="list-style-type: none"><li>• <a href="#">Proving Ground Practice</a> labs:<ul style="list-style-type: none"><li>◦ Key examples: Splodge, Internal</li><li>◦ Additional practice (when ready): wombo</li></ul></li></ul>

# Week 14

## Overview and Study Approach

This week will focus on the enumeration aspect of Active Directory. The information we will gather throughout the Module will have a direct impact on the various attacks we will do in subsequent modules.

## Learning Topics

1) Active Directory Introduction and Enumeration

## Exercises

21.2.1. Active Directory - Enumeration Using Legacy Windows Tools  
21.2.2. Enumerating Active Directory using PowerShell and .NET Classes  
21.2.3. Adding Search Functionality to our Script  
21.2.4. AD Enumeration with PowerView  
21.3.1. Enumerating Operating Systems  
21.3.2. Getting an Overview - Permissions and Logged on Users  
21.3.3. Enumeration Through Service Principal Names  
21.3.4. Enumerating Object Permissions  
21.3.5. Enumerating Domain Shares  
21.4.1. Collecting Data with SharpHound  
21.4.2. Analysing Data using BloodHound

## Estimate Time (Hours)

10

## Supplemental Learning\*

### Videos:

- OffSec Academy Recordings:
  - [OSA - PEN - 200: Week 11A - Active Directory Attacks \(Part 1\)](#)
  - [OSA - PEN - 200: Week 12A - Active Directory Attack \(Part 1\)](#)
  - [OSA - PEN - 200: Week 13A - Active Directory Attack \(Part 2\)](#)
  - [OSA - PEN - 200: Week 14A - Active Directory Attack \(Part 2\)](#)
- OffSec Live Twitch Recordings:
  - [PEN-200 \(2023\): Active Directory Enumeration](#)
  - [Walkthrough of a PEN-200 AD Set](#)

**Relevant Labs: N/A**



# Week 15

Overview and Study Approach	This week will explore authentication mechanisms of Active Directory (AD) and learn where Windows caches authentication objects such as password hashes and tickets, after that, we'll get familiar with the attack methods targeting these authentication mechanisms.
Learning Topics	1) Attacking Active Directory Authentication
Exercises	22.1.1. NTLM Authentication 22.1.2. Kerberos Authentication 22.1.3. Cached AD Credentials 22.2.1. Password Attacks 22.2.2. AS-REP Roasting 22.2.3. Kerberoasting 22.2.4. Silver Tickets 22.2.5. Domain Controller Synchronization
Estimate Time (Hours)	10
Supplemental Learning*	<b>Videos:</b> <ul style="list-style-type: none"><li>• OffSec Academy Recordings:<ul style="list-style-type: none"><li>◦ <a href="#">OSA - PEN - 200: Week 11A - Active Directory Attacks (Part 1)</a></li><li>◦ <a href="#">OSA - PEN - 200: Week 12A - Active Directory Attack (Part 1)</a></li><li>◦ <a href="#">OSA - PEN - 200: Week 13A - Active Directory Attack (Part 2)</a></li><li>◦ <a href="#">OSA - PEN - 200: Week 14A - Active Directory Attack (Part 2)</a></li></ul></li><li>• OffSec Live Twitch Recordings:<ul style="list-style-type: none"><li>◦ <a href="#">PEN-200 (2023): Active Directory Enumeration</a></li><li>◦ <a href="#">Walkthrough of a PEN-200 AD Set</a></li></ul></li></ul> <b>Relevant Labs: N/A</b>

# Week 16

**Overview and Study Approach** This week will be exploring various lateral movement techniques that enable us to authenticate to a system and execute code by utilizing a user's hash or a Kerberos ticket.

**Learning Topics** 1) Lateral Movement in Active Directory

**Exercises**

- 23.1.1. WMI and WinRM
- 23.1.2. PsExec
- 23.1.3. Pass the Hash
- 23.1.4. Overpass the Hash
- 23.1.5. Pass the Ticket
- 23.1.6. DCOM
- 23.2.1. Golden Ticket
- 23.2.2. Shadow Copies

**Estimate Time (Hours)** 12

**Supplemental Learning\***

**Videos:**

- OffSec Academy Recordings:
  - [OSA - PEN - 200: Week 11A - Active Directory Attacks \(Part 1\)](#)
  - [OSA - PEN - 200: Week 12A - Active Directory Attack \(Part 1\)](#)
  - [OSA - PEN - 200: Week 13A - Active Directory Attack \(Part 2\)](#)
  - [OSA - PEN - 200: Week 14A - Active Directory Attack \(Part 2\)](#)
- OffSec Live Twitch Recordings:
  - [PEN-200 \(2023\): Active Directory Enumeration](#)
  - [Walkthrough of a PEN-200 AD Set](#)

**Relevant Labs:** N/A

# Week 17

## Overview and Study Approach

The final topic will cover a complete penetration testing scenario. The remaining time will be devoted to organizing and consolidating all the notes taken on learning concepts from previous weeks, as well as completing any remaining exercises.

## Learning Topics

1) Assembling the Pieces

## Exercises

N/A

## Estimate Time (Hours)

10

## Supplemental Learning\*

N/A

# Week 18

## Overview and Study Approach

It is recommended that the learner takes this week off away from the material and labs, this should help with regrouping, this week can be moved to fit the learner's schedule and liking.

## Learning Topics

N/A

## Learning Sections to Read

N/A

## Exercises

N/A

## Estimate Time (Hours)

10

## Supplemental Learning\*

N/A

# Week 19-22

## Overview and Study Approach

The learner may choose any of the first three challenges and attempt to complete the one chosen within the allotted time:

- Challenge 1 - Medtech
- Challenge 2 - Relia
- Challenge 3 - Skylark

---

Learning Topics

N/A

---

Exercises

N/A

---

Estimate Time (Hours)

40

---

Supplemental Learning\*

N/A

---

# Week 23-24

## Overview and Study Approach

This week the aim is to simulate an exam environment and assess your preparedness while identifying any areas that may require further attention. The time should be utilized to attempt to complete any of the OSCP grade labs (OSCP A, OSCP B, or OSCP C) in under 24 hours. These are retired OSCP exams.

## Learning Topics

N/A

## Exercises

N/A

## Estimate Time (Hours)

20

## Supplemental Learning\*

N/A