


PEN-200 (PWK) Syllabus

Learning Module	Learning Units	Learning Objectives
Penetration Testing with Kali Linux : General Course Introduction	Welcome to PWK	<ul style="list-style-type: none"> Take inventory over what's included in the course
		<ul style="list-style-type: none"> Set up an Attacking Kali VM
		<ul style="list-style-type: none"> Connect to and interact over the PWK VPN
		<ul style="list-style-type: none"> Understand how to complete Module Exercises
	How to Approach the Course	<ul style="list-style-type: none"> Conceptualize a learning model based on increasing uncertainty
		<ul style="list-style-type: none"> Understand the different learning components included in PEN-200
Summary of PWK Learning Modules	<ul style="list-style-type: none"> Obtain a high level overview of what's covered in each PEN-200 Learning Module 	
Introduction to Cybersecurity	The Practice of Cybersecurity	<ul style="list-style-type: none"> Recognize the challenges unique to information security
		<ul style="list-style-type: none"> Understand how "offensive" and "defensive" security reflect each other
		<ul style="list-style-type: none"> Begin to build a mental model of useful mindsets applicable to information security
	Threats and Threat Actors	<ul style="list-style-type: none"> Understand how attackers and defenders learn from each other
		<ul style="list-style-type: none"> Understand the differences between risks, threats, vulnerabilities, and exploits

Introduction to Cybersecurity	Threats and Threat Actors	<ul style="list-style-type: none"> List and describe different classes of threat actor
		<ul style="list-style-type: none"> Recognize some recent cybersecurity attacks
	The CIA Triad	<ul style="list-style-type: none"> Understand why it's important to protect the confidentiality of information
		<ul style="list-style-type: none"> Learn why it's important to protect the integrity of information
		<ul style="list-style-type: none"> Explore why it's important to protect the availability of information
	Security Principles, Controls, and Strategies	<ul style="list-style-type: none"> Understand the importance of multiple layers of defense in a security strategy
		<ul style="list-style-type: none"> Describe threat intelligence and its applications in an organization
		<ul style="list-style-type: none"> Learn why access and user privileges should be restricted as much as possible
		<ul style="list-style-type: none"> Understand why security should not depend on secrecy
		<ul style="list-style-type: none"> Identify policies that can mitigate threats to an organization
		<ul style="list-style-type: none"> Determine which controls an organization can use to mitigate cybersecurity threats
	Cybersecurity Laws, Regulations, Standards, and Frameworks	<ul style="list-style-type: none"> Gain a broad understanding of various legal and regulatory issues surrounding cybersecurity
		<ul style="list-style-type: none"> Understand different frameworks and standards that help organizations orient their cybersecurity activities
Career Opportunities in Cybersecurity	<ul style="list-style-type: none"> Identify career opportunities in cybersecurity 	

Effective Learning Strategies	Learning Theory	<ul style="list-style-type: none"> Understand the general state of our understanding about education and education theory
		<ul style="list-style-type: none"> Understand the basics of memory mechanisms and dual encoding
		<ul style="list-style-type: none"> Recognize some of the problems faced by learners, including "The Curve of Forgetting" and cognitive load
	Unique Challenges to Learning Technical Skills	<ul style="list-style-type: none"> Recognize the differences and advantages of digital learning materials
		<ul style="list-style-type: none"> Understand the challenge of preparing for unknown scenarios
		<ul style="list-style-type: none"> Understand the potential challenges of remote or asynchronous learning
	OffSec Methodology	<ul style="list-style-type: none"> Understand what is meant by a <i>Demonstrative Methodology</i>
		<ul style="list-style-type: none"> Understand the challenge of preparing for unknown scenarios
		<ul style="list-style-type: none"> Understand the potential challenges of remote or asynchronous learning
	Case Study: chmod -x chmod	<ul style="list-style-type: none"> Review a sample of learning material about the executable permission, expand beyond the initial information set, and work through a problem
		<ul style="list-style-type: none"> Understand how OffSec's approach to teaching is reflected in the sample material
	Tactics and Common Methods	<ul style="list-style-type: none"> Learn about Retrieval Practice
		<ul style="list-style-type: none"> Understand Spaced Practice

