N-200 (PWK) Syllabus

Days	Learning Module	Learning Units
1	**Penetration Testing with Kali Linux : General Course Introduction**	Welcome to PWK
		How to Approach the Course
		Summary of PWK Learning Modules
2	**Introduction to Cybersecurity**	The Practice of Cybersecurity
		Threats and Threat Actors
		Threats and Threat Actors
		The CIA Triad
		Security Principles, Controls, and Strategies

		Cybersecurity Laws, Regulations, Standards, and Frameworks
		Career Opportunities in Cybersecurity
3	**Effective Learning Strategies**	Learning Theory
		Unique Challenges to Learning Technical Skills
		OffSec Methodology
		Case Study: chmod -x chmod
		Tactics and Common Methods
		Tactics and Common Methods
		Advice and Suggestions on Exams

		Practical Steps
4	**Report Writing for Penetration Testers**	Understanding Note-Taking
		Understanding Note-Taking
		Writing Effective Technical Penetration Testing Reports
5	**Information Gathering**	The Penetration Testing Lifecycle
		The Penetration Testing Lifecycle
		Passive Information Gathering
		Active Information Gathering
6	**Vulnerability Scanning**	Vulnerability Scanning Theory

		Vulnerability Scanning with Nessus
		Vulnerability Scanning with Nessus
		Vulnerability Scanning with Nmap
7	**Introduction to Web Applications**	Web Application Assessment Methodology
		Web Application Assessment Tools
		Web Application Enumeration
		Web Application Enumeration
		Cross-Site Scripting (XSS)
8	**Common Web Application Attacks**	Directory Traversal
		File Inclusion Vulnerabilities

		File Upload Vulnerabilities
		File Upload Vulnerabilities
		Command Injection
9	**SQL Injection Attacks**	SQL Theory and Database Types
		Manual SQL Exploitation
		Manual and Automated Code Execution
10	**Client-Side Attacks**	Target Reconnaissance
		Exploiting Microsoft Office
		Abusing Windows Library Files
11	**Locating Public Exploits**	Getting Started
		Online Exploit Resources
		Offline Exploit Resources

		Exploiting a Target
12	**Fixing Exploits**	Fixing Memory Corruption Exploits
		Fixing Web Exploits
13	**Antivirus Evasion**	Antivirus Evasion Software Key Components and Operations
		AV Evasion in Practice
14	**Password Attacks**	Attacking Network Services Logins
		Password Cracking Fundamentals
		Working with Password Hashes
15	**Windows Privilege Escalation**	Enumerating Windows

		Leveraging Windows Services
		Abusing other Windows Components
16	**Linux Privilege Escalation**	Enumerating Linux
		Exposed Confidential Information
		Insecure File Permissions
		Insecure System Components
		Insecure System Components
17	**Port Redirection and SSH Tunneling**	Port Forwarding with *NIX Tools
		SSH Tunneling
		Port Forwarding with Windows Tools
18	**Advanced Tunneling**	Tunneling Through Deep Packet Inspection

19	**The Metasploit Framework**	Getting Familiar with Metasploit
		Using Metasploit Payloads
		Performing Post-Exploitation with Metasploit
		Automating Metasploit
20	**Active Directory Introduction and Enumeration**	Active Directory Manual Enumeration
		Manual Enumeration Expanding our Repertoire
		Active Directory Automated Enumeration
21	**Attacking Active Directory Authentication**	Understanding Active Directory Authentication
		Performing Attacks on Active Directory Authentication

22	**Lateral Movement in Active Directory**	Active Directory LAteral Movement Techniques
		Active Directory Persistence
23	**Assembling the Pieces**	Enumerating the Public Network
		Attacking webserver
		Gaining Access to the Internal Network
		Enumerating the Internal Network
		Attacking the Web Application on internal server
		Gaining Access to the Domain Controller

