OffSec SOC-200
12 Week Learning Plan

Welcome to OffSec SOC-200! We are delighted to offer a customized learning plan designed to support your learning journey and ultimately enhance your preparedness for the OffSec Defense Analyst (OSDA) certification.

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

Table of Contents

Week 1

Overview and Study Approach	This week will focus on helping learners understand: 1) the enterprise network and its configurations 2) the phases in computer network exploitation 3) useful models for categorizing adversary methods 4) Linux Applications and Daemons 5) how to automate Defensive Analysis
Learning Module	Attacker Methodology Introduction Linux Endpoint Introduction
Learning Units	Attacker Methodology Introduction: 2.1 - 2.4 Linux Endpoint Introduction : 8.1 - 8.3
Videos for Reinforcement	Linux Endpoint Introduction: 5.1 - 5.2
Exercises	8.1.2 Logging on Linux and the Syslog Framework 8.1.3 Rsyslog Meets Journal 8.1.4 Web Daemon Logging 8.2.1 Python for Log Analysis 8.2.2 DevOps Tools 8.2.3 Hunting for Login Attempts
Challenges	None
Estimate Time (Hours)	20
Supplemental Learning*	SOC-100: Enterprise Network Architecture SOC-100: SOC Management Processes

Week 2

Overview and Study Approach	This week will focus on helping learners: 1) Understand Credential Abuse on Linux 2) Understand the impact of Common Web Application Attacks 3) Learn how to detect User-side privilege escalation attacks 4) Learn how to detect System-side privilege escalation attacks
Learning Module	Linux Server Side Attacks Linux Privilege Escalation
Learning Units	Linux Server Side Attacks: 9.1 - 9.3 Linux Privilege Escalation: 10.1 - 10.3
Videos for Reinforcement	Linux Server Side Attacks: 5.1 - 5.14 Linux Privilege Escalation: 7.1 - 7.2
Exercises	9.1.1. Suspicious Logins 9.1.2. Extra Mile I 9.1.3. Password Brute Forcing 9.1.4. Extra Mile II 9.2.1. Command Injection 9.2.2. Extra Mile III 9.2.3. SQL Injection 9.2.4. Extra Mile IV 10.1.1. Becoming a User 10.1.2. Backdooring a User 10.2.1. Abusing System Programs 10.2.2. Extra Mile I 10.2.3. Weak Permissions 10.2.4. Extra Mile II
Challenges	None
Estimate Time (Hours)	20
Supplemental Learning*	None

Week 3

Overview and Study Approach	This week will focus on helping learners: 1) Understand Log Management 2) Understand ELK Security 3) Demonstrate how to leverage the ELK SIEM for detecting four security incidents 4) Create rules that can identify the behavior if it were repeated
Learning Module	SIEM Part One: Intro to ELK SIEM Part Two: Combining the Logs
Learning Units	SIEM Part One: Intro to ELK: 17.1 - 17.3 SIEM Part Two: Combining the Logs: 18.1 - 18.5
Videos for Reinforcement	SIEM Part One: Intro to ELK: 15.1 - 15.2 SIEM Part Two: Combining the Logs: 16.1 - 16.4
Exercises	17.1.2. Elastic Stack (ELK) 17.1.3. ELK Integrations with OSQuery 17.2.1. Rules and Alerts 17.2.2. Timelines and Cases 18.1.1 Enumeration and Command Injection of web01 18.2.1 Brute Force and Authentication to appsrv01 18.3.1 Persistence and Privilege Escalation on appsrv01 18.4.1 Dump AD Database
Challenges	SOC-200 Labs: Challenge 1 SOC-200 Labs: Challenge 2 SOC-200 Labs: Challenge 3
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** • OffSec Academy Recordings: ○ OSA-SOC-200: Week 1 - Introduction to OSA SOC-200: 1.1 ○ OSA-SOC-200: Week 2 - Challenge 1 Demo: 2.1 ○ OSA-SOC-200: Week 3 - Challenge 2 Demo: 3.1

