

PEN-200 (PWK) Syllabus

Learning Module	Learning Units	Learning Objectives
Penetration Testing with Kali Linux : General Course Introduction	Welcome to PWK	Take inventory over what's included in the course
		Set up an Attacking Kali VM
		Connect to and interact over the PWK VPN
		Understand how to complete Module Exercises
	How to Approach the Course	Conceptualize a learning model based on increasing uncertainty
		Understand the different learning components included in PEN-200
	Summary of PWK Learning Modules	Obtain a high level overview of what's covered in each PEN-200 Learning Module
Introduction to Cybersecurity	The Practice of Cybersecurity	Recognize the challenges unique to information security
		Understand how "offensive" and "defensive" security reflect each other
		Begin to build a mental model of useful mindsets applicable to information security
	Threats and Threat Actors	Understand how attackers and defenders learn from each other
		Understand the differences between risks, threats, vulnerabilities, and exploits

Introduction to Cybersecurity	Threats and Threat Actors	List and describe different classes of threat actor
		Recognize some recent cybersecurity attacks
	The CIA Triad	Understand why it's important to protect the confidentiality of information
		Learn why it's important to protect the integrity of information
		Explore why it's important to protect the availability of information
	Security Principles, Controls, and Strategies	Understand the importance of multiple layers of defense in a security strategy
		Describe threat intelligence and its applications in an organization
		Learn why access and user privileges should be restricted as much as possible
		Understand why security should not depend on secrecy
		Identify policies that can mitigate threats to an organization
		Determine which controls an organization can use to mitigate cybersecurity threats
	Cybersecurity Laws, Regulations, Standards, and Frameworks	Gain a broad understanding of various legal and regulatory issues surrounding cybersecurity
		Understand different frameworks and standards that help organizations orient their cybersecurity activities
	Career Opportunities in Cybersecurity	Identify career opportunities in cybersecurity

Effective Learning Strategies	Learning Theory	Understand the general state of our understanding about education and education theory
		Understand the basics of memory mechanisms and dual encoding
		Recognize some of the problems faced by learners, including "The Curve of Forgetting" and cognitive load
	Unique Challenges to Learning Technical Skills	Recognize the differences and advantages of digital learning materials
		Understand the challenge of preparing for unknown scenarios
		Understand the potential challenges of remote or asynchronous learning
	OffSec Methodology	Understand what is meant by a <i>Demonstrative Methodology</i>
		Understand the challenge of preparing for unknown scenarios
		Understand the potential challenges of remote or asynchronous learning
	Case Study: chmod -x chmod	Review a sample of learning material about the executable permission, expand beyond the initial information set, and work through a problem
		Understand how OffSec's approach to teaching is reflected in the sample material
	Tactics and Common Methods	Learn about Retrieval Practice
		Understand Spaced Practice

Effective Learning Strategies	Tactics and Common Methods	• Explore the SQ3R and PQ4R Method
		• Examine the Feynman Technique
		• Understand the Leitner System
	Advice and Suggestions on Exams	• Develop strategies for dealing with exam-related stress
		• Recognize when you might be ready to take the exam
		• Understand a practical approach to exams
	Practical Steps	• Create a long term strategy
		• Understand how to use a time allotment strategy
		• Learn how and when to narrow your focus
		• Understand the importance of a group of co-learners and finding a community
• Explore how best to pay attention and capitalize on our own successful learning strategies		
Report Writing for Penetration Testers	Understanding Note-Taking	• Review the deliverables for penetration testing engagements
		• Understand the importance of note portability

Report Writing for Penetration Testers	Understanding Note-Taking	Identify the general structure of pentesting documentation
		Choose the right note-taking tool
		Understand the importance of taking screenshots
		Use tools to take screenshots
	Writing Effective Technical Penetration Testing Reports	Identify the purpose of a technical report
		Understand how to specifically tailor content
		Construct an Executive Summary
		Account for specific test environment considerations
		Create a technical summary
		Describe technical findings and recommendations
		Recognize when to use appendices, resources, and references
Information Gathering	The Penetration Testing Lifecycle	Understand the stages of a Penetration Test
		Learn the role of Information Gathering inside each stage

