OffSec LIVE
PEN-200 | PWK

Learning Plan

Welcome to *OffSec Live: PEN-200*!

OffSec Live: PEN-200 is our scheduled and open streaming offering that includes a learning journey designed to facilitate learning, improve engagement and ultimately increase Offensive Security Certified Professional (OSCP) certification preparedness and achievement designed for OffSec students currently enrolled in PEN-200.

OffSec Live: PEN-200 includes a week-by-week learning journey - including learning objectives, recommended hours to dedicate, course modules to focus on and topic / lab exercises to complete - along with twice per week live Twitch streaming sessions where our OffSec team provides course specific, interactive learning guidance and lab concept demonstrations to better assist currently enrolled PEN-200 students. In addition, the *OffSec Live* offering will facilitate a dedicated *OffSec Live* Discord channel where currently enrolled PEN-200 students may collaborate to better understand the PEN-200 materials and methodology.

OffSec Live's weekly Twitch streaming is open to the public, and no additional fees will be charged to active OffSec subscription holders. Currently enrolled OffSec PEN-200 and Learn Unlimited subscription holders will also be provided access to an overall PEN-200 learning journey, recorded Twitch streaming sessions, specialized demonstration lab exercises, and an *OffSec Live* Discord channel. Those who do not have a current OffSec PEN-200 or Learn Unlimited subscription will have access to the weekly *OffSec Live* Twitch streaming sessions.

We hope you enjoy the offering and learning journey!

For additional questions, please see our *OffSec Live: PEN-200* **FAQs** here.

Getting Ready

To prepare for **PEN-200**, please see quick reference guidance that will help you get started with the **OffSec Training Library (OTL)** platform and improve your learning experience.

Getting Started	**Community, Mentoring and Support**
● Familiarize with the OTL ● Virtual Machine Requirements ● Lab Connectivity Guide	● Join OffSec Community (OffSec Discord Server) ● Join *OffSec Live: PEN-200* Community (dedicated OffSec Live Discord channel for student sharing and Office Hours)* ● Mentoring Guideline *(*help with course exercises and lab machines) ● Technical Support Services (help with technical issues such as platform, VPN, lab machine connectivity, etc.) ● OffSecOfficial - Twitch (Coming soon!) ● OffSec Forum (exchange ideas and course discuss issues)
PEN-200 Course	**Exam**
● Getting started with your PEN-200 course ● PEN-200 Topic Exercises (course exercises) ● Learning Path Guide (a set of lab machines that will help you get started)	● Exam Guide ● Exam Preparation (tips and suggestions to prepare for your OSCP exam) ● Exam Scheduling (how to schedule your OSCP exam) ● Reporting (OSCP exam reporting requirements)

**All currently enrolled PEN200 students will have access to the OffSec Live - PEN200 Discord channel.*

For more detailed information and FAQ, please click here!

Preparing for *OffSec Live: PEN-200* - weekly sessions guidance:

Recommended approach

1) Read content for the PEN-200 course Topic covered in the week.
2) Watch videos for PEN-200 Topic covered in the week.
3) Complete the topic exercises covered in the week.
4) Attempt the demo labs for the weekly topic prior to *OffSec Live* Wednesday session.
5) Attempt the PG-Play machine for the week prior to *OffSec Live* Friday session.
6) Complete the target lab exercises each week.

Please note this is a recommendation for preparing for each *OffSec Live* weekly session only. Please follow the recommended best approach + the Learning Journey below to most effectively prepare for the OSCP exam.

PG Play & Practice is *not* a substitute for the PEN200 lab environment. PG Play & Practice demonstrations are meant to augment the PEN200 learning experience only. Successful completion of PEN200 requires active and consistent engagement in the PEN200 lab environment. Those students who successfully complete all topic exercises and more than 50 PEN200 lab machines have a significantly higher OSCP pass rate than those who do not do so.