Week 4

Overview and Study Approach	This week will focus on helping learners understand: 1) Windows Processes and Registry 2) how to leverage the Command Prompt,VBScript and PowerShell 3) Programming on Windows 4) how to leverage Windows logs 5) the basics of Windows user authentication and its abuse 6) the impact of Common Web Aplication Attacks. 7) binary attacks through buffer overflows, and the artifacts they create
Learning Module	Windows Endpoint Introduction Windows Server Side Attacks
Learning Units	Windows Endpoint Introduction: 3.1-3.7 Windows Server Side Attacks: 4.1-4.4
Videos for Reinforcement	Windows Endpoint Introduction: 1.1-1.3 Windows Server Side Attacks: 2.1-2.3
Exercises	3.3.1 Command Prompt 3.3.2 Visual Basic Script (VBScript) 3.3.3 PowerShell 3.5.1 Introduction to Windows Events 3.5.2 PowerShell and Event Logs 3.6.1 System Monitor (Sysmon) 3.6.2 Sysmon and Event Viewer 3.6.3 Sysmon and PowerShell 3.6.4 Remote Access with PowerShell Core 4.1.2 Suspicious Logins 4.1.3 Brute Force Logins 4.2.2 Local File Inclusion 4.2.3 Command Injection 4.2.4 File Upload 4.2.5 Extra Mile 4.3.1 Binary Attacks 4.3.2 Windows Defender Exploit Guard (WDEG)
Challenges	None
Estimate Time (Hours)	20
Supplemental Learning*	None

Week 5

Overview and Study Approach	This week will focus on helping learners understand: 1) Client-Side attacks leveraging Microsoft Office 2) Windows PowerShell logging capabilities 3) common Privilege Escalation attacks on Windows and learn how to detect them
Learning Module	Windows Client-Side Attacks Windows Privilege Escalation
Learning Units	Windows Client-Side Attacks: 5.1-5.3 Windows Privilege Escalation: 6.1-6.3
Videos for Reinforcement	Windows Client-Side Attacks: 3.1-3.2 Windows Privilege Escalation: 4.1-4.2
Exercises	5.1.3 Using Macros 5.2.5 Case Study: PowerShell Logging for Phishing Attacks 5.2.6 Extra Mile 5.2.7 Obfuscating/Deobfuscating Commands 6.1.3 Bypassing UAC 6.2.1 Service Creation 6.2.2 Attacking Service Permissions 6.2.3 Leveraging Unquoted Service Paths
Challenges	None
Estimate Time (Hours)	20
Supplemental Learning*	None

Week 6

Overview and Study Approach	This week will focus on helping learners understand: 1) disk based Persistence 2) registry based Persistence 3) how attackers leverage Windows Authentication 4) how attackers abuse Kerberos Tickets
Learning Module	Windows Persistence Windows Lateral Movement
Learning Units	Windows Persistence: 7.1-7.3 Windows Lateral Movement: 15.1-15.3
Videos for Reinforcement	Windows Persistence: 9.1-9.2 Windows Lateral Movement: 13.1-13.2
Exercises	7.1.1 Persisting via Windows Service 7.1.2 Persisting via Scheduled Tasks 7.1.3 Persisting by DLL-Sideloading/Hijacking 7.2.1 Using Run Keys 7.2.2 Using Winlogon Helper 15.1.1 Pass The Hash 15.1.2 Brute Force Domain Credentials 15.1.3 Terminal Services 15.2.1 Pass The Ticket 15.2.2 Kerberoasting
Challenges	SOC-200 Labs: Challenge 3 SOC-200 Labs: Challenge 4
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** • OffSec Academy Recordings: ○ OSA-SOC-200: Week 4 - Challenge 4 Demo: 4.1