Effective Learning Strategies	Tactics and Common Methods	<ul style="list-style-type: none"> Explore the SQ3R and PQ4R Method
		<ul style="list-style-type: none"> Examine the Feynman Technique
		<ul style="list-style-type: none"> Understand the Leitner System
	Advice and Suggestions on Exams	<ul style="list-style-type: none"> Develop strategies for dealing with exam-related stress
		<ul style="list-style-type: none"> Recognize when you might be ready to take the exam
		<ul style="list-style-type: none"> Understand a practical approach to exams
	Practical Steps	<ul style="list-style-type: none"> Create a long term strategy
		<ul style="list-style-type: none"> Understand how to use a time allotment strategy
		<ul style="list-style-type: none"> Learn how and when to narrow your focus
		<ul style="list-style-type: none"> Understand the importance of a group of co-learners and finding a community
<ul style="list-style-type: none"> Explore how best to pay attention and capitalize on our own successful learning strategies 		
Report Writing for Penetration Testers	Understanding Note-Taking	<ul style="list-style-type: none"> Review the deliverables for penetration testing engagements
		<ul style="list-style-type: none"> Understand the importance of note portability

Report Writing for Penetration Testers	Understanding Note-Taking	<ul style="list-style-type: none"> Identify the general structure of pentesting documentation
		<ul style="list-style-type: none"> Choose the right note-taking tool
		<ul style="list-style-type: none"> Understand the importance of taking screenshots
		<ul style="list-style-type: none"> Use tools to take screenshots
	Writing Effective Technical Penetration Testing Reports	<ul style="list-style-type: none"> Identify the purpose of a technical report
		<ul style="list-style-type: none"> Understand how to specifically tailor content
		<ul style="list-style-type: none"> Construct an Executive Summary
		<ul style="list-style-type: none"> Account for specific test environment considerations
		<ul style="list-style-type: none"> Create a technical summary
		<ul style="list-style-type: none"> Describe technical findings and recommendations
	<ul style="list-style-type: none"> Recognize when to use appendices, resources, and references 	
Information Gathering	The Penetration Testing Lifecycle	<ul style="list-style-type: none"> Understand the stages of a Penetration Test
		<ul style="list-style-type: none"> Learn the role of Information Gathering inside each stage

Information Gathering	The Penetration Testing Lifecycle	<ul style="list-style-type: none"> Understand the differences between Active and Passive Information Gathering
	Passive Information Gathering	<ul style="list-style-type: none"> Understand the two different Passive Information Gathering approaches
		<ul style="list-style-type: none"> Learn about Open Source Intelligence (OSINT)
		<ul style="list-style-type: none"> Understand Web Server and DNS passive information gathering
	Active Information Gathering	<ul style="list-style-type: none"> Learn to perform Netcat and Nmap port scanning
		<ul style="list-style-type: none"> Conduct DNS, SMB, SMTP, and SNMP Enumeration
<ul style="list-style-type: none"> Understand Living off the Land Techniques 		
Vulnerability Scanning	Vulnerability Scanning Theory	<ul style="list-style-type: none"> Gain a basic understanding of the Vulnerability Scanning process
		<ul style="list-style-type: none"> Learn about the different types of Vulnerability Scans
		<ul style="list-style-type: none"> Understand the considerations of a Vulnerability Scan
	Vulnerability Scanning with Nessus	<ul style="list-style-type: none"> Install Nessus
		<ul style="list-style-type: none"> Understand the different Nessus Components
		<ul style="list-style-type: none"> Configure and perform a vulnerability scan