OffSec Live- PEN-200 Learning Journey:

	***OffSec Live: PEN-200* Learning Journey**	
Week 1: Terminal Best Practices	**Learning Objectives**	1) Understand some popular Linux command line programs. 2) Learn more about the Bash/ZSH environment. 3) Learn about environment variables and how to use them.
	Learning time (Hours)	10
	Office Hours	Monday, June 20 - NONE
	OffSec Live Weekly Demo	Wednesday, June 22 - 12 pm - 1 pm (ET): Kick-off Terminal best practices
	OffSec Live Weekly Demo	Friday, June 24 - 12 pm - 1 pm (ET): Terminal best practices
	Readings: Topic in LMS	Command-Line Fun: 3.1 - 3.9
	Watch: Videos in LMS	Command-Line Fun: 2.1 - 2.5
	Topic exercises to complete	3.1.4. Practice - The Bash Environment 3.2.6. Practice - Piping and Redirection 3.3.6. Practice - Text Searching and Manipulation 3.5.4. Practice - Comparing Files 3.6.4. Practice - Managing Processes 3.7.3. Practice - File and Command Monitoring 3.8.4. Practice - Downloading Files 3.9.4. Practice - Customizing the Bash Environment
	Lab exercises to complete	None

OffSec LIVE
PEN-200 | PWK

Week 2 : Practical Tools	**Learning Objectives**	1) Understand some practical tools that are found in every pentester's toolkit. 2) Understand packet structures and learn how to sniff traffic. 3) Identify the difference between reverse and bind shells.
	Learning time (Hours)	10
	Office Hours	Monday, June 27 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, June 29 - 12 pm - 1 pm (ET): Practical Tools
	OffSec Live Weekly Demo	Friday, July 1 - 12 pm - 1 pm (ET): PG Play - USV2017
	Readings: Topic in LMS	Practical Tools: 4.1 - 4.5
	Watch: Videos in LMS	Practical Tools: 3.1 - 3.5
	Topic exercises to complete	4.1.5. Practice - Netcat 4.2.5. Practice - Socat 4.3.9. Practice - PowerShell and Powercat 4.4.6. Practice - Wireshark 4.5.3. Practice - Tcpdump
	Lab exercises to complete	None

Week 3: Passive Information Gathering	**Learning Objectives**	1) Learn the importance of Passive Information Gathering. 2) Practical examples that show the impact of online presence.
	Learning time (Hours)	10
	Office Hours	Monday, July 4, 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, July 6 - 12 pm - 1 pm (ET): Passive Information Gathering
	OffSec Live Weekly Demo	Friday, July 8, 1 pm - 2 pm (ET): MegaCorpOne
	Readings: Topic in LMS	Passive Information Gathering: 6.1 - 6.16
	Watch: Videos in LMS	Passive Information Gathering: 5.1 - 5.14
	Topic exercises to complete	6.3.1. Practice - Whois Enumeration 6.4.1. Practice - Google Hacking 6.5.1. Practice - Netcraft 6.6.1. Practice Recon-ng 6.7.1. Practice - Open-Source Code 6.12.3. Practice - User Information Gathering 6.13.2. Practice - Social Media Tools
	Lab exercises to complete	10.11.1.222 - Chris

Week 4: Active Information Gathering	**Learning objectives**	1) Understand some common active information gathering techniques including port scanning and DNS, SMB, NFS, SMTP, and SNMP enumeration.
	Learning time (Hours)	10
	Office Hours	Monday, July 11, 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, July 13, 12 pm - 1 pm (ET): Active Information Gathering
	OffSec Live Weekly Demo	Friday, July 15, 12 pm - 1 pm (ET): Getting Started with PWK Labs - Jeremy Miller, PG Play - Born2root
	Readings: Topic in LMS	Active Information Gathering: 7.1 - 7.7
	Watch: Videos in LMS	Active Information Gathering: 6.1 - 6.3
	Topic exercises to complete	7.1.7. Practice - DNS Enumeration 7.2.3. Practice - Port Scanning 7.3.3. Practice - SMB Enumeration 7.4.3. Practice - NFS Enumeration 7.5.1. Practice - SMTP Enumeration 7.6.4. Practice - SNMP Enumeration
	Lab exercises to complete	Complete Initial Enumeration of PWK Labs. 10.11.1.5 - Alice 10.11.1.146 - Susie 10.11.1.231 - Mailman

Week 5: Vulnerability Scanning	**Learning objectives**	1) Understand automated and manual vulnerability scanning.
	Learning time (Hours)	10
	Office Hours	Monday, July 18, 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, July 20, 12 pm - 1 pm (ET): Vulnerability Scanning
	OffSec Live Weekly Demo	Friday, July 22 - 12 pm - 1 pm (ET): PG Play - Sumo
	Readings: Topic in LMS	Vulnerability Scanning: 8.1 - 8.4
	Watch: Videos in LMS	Vulnerability Scanning: 7.1 - 7.3
	Topic exercises to complete	8.2.9. Practice - Scanning with Individual Nessus Plugins 8.3.1. Practice - Vulnerability Scanning with Nmap
	Lab exercises to complete	Scan PWK Lab machines for specific vulnerabilities. 10.11.1.5 - Alice 10.11.1.146 - Susie