Learning Objectives	Hours
● Take inventory over what’s included in the course	2
● Set up an Attacking Kali VM	
● Connect to and interact over the PWK VPN	
● Understand how to complete Module Exercises	
● Conceptualize a learning model based on increasing uncertainty	
● Understand the different learning components included in PEN-200	
● Obtain a high level overview of what’s covered in each PEN-200 Learning Module	
● Recognize the challenges unique to information security	2
● Understand how "offensive" and "defensive" security reflect each other	
● Begin to build a mental model of useful mindsets applicable to information security	
● Understand how attackers and defenders learn from each other	
● Understand the differences between risks, threats, vulnerabilities, and exploits	
● List and describe different classes of threat actor	
● Recognize some recent cybersecurity attacks	
● 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	
● 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	
● Gain a broad understanding of various legal and regulatory issues surrounding cybersecurity	
● Understand different frameworks and standards that help organizations orient their cybersecurity activities	
● Identify career opportunities in cybersecurity	
● Understand the general state of our understanding about education and education theory	2
● 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	
● 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	
● Understand what is meant by a *Demonstrative Methodology*	
● Understand the challenge of preparing for unknown scenarios	
● Understand the potential challenges of remote or asynchronous learning	
● 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	
● Learn about Retrieval Practice	
● Understand Spaced Practice	
● Explore the SQ3R and PQ4R Method	
● Examine the Feynman Technique	
● Understand the Leitner System	
● Develop strategies for dealing with exam-related stress	
● Recognize when you might be ready to take the exam	
● Understand a practical approach to exams	

● 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	
● Review the deliverables for penetration testing engagements	2
● Understand the importance of note portability	
● Identify the general structure of pentesting documentation	
● Choose the right note-taking tool	
● Understand the importance of taking screenshots	
● Use tools to take screenshots	
● 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	
● Understand the stages of a Penetration Test	2
● Learn the role of Information Gathering inside each stage	
● Understand the differences between Active and 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	
● Learn to perform Netcat and Nmap port scanning	
● Conduct DNS, SMB, SMTP, and SNMP Enumeration	
● Understand Living off the Land Techniques	
● Gain a basic understanding of the Vulnerability Scanning process	2

● Learn about the different types of Vulnerability Scans	
● Understand the considerations of a Vulnerability Scan	
● Install Nessus	
● Understand the different Nessus Components	
● Configure and perform a vulnerability scan	
● 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	
● Understand the basics of the Nmap Scripting Engine (NSE)	
● Perform a lightweight Vulnerability Scan with Nmap	
● Work with custom NSE scripts	
● Understand web application security testing requirements	2
● Learn different types of methodologies of web application testing	
● Learn about the OWASP Top10 and most common web vulnerabilities	
● Perform common enumeration techniques on web applications	
● Understand Web Proxies theory	
● Learn how Burp Suite proxy works for web application testing	
● Learn how to debug Web Application source code	
● Understand how to enumerate and inspect Headers, Cookies, and Source Code	
● Learn how to conduct API testing methodologies	
● Understand Cross-Site Scripting vulnerability types	
● Exploit basic Cross-Site Scripting	
● Perform Privilege Escalation via Cross-Site Scripting	
● Understand absolute and relative paths	2
● Learn how to exploit directory traversal vulnerabilities	
● Use encoding for special characters	
● 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	
● Understand File Upload Vulnerabilities	
● Learn how to identify File Upload vulnerabilities	
● Explore different vectors to exploit File Upload vulnerabilities	
● 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	
● Refresh SQL theory fundamentals	2
● Learn different DB types	
● Understand different SQL syntax	
● Manually identify SQL injection vulnerabilities	
● Understand UNION SQLi payloads	
● Learn about Error SQLi payloads	
● Understand Blind SQLi payloads	
● Exploit MSSQL Databases with xp_cmdshell	
● Automate SQL Injection with SQLmap	
● Gather information to prepare client-side attacks	2
● Leverage client fingerprinting to obtain information	
● Understand variations of Microsoft Office client-side attacks	
● Install Microsoft Office	
● Leverage Microsoft Word Macros	
● Prepare an attack with Windows library files	
● Leverage Windows shortcuts to obtain code execution	
● Understand the risk of executing untrusted exploits	2
● Understand the importance of analyzing the exploit code before execution	
● 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	
● Access Multiple Exploit Frameworks	
● Use SearchSploit	