Vulnerability Scanning	Vulnerability Scanning with Nessus	<ul style="list-style-type: none"> Understand and work with the results of a vulnerability scan with Nessus
		<ul style="list-style-type: none"> Provide credentials to perform an authenticated vulnerability scan
		<ul style="list-style-type: none"> Gain a basic understanding of Nessus Plugins
	Vulnerability Scanning with Nmap	<ul style="list-style-type: none"> Understand the basics of the Nmap Scripting Engine (NSE)
		<ul style="list-style-type: none"> Perform a lightweight Vulnerability Scan with Nmap
		<ul style="list-style-type: none"> Work with custom NSE scripts
Introduction to Web Applications	Web Application Assessment Methodology	<ul style="list-style-type: none"> Understand web application security testing requirements
		<ul style="list-style-type: none"> Learn different types of methodologies of web application testing
		<ul style="list-style-type: none"> Learn about the OWASP Top10 and most common web vulnerabilities
	Web Application Assessment Tools	<ul style="list-style-type: none"> Perform common enumeration techniques on web applications
		<ul style="list-style-type: none"> Understand Web Proxies theory
		<ul style="list-style-type: none"> Learn how Burp Suite proxy works for web application testing
	Web Application Enumeration	<ul style="list-style-type: none"> Learn how to debug Web Application source code

Introduction to Web Applications	Web Application Enumeration	<ul style="list-style-type: none"> Understand how to enumerate and inspect Headers, Cookies, and Source Code
		<ul style="list-style-type: none"> Learn how to conduct API testing methodologies
	Cross-Site Scripting (XSS)	<ul style="list-style-type: none"> Understand Cross-Site Scripting vulnerability types
		<ul style="list-style-type: none"> Exploit basic Cross-Site Scripting
Common Web Application Attacks	Directory Traversal	<ul style="list-style-type: none"> Understand absolute and relative paths
		<ul style="list-style-type: none"> Learn how to exploit directory traversal vulnerabilities
		<ul style="list-style-type: none"> Use encoding for special characters
	File Inclusion Vulnerabilities	<ul style="list-style-type: none"> Learn the difference between File Inclusion and Directory Traversal vulnerabilities
		<ul style="list-style-type: none"> Gain an understanding of File Inclusion vulnerabilities
		<ul style="list-style-type: none"> Understand how to leverage Local File Inclusion (LFI) to obtain code execution
		<ul style="list-style-type: none"> Explore PHP Wrapper usage
<ul style="list-style-type: none"> Learn how to perform Remote File Inclusion (RFI) attacks 		

Common Web Application Attacks	File Upload Vulnerabilities	<ul style="list-style-type: none"> Understand File Upload Vulnerabilities
		<ul style="list-style-type: none"> Learn how to identify File Upload vulnerabilities
	File Upload Vulnerabilities	<ul style="list-style-type: none"> Explore different vectors to exploit File Upload vulnerabilities
	Command Injection	<ul style="list-style-type: none"> Learn about command injection in web applications
		<ul style="list-style-type: none"> Use operating system commands for OS command injection
		<ul style="list-style-type: none"> Understand how to leverage command injection to gain system access
SQL Injection Attacks	SQL Theory and Database Types	<ul style="list-style-type: none"> Refresh SQL theory fundamentals
		<ul style="list-style-type: none"> Learn different DB types
		<ul style="list-style-type: none"> Understand different SQL syntax
	Manual SQL Exploitation	<ul style="list-style-type: none"> Manually identify SQL injection vulnerabilities
		<ul style="list-style-type: none"> Understand UNION SQLi payloads
		<ul style="list-style-type: none"> Learn about Error SQLi payloads
		<ul style="list-style-type: none"> Understand Blind SQLi payloads

SQL Injection Attacks	Manual and Automated Code Execution	<ul style="list-style-type: none"> Exploit MSSQL Databases with xp_cmdshell
		<ul style="list-style-type: none"> Automate SQL Injection with SQLmap
Client-Side Attacks	Target Reconnaissance	<ul style="list-style-type: none"> Gather information to prepare client-side attacks
		<ul style="list-style-type: none"> Leverage client fingerprinting to obtain information
	Exploiting Microsoft Office	<ul style="list-style-type: none"> Understand variations of Microsoft Office client-side attacks
		<ul style="list-style-type: none"> Install Microsoft Office
		<ul style="list-style-type: none"> Leverage Microsoft Word Macros
	Abusing Windows Library Files	<ul style="list-style-type: none"> Prepare an attack with Windows library files
<ul style="list-style-type: none"> Leverage Windows shortcuts to obtain code execution 		
Locating Public Exploits	Getting Started	<ul style="list-style-type: none"> Understand the risk of executing untrusted exploits
		<ul style="list-style-type: none"> Understand the importance of analyzing the exploit code before execution
	Online Exploit Resources	<ul style="list-style-type: none"> Access multiple online exploit resources
		<ul style="list-style-type: none"> Differentiate between various online exploit resources