Information Gathering	The Penetration Testing Lifecycle	Understand the differences between Active and Passive Information Gathering
	Passive Information Gathering	Understand the two different Passive Information Gathering approaches
		Learn about Open Source Intelligence (OSINT)
		Understand Web Server and DNS passive information gathering
	Active Information Gathering	Learn to perform Netcat and Nmap port scanning
		Conduct DNS, SMB, SMTP, and SNMP Enumeration
		Understand Living off the Land Techniques
Vulnerability Scanning	Vulnerability Scanning Theory	Gain a basic understanding of the Vulnerability Scanning process
		Learn about the different types of Vulnerability Scans
		Understand the considerations of a Vulnerability Scan
	Vulnerability Scanning with Nessus	Install Nessus
		Understand the different Nessus Components
		Configure and perform a vulnerability scan

Vulnerability Scanning	Vulnerability Scanning with Nessus	Understand and work with the results of a vulnerability scan with Nessus
		Provide credentials to perform an authenticated vulnerability scan
		Gain a basic understanding of Nessus Plugins
	Vulnerability Scanning with Nmap	Understand the basics of the Nmap Scripting Engine (NSE)
		Perform a lightweight Vulnerability Scan with Nmap
		Work with custom NSE scripts
Introduction to Web Applications	Web Application Assessment Methodology	Understand web application security testing requirements
		Learn different types of methodologies of web application testing
		Learn about the OWASP Top10 and most common web vulnerabilities
	Web Application Assessment Tools	Perform common enumeration techniques on web applications
		Understand Web Proxies theory
		Learn how Burp Suite proxy works for web application testing
	Web Application Enumeration	Learn how to debug Web Application source code

Introduction to Web Applications	Web Application Enumeration	Understand how to enumerate and inspect Headers, Cookies, and Source Code
		Learn how to conduct API testing methodologies
	Cross-Site Scripting (XSS)	Understand Cross-Site Scripting vulnerability types
		Exploit basic Cross-Site Scripting
		Perform Privilege Escalation via Cross-Site Scripting
Common Web Application Attacks	Directory Traversal	Understand absolute and relative paths
		Learn how to exploit directory traversal vulnerabilities
		Use encoding for special characters
	File Inclusion Vulnerabilities	Learn the difference between File Inclusion and Directory Traversal vulnerabilities
		Gain an understanding of File Inclusion vulnerabilities
		Understand how to leverage Local File Inclusion (LFI) to obtain code execution
		Explore PHP Wrapper usage
		Learn how to perform Remote File Inclusion (RFI) attacks

Common Web Application Attacks	File Upload Vulnerabilities	Understand File Upload Vulnerabilities
		Learn how to identify File Upload vulnerabilities
	File Upload Vulnerabilities	Explore different vectors to exploit File Upload vulnerabilities
	Command Injection	Learn about command injection in web applications
		Use operating system commands for OS command injection
		Understand how to leverage command injection to gain system access
SQL Injection Attacks	SQL Theory and Database Types	Refresh SQL theory fundamentals
		Learn different DB types
		Understand different SQL syntax
	Manual SQL Exploitation	Manually identify SQL injection vulnerabilities
		Understand UNION SQLi payloads
		Learn about Error SQLi payloads
		Understand Blind SQLi payloads

