Concepts of Ethical Hacking

ABOUT COURSE

This course is a foundational training to Modulus line of penetration testing courses becauses it teaches you to think like a hacker.
You will learn the value of vulnerability assessments, how malwares and viruses work, how an attacker attacks and most importantly how to implement counter response and preventative measures when it comes to a network or an application hack. Therefore, you can teach yourself to setup dynamic defenses to prevent a hack or an intrusion.

LEARNING OUTCOMES

01. Lay the foundation to attack like an adversary

02. Learn Linux & Windows Basics

03. Learn to avoid phishing, virus, malwares and ransomwares

04. The ability to secure and protect any network from hackers and loss of data

Intro to Ethical Hacking

18. Introduction & Lab Setup

1. IP Addresses
2. MAC Addresses
3. TCP, UDP, and the Three-Way Handshake
4. Common Ports and Protocols
5. The OSI Model
6. Subnetting: Part 1 - Methodology
7. Subnetting: Part 2 - Hands-On Challenge
8. Installing VMWare / Virtualbox
9. Installing Kali Linux

19. Introduction to Linux

1. Exploring Kali Linux
2. Navigating the File System
3. Users and Privileges
4. Common Network Commands
5. Viewing, Creating, and Editing Files
6. Starting and Stopping Kali Services
7. Installing and Updating Tools
8. Scripting with Bash

20. Python 101

1. Introduction
2. Strings
3. Math
4. Variables & Methods
5. Functions
6. Boolean Expressions
7. Relational and Boolean Operators
8. Conditional Statements
9. Lists
10. Tuples
11. Looping
12. Importing Modules
13. Advanced Strings
14. Dictionaries
15. Sockets

21. Information Gathering

1. Passive Reconnaissance Overview
2. Identifying Our Target
3. Mail Address Gathering with Hunter.io
4. Gathering Breached Credentials with Breach-Parse
5. Utilizing theharvester
6. Hunting Subdomains
7. Identifying Website Technologies
8. Information Gathering with Burp Suite
9. Google Fu
10. Utilizing Social Media

22. Scanning and Information Additional Scanning tools

1. Installing Kioptrix
2. Scanning with NMAP
3. Enumerating HTTP/HTTPS
4. Enumerating SMB
5. Enumerating SSH
6. Researching Potential Vulnerabilities
7. Scanning with Masscan
8. Scanning with Metasploit
9. Scanning with Nessus

23. Exploitation Basics

1. Reverse Shells vs Bind Shells
2. Staged vs Non-Staged Payloads
3. Gaining Root with Metasploit
4. Manual Exploitation
5. Brute Force Attacks
6. Password Spraying and Credential Stuffing

24. Mid-Course Capstone

1. Introduction
2. Walkthrough - Lame
3. Walkthrough - Blue
4. Walkthrough - Devel
5. Walkthrough - Jerry
6. Walkthrough - Nibbles
7. Walkthrough - Optimum
8. Walkthrough - Bashed
9. Walkthrough - Grandpa
10. Walkthrough - Netmon

25. Introduction to Exploit Developemt

1. Required Installations
2. Buffer Overflows Explained
3. Spiking
4. Fuzzing
5. Finding the Offset
6. Overwriting the EIP
7. Finding Bad Characters
8. Finding the Right Module
9. Generating Shellcode and Getting Root

26. Active Directory Lab

1. Active Directory Overview
2. Physical Active Directory Components
3. Logical Active Directory Components
4. Lab Overview and Requirements
5. Downloading Necessary ISOs
6. Setting Up the Domain Controller
7. Setting Up the User Machines
8. Setting Up Users, Groups, and Policies
9. Joining Our Machines to the Domain

27. Attacking Active Directory - Intital Attack vectors

1. Introduction
2. LLMNR Poisoning Overview
3. Capturing NTLMv2 Hashes with Responder
4. Password Cracking with Hashcat
5. LLMNR Poisoning Defenses
6. MB Relay Attacks Overview
7. Quick Lab Update
8. Discovering Hosts with SMB Signing Disabled
9. SMB Relay Attack Demonstration
10. SMB Relay Attack Defenses
11. Gaining Shell Access
12. IPv6 Attacks Overview
13. Installing mitm6
14. Setting Up LDAPS
15. IPv6 Attack Defenses
16. Other Attack Vectors and Strategies

28. Attacking Active Directory - Post Compromise Enumeration

1. Introduction
2. PowerView Overview
3. Domain Enumeration with PowerView
4. Bloodhound Overview and Setup
5. Grabbing Data with Invoke-Bloodhound
5. Enumerating Domain Data with Bloodhound

29. Attacking Active Directory - Post Compromise Attacks

1. Introduction
2. Pass the Hash / Password Overview
3. Installing crackmapexec
4. Pass the Password Attacks
5. Dumping Hashes with secretsdump.py
6. Cracking NTLM Hashes with Hashcat
7. Pass Attack Mitigations
8. Token Impersonation Overview
9. Token Impersonation with Incognito
10. Token Impersonation Mitigation
11. Kerberoasting Overview
12. Kerberoasting Walkthrough
13. Kerberoasting Mitigation
14. GPP / cPassword Attacks Overview
15. Abusing GPP
16. Mimikatz Overview
17. Credential Dumping with Mimikatz
18. Golden Ticket Attacks
19. Conclusion and Additional Resources

30. Post Exploitation

1. Introduction
2. File Transfers Review
3. Maintaining Access Overview
4. Pivoting Lab Setup
5. Pivoting Walkthrough
6. Cleaning Up

31. Post Exploitation

1. Installing Go
2. Finding Subdomains with Assetfinder
3. Finding Subdomains with Amass and Alive Domains with Httprobe
4. Screenshotting Websites with GoWitness
5. Automating the Enumeration Process

32. Testing Top 10 Web Application Vulnerabiltites

1. Introduction
2. The OWASP Top 10 and OWASP Testing Checklist
3. Installing OWASP Juice Shop
4. Installing Foxy Proxy
5. Exploring Burp Suite
6. Introducing the Score Board
7. SQL Injection Attacks Overview
8. SQL Injection Walkthrough
9. SQL Injection Defenses
10. Broken Authentication Overview and Defenses
11. Testing for Broken Authentication
12. Sensitive Data Exposure Overview and Defenses
13. Testing for Sensitive Data Exposure
14. XML External Entities (XXE) Overview
15. XXE Attack and Defense
16. Broken Access Control Overview
17. Broken Access Control Walkthrough
18. Security Misconfiguration Attacks and Defenses
19. Cross-Site Scripting (XSS) Overview
20. Reflected XSS Walkthrough
21. Stored XSS Walkthrough
22. Preventing XSS
23. Insecure Deserialization
24. Using Components with Known Vulnerabilities
25. Insufficient Logging and Monitoring

33. Post Exploitation

1. Wireless Penetration Testing Overview
- WPA PSK Exploit Walkthrough

34. Legal Documents and Report Writing

1. Common Legal Documents
2. Pentest Report Writing
3. Reviewing a Real Pentest Report