Week 6: Web Application Attacks	**Learning objectives**	1) Learn web application vulnerability enumeration and exploitation. 2) Demonstrate the exploitation of several common web application vulnerabilities listed in the OWASP Top 10.
	Learning time (Hours)	15
	Office Hours	Monday, July 25 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, July 27 - 12 pm - 1 pm (ET): Web App Attacks
	OffSec Live Weekly Demo	Friday, July 29 - 12 pm - 1 pm (ET): PG Box - PG Play - Dc5
	Readings: Topic in LMS	Web Application Attacks: 9.1 - 9.3
	Watch: Videos in LMS	Web Application Attacks: 8.1 - 8.3
	Topic exercises to complete	9.2.6. Practice - Web Application Enumeration 9.3.4. Practice - Web Application Assessment Tools
	Lab exercises to complete	10.11.1.71 - Alpha 10.11.1.72 - Beta 10.11.1.13 - Disco 10.11.1.50 - Bethany 10.11.1.217 - Hotline

Week 7: Web Application Attacks	**Learning Objectives**	1) Learn web application vulnerability enumeration and exploitation. 2) Demonstrate the exploitation of several common web application vulnerabilities listed in the OWASP Top 10.
	Learning time (Hours)	15
	Office Hours	Monday, August 1 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, August 3 - 12 pm - 1 pm (ET): Web App Attacks
	OffSec Live Weekly Demo	Friday, August 5 - 12 pm - 1 pm (ET): PG Play - Dc5
	Readings: Topic in LMS	Web Application Attacks: 9.4 - 9.10
	Watch: Videos in LMS	Web Application Attacks: 8.4 - 8.9
	Topic exercises to complete	9.5.2. Practice - Exploiting Admin Consoles 9.6.6. Practice - Cross-Site Scripting (XSS) 9.7.2. Practice - Directory Traversal Vulnerabilities 9.8.7. Practice - Remote File Inclusion (RFI) 9.8.10. Practice - PHP Wrappers 9.9.9. Practice - Extracting Data from the Database 9.9.11. Practice - From SQL Injection to Code Execution 9.9.13. Practice - Automating SQL Injection 9.10.1. Practice - Extra Miles
	Lab exercises to complete	10.11.1.222 - Chris 10.11.1.231 - Mailman 10.11.1.251 - Sean + 2 PWK Lab Machines

Week 8 : Catch-up Week	**Learning objectives**	None
	Learning time (Hours)	None
	Office Hours	None
	OffSec Live Weekly Demo	None
	Readings: Topic in LMS	None
	Watch: Videos in LMS	None
	Topic exercises to complete	None
	Lab exercises to complete	None

Week 9: Introduction to Buffer Overflows and Windows Buffer Overflows	**Learning objectives**	1) Learn the principles behind a buffer overflow attack. 2) Discover and exploit a remote buffer overflow.
	Learning time (Hours)	15
	Office Hours	Monday, August 15 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, August 17 - 12 pm - 1 pm (ET): Introduction to Buffer Overflows
	OffSec Live Weekly Demo	Friday, August 19 - 12 pm - 1 pm (ET): Windows Buffer Overflow
	Readings: Topic in LMS	Introduction to Buffer Overflows: 10.1 - 10.3 Windows Buffer Overflows: 11.1 - 11.3
	Watch: Videos in LMS	Introduction to Buffer Overflows: 9.1 - 9.2 Windows Buffer Overflows: 10.1 - 10.3
	Topic exercises to complete	10.2.5. Practice - Introduction to Buffer Overflows 11.1.2. Practice - Discovering the Vulnerability 11.2.4. Practice - Controlling EIP 11.2.8. Practice - Checking for Bad Characters 11.2.10. Practice - Finding a Return Address 11.2.15. Practice - Improving the Exploit 11.2.16. Extra Mile Exercises
	Lab exercises to complete	None