		<ul style="list-style-type: none"> Understand the risks between online exploit resources
		<ul style="list-style-type: none"> Use Google search operators to discover public exploits
Locating Public Exploits	Offline Exploit Resources	<ul style="list-style-type: none"> Access Multiple Exploit Frameworks
		<ul style="list-style-type: none"> Use SearchSploit
		<ul style="list-style-type: none"> Use Nmap NSE Scripts
	Exploiting a Target	<ul style="list-style-type: none"> Follow a basic penetration test workflow to enumerate a target system
		<ul style="list-style-type: none"> Completely exploit a machine that is vulnerable to public exploits
		<ul style="list-style-type: none"> Discover appropriate exploits for a target system
		<ul style="list-style-type: none"> Execute a public exploit to gain a limited shell on a target host
Fixing Exploits	Fixing Memory Corruption Exploits	<ul style="list-style-type: none"> Understand high-level buffer overflow theory
		<ul style="list-style-type: none"> Cross-compile binaries
		<ul style="list-style-type: none"> Modify and update memory corruption exploits
	Fixing Web Exploits	<ul style="list-style-type: none"> Fix Web application exploits

		<ul style="list-style-type: none"> • Troubleshoot common web application exploit issues
Antivirus Evasion	Antivirus Evasion Software Key Components and Operations	<ul style="list-style-type: none"> • Recognize known vs unknown threats
		<ul style="list-style-type: none"> • Understand AV key components
		<ul style="list-style-type: none"> • Understand AV detection engines
	AV Evasion in Practice	<ul style="list-style-type: none"> • Understand antivirus evasion testing best practices
		<ul style="list-style-type: none"> • Manually evade AV solutions
		<ul style="list-style-type: none"> • Leverage automated tools for AV evasion
Password Attacks	Attacking Network Services Logins	<ul style="list-style-type: none"> • Attack SSH and RDP Logins
		<ul style="list-style-type: none"> • Attack HTTP POST login forms
	Password Cracking Fundamentals	<ul style="list-style-type: none"> • Understand the fundamentals of password cracking
		<ul style="list-style-type: none"> • Mutate Wordlists
		<ul style="list-style-type: none"> • Explain the basic password cracking methodology

		<ul style="list-style-type: none"> • Attack password manager key files
		<ul style="list-style-type: none"> • Attack the passphrase of SSH private keys
Password Attacks	Working with Password Hashes	<ul style="list-style-type: none"> • Obtain and crack NTLM hashes
		<ul style="list-style-type: none"> • Pass NTLM hashes
		<ul style="list-style-type: none"> • Obtain and crack Net-NTLMv2 hashes
		<ul style="list-style-type: none"> • Relay Net-NTLMv2 hashes

Windows Privilege Escalation	Enumerating Windows	<ul style="list-style-type: none"> • Understand Windows privileges and access control mechanisms
		<ul style="list-style-type: none"> • Obtain situational awareness
		<ul style="list-style-type: none"> • Search for sensitive information on Windows systems
		<ul style="list-style-type: none"> • Find sensitive information generated by PowerShell
		<ul style="list-style-type: none"> • Become familiar with automated enumeration tools
	Leveraging Windows Services	<ul style="list-style-type: none"> • Hijack service binaries
		<ul style="list-style-type: none"> • Hijack service DLLs