Week 7

Overview and Study Approach	This week will focus on helping learners understand: 1) Intrusion Detection Systems 2) how to detect C2 Infrastructure 3) the basics of Antivirus software 4) the Antimalware Scan Interface (AMSI) 5) the concept and implementation of network segmentation 6) egress filtering as well as attack and detection methods
Learning Module	Network Detections Antivirus Alerts and Evasion Network Evasion and Tunneling
Learning Units	Network Detections: 11.1-11.4 Antivirus Alerts and Evasion: 12.1-12.3 Network Evasion and Tunneling: 13.1-13.4
Videos for Reinforcement	Network Detections: 8.1-8.3 Antivirus Alerts and Evasion: 10.1-10.2 Network Evasion and Tunneling: 12.1-12.2
Exercises	11.1.2 Foundations of IDS and Rule Crafting 11.2.1 Known Vulnerabilities 11.2.2 Extra Mile I 11.2.3 Novel Vulnerabilities 11.3.1 C2 Infrastructure 11.3.2 Extra Mile II 11.3.3 Network Communications 12.1.2 Signature-Based Detection 12.1.3 Real-time Heuristic and Behavioral-Based Detection 12.2.2 Bypassing AMSI 13.2.1 Detecting Egress Busting 13.3.2 Port Forwarding and Tunneling in Practice
Challenges	None
Estimate Time (Hours)	25
Supplemental Learning*	None

Week 8

Overview and Study Approach	This week will focus on helping learners: 1) Learn how attackers abuse the Lightweight Directory Access Protocol 2) Learn how to detect Active Directory enumeration 3) Understand how attackers keep Domain Access
Learning Module	Active Directory Enumeration Active Directory Persistence
Learning Units	Active Directory Enumeration: 14.1-14.3 Active Directory Persistence: 16.1-16.2
Videos for Reinforcement	Active Directory Enumeration: 11.1-11.2 Active Directory Persistence: 14.1
Exercises	14.1.1 Understanding LDAP 14.1.2 Interacting with LDAP 14.1.3 Enumerating Active Directory with PowerView 14.2.1 Auditing Object Access 14.2.2 Baseline Monitoring 14.2.3 Using Honey Tokens 16.1.1 Domain Group Memberships 16.1.2 Domain User Modifications 16.1.3 Golden Tickets
Challenges	SOC-200 Labs: Challenge 5 SOC-200 Labs: Challenge 6
Estimate Time (Hours)	20
Supplemental Learning*	**Videos:** • OffSec Academy Recordings: ◦ OSA-SOC-200: Week 5 - Challenge 6 Demo: 5.1

Week 9

Overview and Study Approach	In this week learners will practice the skills they have learnt so far against the SOC-200 Challenge Labs.
Learning Module	None
Learning Units	None
Videos for Reinforcement	OSA-SOC-200: Week 6 - Challenge 8 Demo: 6.1
Exercises	None
Challenges	SOC-200 Labs: Challenge 7 SOC-200 Labs: Challenge 8
Estimate Time (Hours)	10
Supplemental Learning*	None

Week 10

Overview and Study Approach	In this week learners will practice the skills they have learnt so far against the SOC-200 Challenge Labs.
Learning Module	None
Learning Units	None
Videos for Reinforcement	OSA-SOC-200: Week 7 - Challenge 9 Demo: 7.1
Exercises	None
Challenges	SOC-200 Labs: Challenge 9 SOC-200 Labs: Challenge 10
Estimate Time (Hours)	10
Supplemental Learning*	None

Week 11

Overview and Study Approach	In this week learners will practice the skills they have learnt so far against the SOC-200 Challenge Labs.
Learning Module	None
Learning Units	None
Videos for Reinforcement	OSA-SOC-200: Week 8 - Challenge 11 Demo: 8.1
Exercises	None
Challenges	SOC-200 Labs: Challenge 11 SOC-200 Labs: Challenge 12
Estimate Time (Hours)	10
Supplemental Learning*	None

Week 12

Overview and Study Approach	In this week learners will practice the skills they have learnt so far against the SOC-200 Challenge Labs.
Learning Module	None
Learning Units	None
Videos for Reinforcement	None
Exercises	None
Challenges	SOC-200 Labs: Challenge 13 SOC-200 Labs: Challenge 14 SOC-200 Labs: Challenge 15
Estimate Time (Hours)	10
Supplemental Learning*	None