Week 10: Linux Buffer Overflows	**Learning objectives**	1) Introduction Linux buffer overflows.
	Learning time (Hours)	15
	Office Hours	Monday, August 22 - 12 pm - 1 pm (ET): Linux Buffer Overflows
	OffSec Live Weekly Demo	Wednesday, August 24 - 12 pm - 1 pm (ET): Linux Buffer Overflows
	OffSec Live Weekly Demo	Friday, August 26 - 12 pm - 1 pm (ET): PG Play - Covfefe
	Readings: Topic in LMS	Linux Buffer Overflows: 12.1 - 12.8
	Watch: Videos in LMS	Linux Buffer Overflows: 11.1 - 11.8
	Topic exercises to complete	12.2.1. Practice - Replicating the Crash 12.3.1. Practice - Controlling EIP 12.5.1. Practice - Checking for Bad Characters 12.6.1. Practice - Finding a Return Address 12.7.1. Practice - Getting a Shell
	Lab exercises to complete	3 PWK Labs Machines

Week 11: Client-Side Attacks	**Learning objectives**	1) Identify factors that are important to consider for client-side attacks. 2) Learn exploitation scenarios involving malicious HTML Applications and Microsoft Word documents.
	Learning time (Hours)	15
	Office Hours	Monday, August 29 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, August 31 - 12 pm - 1 pm (ET): Client-Side Attacks
	OffSec Live Weekly Demo	Friday, September 2 - 12 pm - 1 pm (ET): PG Play - BTRSys2.1
	Readings: Topic in LMS	Client-Side Attacks: 13.1 - 13.4
	Watch: Videos in LMS	Client-Side Attacks: 12.1 - 12.3
	Topic exercises to complete	13.1.5. Practice - Know Your Target 13.2.3. Practice - Leveraging HTML Applications 13.3.3. Practice - Microsoft Word Macro 13.3.5. Practice - Object Linking and Embedding 13.3.7. Practice - Evading Protected View
	Lab exercises to complete	3 PWK Labs Machines

Week 12: Locating and Fixing Public Exploits	**Learning objectives**	1) Identify online resources that host exploits for publicly known vulnerabilities. 2) Learn how to modify public exploit code to fit a specific attack platform and target.
	Learning time (Hours)	15
	Office Hours	Monday, September 5 - 1 pm - 2 pm (ET)
	OffSec Live Weekly Demo	Wednesday, September 7 - 1 pm - 2 pm (ET): Locating Public Exploits and Fixing Exploits
	OffSec Live Weekly Demo	Friday, September 9 - 1 pm - 2 pm (ET): PG Play - Bbscute
	Readings: Topic in LMS	Locating Public Exploits: 14.1 - 14.4 Fixing Exploits: 15.1 - 15.3
	Watch: Videos in LMS	Locating Public Exploits: 13.1 - 13.3 Fixing Exploits: 14.1 - 14.2
	Topic exercises to complete	14.3.1. Practice - Putting It All Together 15.1.4. Practice - Cross-Compiling Exploit Code 15.1.6. Practice - Changing the Socket Information 15.1.8. Practice - Changing the Return Address 15.1.10. Practice - Changing the Payload 15.2.4. Practice - Changing Connectivity Information 15.2.6. Practice - Troubleshooting the "index out of range" Error
	Lab exercises to complete	10.11.1.146 - Susie 10.11.1.71 - Alpha 10.11.1.71 - Beta 10.11.1.50 - Bethany 10.11.1.231 - Mailman 10.11.1.5 - Alice

Week 13: File Transfers and Anti Virus Bypass	**Learning objectives:**	1) Identify various file transfer methods that can be used in an assessment. 2) Learn how to bypass antivirus software on target machines.
	Learning time (Hours)	18
	Office Hours	Monday, September 12 -1 pm - 2 pm (ET)
	OffSec Live Weekly Demo	Wednesday, September 14 - 1 pm - 2 pm (ET): File Transfers and Anti Virus Bypass
	OffSec Live Weekly Demo	Friday, September 16 - 1 pm - 2 pm (ET): PG Play - Inclusiveness
	Readings: Topic in LMS	File Transfers: 16.1 - 16.3 Anti Virus Bypass : 17.1 - 17.4
	Watch: Videos in LMS	File Transfers: 15.1 - 15.2 Anti Virus Bypass: 16.1 - 16.3
	Topic exercises to complete	16.1.4. Practice - Considerations and Preparations 16.2.6. Practice - Transferring Files with Windows Hosts 17.3.5. Practice - Antivirus Evasion
	Lab exercises to complete	10.11.1.251 - Sean 10.11.1.146 - Susie + 3 PWK Lab Machines