		<ul style="list-style-type: none"> Abuse Unquoted service paths
Windows Privilege Escalation	Abusing other Windows Components	<ul style="list-style-type: none"> Leverage Scheduled Tasks to elevate our privileges
		<ul style="list-style-type: none"> Understand the different types of exploits leading to privilege escalation
		<ul style="list-style-type: none"> Abuse privileges to execute code as privileged user accounts
Linux Privilege Escalation	Enumerating Linux	<ul style="list-style-type: none"> Understand files and user privileges on Linux
		<ul style="list-style-type: none"> Perform manual enumeration
		<ul style="list-style-type: none"> Conduct automated enumeration
	Exposed Confidential Information	<ul style="list-style-type: none"> Understand user history files
		<ul style="list-style-type: none"> Inspect user trails for credential harvesting
		<ul style="list-style-type: none"> Inspect system trails for credential harvesting
	Insecure File Permissions	<ul style="list-style-type: none"> Abuse insecure cron jobs to escalate privileges
		<ul style="list-style-type: none"> Abuse Insecure file permissions to escalate privileges
	Insecure System Components	<ul style="list-style-type: none"> Abuse SUID programs and capabilities for privilege escalation
		<ul style="list-style-type: none"> Circumvent special sudo permissions to

		escalate privileges
Linux Privilege Escalation	Insecure System Components	<ul style="list-style-type: none"> Enumerate the system's kernel for known vulnerabilities, then abuse them for privilege escalation
Port Redirection and SSH Tunneling	Port Forwarding with *NIX Tools	<ul style="list-style-type: none"> Learn about port forwarding
		<ul style="list-style-type: none"> Understand why and when to use port forwarding
		<ul style="list-style-type: none"> Use Socat for port forwarding
	SSH Tunneling	<ul style="list-style-type: none"> Learn about SSH tunneling
		<ul style="list-style-type: none"> Understand how to perform SSH local port forwarding
		<ul style="list-style-type: none"> Understand how to perform SSH dynamic port forwarding
		<ul style="list-style-type: none"> Understand how to perform SSH remote port forwarding
		<ul style="list-style-type: none"> Understand how to perform SSH remote dynamic port forwarding
	Port Forwarding with Windows Tools	<ul style="list-style-type: none"> Understand port forwarding and tunneling with ssh.exe on Windows
		<ul style="list-style-type: none"> Understand port forwarding and tunneling with Plink
<ul style="list-style-type: none"> Understand port forwarding with Netsh 		
Advanced Tunneling	Tunneling Through Deep Packet Inspection	<ul style="list-style-type: none"> Learn about HTTP tunneling

		<ul style="list-style-type: none"> • Perform HTTP tunneling with Chisel
		<ul style="list-style-type: none"> • Learn about DNS tunneling
		<ul style="list-style-type: none"> • Perform DNS tunneling with dnscat
The Metasploit Framework	Getting Familiar with Metasploit	<ul style="list-style-type: none"> • Setup and navigate Metasploit
		<ul style="list-style-type: none"> • Use auxiliary modules
		<ul style="list-style-type: none"> • Leverage exploit modules
	Using Metasploit Payloads	<ul style="list-style-type: none"> • Understand the differences between staged and non-staged payloads
		<ul style="list-style-type: none"> • Explore the Meterpreter payload
		<ul style="list-style-type: none"> • Create executable payloads
	Performing Post-Exploitation with Metasploit	<ul style="list-style-type: none"> • Use core Meterpreter post-exploitation features
		<ul style="list-style-type: none"> • Use post-exploitation modules
		<ul style="list-style-type: none"> • Perform pivoting with Metasploit
The Metasploit Framework	Automating Metasploit	<ul style="list-style-type: none"> • Create resource scripts
		<ul style="list-style-type: none"> • Use resource scripts in Metasploit