● Use Nmap NSE Scripts	
● 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	
● Understand high-level buffer overflow theory	2
● Cross-compile binaries	
● Modify and update memory corruption exploits	
● Fix Web application exploits	
● Troubleshoot common web application exploit issues	
● Recognize known vs unknown threats	2
● Understand AV key components	
● Understand AV detection engines	
● Understand antivirus evasion testing best practices	
● Manually evade AV solutions	
● Leverage automated tools for AV evasion	
● Attack SSH and RDP Logins	2
● Attack HTTP POST login forms	
● Understand the fundamentals of password cracking	
● Mutate Wordlists	
● Explain the basic password cracking methodology	
● Attack password manager key files	
● Attack the passphrase of SSH private keys	
● Obtain and crack NTLM hashes	
● Pass NTLM hashes	
● Obtain and crack Net-NTLMv2 hashes	
● Relay Net-NTLMv2 hashes	
● Understand Windows privileges and access control mechanisms	2
● Obtain situational awareness	
● Search for sensitive information on Windows systems	
● Find sensitive information generated by PowerShell	
● Become familiar with automated enumeration tools	

● Hijack service binaries	
● Hijack service DLLs	
● Abuse Unquoted service paths	
● 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	
● Understand files and user privileges on Linux	2
● Perform manual enumeration	
● Conduct automated enumeration	
● Understand user history files	
● Inspect user trails for credential harvesting	
● Inspect system trails for credential harvesting	
● Abuse insecure cron jobs to escalate privileges	
● Abuse Insecure file permissions to escalate privileges	
● Abuse SUID programs and capabilities for privilege escalation	
● Circumvent special sudo permissions to	
escalate privileges	
● Enumerate the system's kernel for known vulnerabilities, then abuse them for privilege escalation	
● Learn about port forwarding	2
● Understand why and when to use port forwarding	
● Use Socat for port forwarding	
● 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	
● Understand port forwarding and tunneling with ssh.exe on Windows	
● Understand port forwarding and tunneling with Plink	
● Understand port forwarding with Netsh	
● Learn about HTTP tunneling	2
● Perform HTTP tunneling with Chisel	

● Learn about DNS tunneling	
● Perform DNS tunneling with dnscat	
● Setup and navigate Metasploit	2
● Use auxiliary modules	
● Leverage exploit modules	
● Understand the differences between staged and non-staged payloads	
● Explore the Meterpreter payload	
● Create executable payloads	
● Use core Meterpreter post-exploitation features	
● Use post-exploitation modules	
● Perform pivoting with Metasploit	
● Create resource scripts	
● Use resource scripts in Metasploit	
● Enumerate Active Directory using legacy Windows applications	2
● Use PowerShell and .NET to perform additional AD enumeration	
● Enumerate Operating Systems Permissions and logged on users	
● Enumerate Through Service Principal Names	
● Enumerate Object Permissions	
● Explore Domain Shares	
● Collect domain data using SharpHound	
● Analyze domain data using BloodHound	
● Understand NTLM Authentication	2
● Understand Kerberos Authentication	
● Become familiar with cached AD Credentials	
● 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	

● Understand WMI, WinRS, and WinRM lateral movement techniques	2
● Abuse PsExec for lateral movement	
● Learn about Pass The Hash and Overpass The Hash as lateral movement techniques	
● Misuse DCOM to move laterally	
● 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	
● Enumerate machines on a public network	2
● Obtain useful information to utilize for later attacks	
● 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	
● Validate domain credentials from a non-domain-joined machine	
● Perform phishing to get access to internal network	
● Gain situational awareness in a network	
● Enumerate hosts, services, and sessions in a target network	
● Identify attack vectors in target network	
● Perform Kerberoasting	
● Abuse a WordPress Plugin function for a Relay attack	
● Gather information to prepare client-side attacks	
● Leverage client fingerprinting to obtain information	