Week 14: Privilege Escalation (Linux, Windows)	**Learning objectives**	1) Learn privilege escalation techniques to elevate privileges on Windows and Linux-based targets from non-privileged user accounts.
	Learning time (Hours)	18
	Office Hours	Monday, September 19 -12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, September 21 - 12 pm - 1 pm (ET): Privilege Escalation (Linux, Windows)
	OffSec Live Weekly Demo	Friday, September 23 - 12 pm - 1 pm (ET): PG Play - Funbox
	Readings: Topic in LMS	Privilege Escalation: 18.1 - 18.4
	Watch: Videos in LMS	Privilege Escalation: 17.1 - 17.3
	Topic exercises to complete	18.1.2. Practice - Manual Enumeration 18.1.4. Practice - Automated Enumeration 18.2.4. Practice - User Account Control (UAC) Bypass: fodhelper.exe Case Study 18.2.6. Practice - Insecure File Permissions: Serviio Case Study 18.3.3. Practice - Insecure File Permissions: Cron Case Study 18.3.5. Practice - Insecure File Permissions: /etc/passwd Case Study
	Lab exercises to complete	10.11.1.13 - Disco + 3 PWK Lab Machines

Week 15: Windows Privilege Escalation Vectors	**Learning objectives**	1) Learn privilege escalation techniques to elevate privileges on Windows and Linux-based targets from non-privileged user accounts.
	Learning time (Hours)	20
	Office Hours	Monday, September 26 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, September 28 - 12 pm - 1 pm (ET): Windows Privilege Escalation Vectors
	OffSec Live Weekly Demo	Friday, September 30 - 1 pm - 2 pm (ET): PG Practice - Spaghetti
	Readings: Topic in LMS	None
	Watch: Videos in LMS	None
	Topic exercises to complete	None
	Lab exercises to complete	3 PWK Lab Machines

Week 16: Password Attacks	**Learning objectives**	1) Learn how to leverage password attacks to gain access to a Windows-based target.
	Learning time (Hours)	20
	Office Hours	Monday, October 3 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, October 5 - 12 pm - 1 pm (ET): Password Attacks
	OffSec Live Weekly Demo	Friday, October 7 - 12 pm - 1 pm (ET): PG Play - FowSniff
	Readings: Topic in LMS	Password Attacks: 19.1 - 19.5
	Watch: Videos in LMS	Password Attacks: 18.1 - 18.4
	Topic exercises to complete	19.2.1. Practice - Brute Force Wordlists 19.3.2. Practice - HTTP htaccess Attack with Medusa 19.3.4. Practice - Remote Desktop Protocol Attack with Crowbar 19.3.6. Practice - SSH Attack with THC-Hydra 19.3.8. Practice - HTTP POST Attack with THC-Hydra 19.4.2. Practice - Retrieving Password Hashes 19.4.4. Practice - Passing the Hash in Windows 19.4.6. Practice - Password Cracking
	Lab exercises to complete	10.11.1.123 - xor-app59 + 4 PWK Lab Machines

Week 17 : Port Redirection and Tunneling	**Learning objectives**	1) Understand various forms of port redirection, tunneling, and traffic encapsulation. 2) Manipulate the directional flow of targeted traffic in restricted network environments.
	Learning time (Hours)	20
	Office Hours	Monday, October 10 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, October 12 - 12 pm - 1 pm (ET): Port Redirection and Tunneling
	OffSec Live Weekly Demo	Friday, October 14 - 12 pm - 1 pm (ET): PG Practice - Nukem
	Readings: Topic in LMS	Port Redirection and Tunneling: 20.1 - 20.6
	Watch: Videos in LMS	Port Redirection and Tunneling: 19.1 - 19.5
	Topic exercises to complete	20.1.2. Practice - Port Forwarding 20.2.6. Practice - SSH Dynamic Port Forwarding 20.3.1. Practice - PLINK.exe 20.4.1. Practice - NETSH 20.5.1. Practice - HTTPTunnel-ing Through Deep Packet Inspection
	Lab exercises to complete	4 PWK Lab Machines

Week 18 : Active Directory Attacks (Part 1)	**Learning objectives**	1) Learn the basic concepts of Active Directory. 2) Demonstrate Active Directory enumeration, authentication, and lateral movement techniques.
	Learning time (Hours)	20
	Office Hours	Monday, October 17 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, October 19 - 12 pm - 1 pm: Active Directory Attacks (Part 1)
	OffSec Live Weekly Demo	Friday, October 21 - 12 pm - 1 pm (ET): TBD
	Readings: Topic in LMS	Active Directory Attacks: 21.1 - 21.6
	Watch: Videos in LMS	Active Directory Attacks: 20.1 - 20.5
	Topic exercises to complete	21.2.2. Practice - Traditional Approach 21.2.4. Practice - A Modern Approach 21.2.6. Practice - Resolving Nested Groups 21.2.8. Practice - Currently Logged on Users 21.2.10. Practice - Enumeration Through Service Principal Names 21.3.4. Practice - Cached Credential Storage and Retrieval 21.4.3. Practice - Overpass the Hash 21.4.5. Practice - Pass the Ticket 21.4.7. Practice - Distributed Component Object Model 21.5.4. Practice - Active Directory Attacks
	Lab exercises to complete	4 PWK Lab Machines