SQL Injection Attacks	Manual and Automated Code Execution	Exploit MSSQL Databases with xp_cmdshell
		Automate SQL Injection with SQLmap
Client-Side Attacks	Target Reconnaissance	Gather information to prepare client-side attacks
		Leverage client fingerprinting to obtain information
	Exploiting Microsoft Office	Understand variations of Microsoft Office client-side attacks
		Install Microsoft Office
		Leverage Microsoft Word Macros
	Abusing Windows Library Files	Prepare an attack with Windows library files
		Leverage Windows shortcuts to obtain code execution
Locating Public Exploits	Getting Started	Understand the risk of executing untrusted exploits
		Understand the importance of analyzing the exploit code before execution
	Online Exploit Resources	Access multiple online exploit resources
		Differentiate between various online exploit resources

		• Understand the risks between online exploit resources
		• Use Google search operators to discover public exploits
Locating Public Exploits	Offline Exploit Resources	• Access Multiple Exploit Frameworks
		• Use SearchSploit
		• Use Nmap NSE Scripts
	Exploiting a Target	• Follow a basic penetration test workflow to enumerate a target system
		• Completely exploit a machine that is vulnerable to public exploits
		• Discover appropriate exploits for a target system
• Execute a public exploit to gain a limited shell on a target host		
Fixing Exploits	Fixing Memory Corruption Exploits	• Understand high-level buffer overflow theory
		• Cross-compile binaries
		• Modify and update memory corruption exploits
	Fixing Web Exploits	• Fix Web application exploits

		• Troubleshoot common web application exploit issues
Antivirus Evasion	Antivirus Evasion Software Key Components and Operations	• Recognize known vs unknown threats
		• Understand AV key components
		• Understand AV detection engines
	AV Evasion in Practice	• Understand antivirus evasion testing best practices
		• Manually evade AV solutions
		• Leverage automated tools for AV evasion
Password Attacks	Attacking Network Services Logins	• Attack SSH and RDP Logins
		• Attack HTTP POST login forms
	Password Cracking Fundamentals	• Understand the fundamentals of password cracking
		• Mutate Wordlists
		• Explain the basic password cracking methodology

Password Attacks		Attack password manager key files
		Attack the passphrase of SSH private keys
	Working with Password Hashes	Obtain and crack NTLM hashes
		Pass NTLM hashes
		Obtain and crack Net-NTLMv2 hashes
		Relay Net-NTLMv2 hashes

Windows Privilege Escalation	Enumerating Windows	Understand Windows privileges and access control mechanisms
		Obtain situational awareness
		Search for sensitive information on Windows systems
		Find sensitive information generated by PowerShell
		Become familiar with automated enumeration tools
	Leveraging Windows Services	Hijack service binaries
		Hijack service DLLs

		• Abuse Unquoted service paths
Windows Privilege Escalation	Abusing other Windows Components	• Leverage Scheduled Tasks to elevate our privileges
		• Understand the different types of exploits leading to privilege escalation
		• Abuse privileges to execute code as privileged user accounts
Linux Privilege Escalation	Enumerating Linux	• Understand files and user privileges on Linux
		• Perform manual enumeration
		• Conduct automated enumeration
	Exposed Confidential Information	• Understand user history files
		• Inspect user trails for credential harvesting
		• Inspect system trails for credential harvesting
	Insecure File Permissions	• Abuse insecure cron jobs to escalate privileges
		• Abuse Insecure file permissions to escalate privileges
	Insecure System Components	• Abuse SUID programs and capabilities for privilege escalation
		• Circumvent special sudo permissions to

		escalate privileges
Linux Privilege Escalation	Insecure System Components	Enumerate the system's kernel for known vulnerabilities, then abuse them for privilege escalation
Port Redirection and SSH Tunneling	Port Forwarding with *NIX Tools	Learn about port forwarding
		Understand why and when to use port forwarding
		Use Socat for port forwarding
	SSH Tunneling	Learn about SSH tunneling
		Understand how to perform SSH local port forwarding
		Understand how to perform SSH dynamic port forwarding
		Understand how to perform SSH remote port forwarding
		Understand how to perform SSH remote dynamic port forwarding
	Port Forwarding with Windows Tools	Understand port forwarding and tunneling with ssh.exe on Windows
		Understand port forwarding and tunneling with Plink
		Understand port forwarding with Netsh
Advanced Tunneling	Tunneling Through Deep Packet Inspection	Learn about HTTP tunneling