Active Directory Introduction and Enumeration	Active Directory Manual Enumeration	<ul style="list-style-type: none"> Enumerate Active Directory using legacy Windows applications
		<ul style="list-style-type: none"> Use PowerShell and .NET to perform additional AD enumeration
	Manual Enumeration Expanding our Repertoire	<ul style="list-style-type: none"> Enumerate Operating Systems Permissions and logged on users
		<ul style="list-style-type: none"> Enumerate Through Service Principal Names
		<ul style="list-style-type: none"> Enumerate Object Permissions
		<ul style="list-style-type: none"> Explore Domain Shares
	Active Directory Automated Enumeration	<ul style="list-style-type: none"> Collect domain data using SharpHound
<ul style="list-style-type: none"> Analyze domain data using BloodHound 		
Attacking Active Directory Authentication	Understanding Active Directory Authentication	<ul style="list-style-type: none"> Understand NTLM Authentication
		<ul style="list-style-type: none"> Understand Kerberos Authentication
		<ul style="list-style-type: none"> Become familiar with cached AD Credentials
Attacking Active Directory Authentication	Performing Attacks on Active Directory Authentication	<ul style="list-style-type: none"> Use password attacks to obtain valid user credentials
		<ul style="list-style-type: none"> Abuse the enabled user account options

		<ul style="list-style-type: none"> Abuse the Kerberos SPN authentication mechanism
		<ul style="list-style-type: none"> Forge service tickets
		<ul style="list-style-type: none"> Impersonate a domain controller to retrieve any domain user credentials
Lateral Movement in Active Directory	Active Directory Lateral Movement Techniques	<ul style="list-style-type: none"> Understand WMI, WinRS, and WinRM lateral movement techniques
		<ul style="list-style-type: none"> Abuse PsExec for lateral movement
		<ul style="list-style-type: none"> Learn about Pass The Hash and Overpass The Hash as lateral movement techniques
		<ul style="list-style-type: none"> Misuse DCOM to move laterally
	Active Directory Persistence	<ul style="list-style-type: none"> Understand the general purpose of persistence techniques
		<ul style="list-style-type: none"> Leverage golden tickets as a persistence attack
<ul style="list-style-type: none"> Learn about shadow copies and how they can be abused for persistence 		
Assembling the Pieces	Enumerating the Public Network	<ul style="list-style-type: none"> Enumerate machines on a public network
		<ul style="list-style-type: none"> Obtain useful information to utilize for later attacks
	Attacking WEBSRV1	<ul style="list-style-type: none"> Utilize vulnerabilities in WordPress Plugins

		<ul style="list-style-type: none"> Crack the passphrase of a SSH private key
		<ul style="list-style-type: none"> Elevate privileges using sudo commands
		<ul style="list-style-type: none"> Leverage developer artifacts to obtain sensitive information
	Gaining Access to the Internal Network	<ul style="list-style-type: none"> Validate domain credentials from a non-domain-joined machine
		<ul style="list-style-type: none"> Perform phishing to get access to internal network
	Enumerating the Internal Network	<ul style="list-style-type: none"> Gain situational awareness in a network
		<ul style="list-style-type: none"> Enumerate hosts, services, and sessions in a target network
		<ul style="list-style-type: none"> Identify attack vectors in target network
	Attacking the Web Application on INTERNALSRV1	<ul style="list-style-type: none"> Perform Kerberoasting
		<ul style="list-style-type: none"> Abuse a WordPress Plugin function for a Relay attack
	Gaining Access to the Domain Controller	<ul style="list-style-type: none"> Gather information to prepare client-side attacks
		<ul style="list-style-type: none"> Leverage client fingerprinting to obtain information
Trying Harder: The Labs	PWK Challenge Lab Overview	<ul style="list-style-type: none"> Learn about the different kinds of Challenge Labs
		<ul style="list-style-type: none"> Obtain a high level overview of each scenario

		<ul style="list-style-type: none"> • Understand how to treat the mock OSCP Challenge Labs
	Challenge Lab Details	<ul style="list-style-type: none"> • Understand how to think about the concept of dependency
		<ul style="list-style-type: none"> • Understand the lack of meaning inherent to IP address ordering
		<ul style="list-style-type: none"> • Learn about the concept of “decoy” machines
		<ul style="list-style-type: none"> • Learn how Routers and Network Address Translation affect the scenarios
		<ul style="list-style-type: none"> • Understand how to treat the credentials and password attacks
	The OSCP Exam Information	<ul style="list-style-type: none"> • Learn about the OSCP Certification Exam