Week 19: Active Directory Attacks (Part 2)	**Learning objectives**	1) Learn the basic concepts of Active Directory 2) Demonstrate Active Directory enumeration, authentication, and lateral movement techniques.
	Learning time (Hours)	20
	Office Hours	Monday, October 24 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, October 26 - 12 pm - 1 pm (ET): Active Directory Attacks (Part 2)
	OffSec Live Weekly Demo	Friday, October 28 - 12 pm - 1 pm (ET): TBD
	Readings: Topic in LMS	None
	Watch: Videos in LMS	None
	Topic exercises to complete	None
	Lab exercises to complete	4 PWK Lab Machines

Week 20: Assembling the pieces	**Learning objectives:**	1) Conduct a simulated penetration test inspired by real-world findings.
	Learning time (Hours)	20
	Office Hours	Monday, October 31 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, November 2 - 12 pm - 1 pm (ET): Assembling the pieces
	OffSec Live Weekly Demo	Friday, November 4 - 12 pm - 1 pm (ET): TBD
	Readings: Topic in LMS	Assembling the pieces: 24.1 - 24.10
	Watch: Videos in LMS	Assembling the pieces: 23.1 - 23.9
	Topic exercises to complete	None
	Lab exercises to complete	4 PWK Lab Machines

Week 21:	**Learning objectives:**	1) Practice concepts with PWK Lab machines/Challenge Labs.
	Learning time (Hours)	20
	Office Hours	Monday, November 7 - 12 pm - 1 pm (ET)
	OffSec Live Weekly Demo	Wednesday, November 9 - 12 pm - 1 pm (ET): Discussion on cybersecurity careers
	OffSec Live Weekly Demo	Friday, November 11: None
	Readings: Topic in LMS	None
	Watch: Videos in LMS	None
	Topic exercises to complete	None
	Lab exercises to complete	5 PWK Lab Machines

Week 22	**Learning objectives:**	1) Practice concepts with PWK Lab machines/Challenge Labs.
	Learning time (Hours)	20
	Office Hours	Monday, November 14: None
	OffSec Live Weekly Demo	Wednesday, November 16 - 12 pm - 1 pm (ET): How to prepare for the OSCP exam
	OffSec Live Weekly Demo	Friday, November 18: None
	Readings: Topic in LMS	None
	Watch: Videos in LMS	None
	Topic exercises to complete	None
	Lab exercises to complete	5 PWK Lab Machines

Week 23	**Learning objectives:**	1) Practice concepts with PWK Lab machines/Challenge Labs.
	Learning time (Hours)	20
	Office Hours	Monday, November 21: None
	OffSec Live Weekly Demo	Wednesday, November 23: None
	OffSec Live Weekly Demo	Friday, November 25: None
	Readings: Topic in LMS	None
	Watch: Videos in LMS	None
	Topic exercises to complete	None
	Lab exercises to complete	5 PWK Lab Machines

Week 24	**Learning objectives:**	1) Practice concepts with PWK Lab machines/Challenge Labs.
	Learning time (Hours)	20
	Office Hours	Monday, November 28: None
	OffSec Live Weekly Demo	Wednesday, November 30 12 pm - 1 pm (ET): AMA Session - Morten, Sicky and Jeremy
	OffSec Live Weekly Demo	Friday, December 2: None
	Readings: Topic in LMS	None
	Watch: Videos in LMS	None
	Topic exercises to complete	None
	Lab exercises to complete	5 PWK Lab Machines

Week 25	**Learning objectives:**	1) Attempt the Mock Exam.
	Learning time (Hours)	20
	Office Hours	Monday, December 5: None
	OffSec Live Weekly Demo	Wednesday, December 7: None
	OffSec Live Weekly Demo	Friday, December 9: None
	Readings: Topic in LMS	None
	Watch: Videos in LMS	None
	Topic exercises to complete	None
	Lab exercises to complete	5 PWK Lab Machines