		• Perform HTTP tunneling with Chisel
		• Learn about DNS tunneling
		• Perform DNS tunneling with dnscat
The Metasploit Framework	Getting Familiar with Metasploit	• Setup and navigate Metasploit
		• Use auxiliary modules
		• Leverage exploit modules
	Using Metasploit Payloads	• Understand the differences between staged and non-staged payloads
		• Explore the Meterpreter payload
		• Create executable payloads
	Performing Post-Exploitation with Metasploit	• Use core Meterpreter post-exploitation features
		• Use post-exploitation modules
		• Perform pivoting with Metasploit
The Metasploit Framework	Automating Metasploit	• Create resource scripts
		• Use resource scripts in Metasploit

Active Directory Introduction and Enumeration	Active Directory Manual Enumeration	Enumerate Active Directory using legacy Windows applications
		Use PowerShell and .NET to perform additional AD enumeration
	Manual Enumeration Expanding our Repertoire	Enumerate Operating Systems Permissions and logged on users
		Enumerate Through Service Principal Names
		Enumerate Object Permissions
		Explore Domain Shares
	Active Directory Automated Enumeration	Collect domain data using SharpHound
		Analyze domain data using BloodHound
Attacking Active Directory Authentication	Understanding Active Directory Authentication	Understand NTLM Authentication
		Understand Kerberos Authentication
		Become familiar with cached AD Credentials
Attacking Active Directory Authentication	Performing Attacks on Active Directory Authentication	Use password attacks to obtain valid user credentials
		Abuse the enabled use account options

		• Abuse the Kerberos SPN authentication mechanism
		• Forge service tickets
		• Impersonate a domain controller to retrieve any domain user credentials
Lateral Movement in Active Directory	Active Directory Lateral Movement Techniques	• Understand WMI, WinRS, and WinRM lateral movement techniques
		• Abuse PsExec for lateral movement
		• Learn about Pass The Hash and Overpass The Hash as lateral movement techniques
		• Misuse DCOM to move laterally
	Active Directory Persistence	• Understand the general purpose of persistence techniques
		• Leverage golden tickets as a persistence attack
		• Learn about shadow copies and how they can be abused for persistence
Assembling the Pieces	Enumerating the Public Network	• Enumerate machines on a public network
		• Obtain useful information to utilize for later attacks
	Attacking WEBSRV1	• Utilize vulnerabilities in WordPress Plugins

		Crack the passphrase of a SSH private key
		Elevate privileges using sudo commands
		Leverage developer artifacts to obtain sensitive information
	Gaining Access to the Internal Network	Validate domain credentials from a non-domain-joined machine
		Perform phishing to get access to internal network
	Enumerating the Internal Network	Gain situational awareness in a network
		Enumerate hosts, services, and sessions in a target network
		Identify attack vectors in target network
	Attacking the Web Application on INTERNALSRV1	Perform Kerberoasting
		Abuse a WordPress Plugin function for a Relay attack
Trying Harder: The Labs	Gaining Access to the Domain Controller	Gather information to prepare client-side attacks
		Leverage client fingerprinting to obtain information
	PWK Challenge Lab Overview	Learn about the different kinds of Challenge Labs
		Obtain a high level overview of each scenario

		Understand how to treat the mock OSCP Challenge Labs
	Challenge Lab Details	Understand how to think about the concept of dependency
		Understand the lack of meaning inherent to IP address ordering
		Learn about the concept of “decoy” machines
		Learn how Routers and Network Address Translation affect the scenarios
		Understand how to treat the credentials and password attacks
	The OSCP Exam Information	Learn about the OSCP Certification Exam