Ethical Hacking and Penetration Testing

Institute of Continuing Education

COURSE OUTLINE

Course Overview

The digital landscape is evolving at an unprecedented rate and cyber threats lurk around every corner. Cybersecurity resilience in the modern world cannot be just an add on - it's a necessity. Offensive security professionals like ethical hackers and penetration testers can help proactively discover unknown threats and address them before the cybercriminals do.

This course is designed to prepare you with an Ethical Hacker skillset and give you a solid understanding of offensive security. You will become proficient in the art of scoping, executing, and reporting on vulnerability assessments, while recommending mitigation strategies. Follow an engaging gamified narrative throughout the course and get lots of practice with hands-on labs inspired by real-world scenarios.

After completing this course, continue your cybersecurity career in offensive security as an ethical hacker or penetration tester. Or use this course to strengthen your defensive security knowledge. By understanding the mindset of threat actors, you will be able to more effectively implement security controls and monitor, analyze, and respond to current security threats.

Career Pathways

Career pathways in ethical hacking and penetration testing include starting as penetration testers, progressing to cybersecurity consultants or vulnerability analysts, and potentially reaching roles such as Chief Information Security Officers (CISOs) in major corporations.

Target Audience

The target audience for an ethical hacking and penetration testing course includes IT professionals, computer science students, cybersecurity enthusiasts, organizations aiming to strengthen their digital defenses, and individuals transitioning into the cybersecurity domain.

Prerequisites

Junior Cybersecurity Analyst Career Path, or equivalent entry-level cybersecurity knowledge, Basic programming knowledge.

Course Objectives

- **Understand Cybersecurity Fundamentals:** Grasp the foundational concepts, terminologies, and challenges in the cybersecurity realm.
- **Ethical Hacking Principles:** Learn the ethics and legal considerations of hacking, ensuring activities are always within the bounds of legality and morality.
- **Penetration Testing Techniques:** Acquire hands-on skills to conduct systematic penetration tests on computer systems, networks, and applications.
- **Vulnerability Assessment:** Identify, analyze, and prioritize vulnerabilities in a system to ensure robust security measures.
- **Tools and Technologies:** Familiarize with the latest tools, software, and methodologies used by ethical hackers and penetration testers.

- **Security Threats and Countermeasures:** Understand various types of cyber threats and the appropriate defensive strategies against them.
- **Reporting and Communication:** Learn to effectively communicate findings, risks, and recommendations to both technical and non-technical stakeholders.
- **Incident Response:** Acquire skills to respond swiftly and efficiently to security breaches or incidents to minimize damage.
- **Hands-on Labs:** Engage in practical simulations and exercises to apply theoretical knowledge in real-world scenarios.
- **Stay Updated:** Emphasize the importance of continuous learning to keep abreast with the rapidly evolving cybersecurity landscape.

Course Curriculum

Module 1: Introduction to Ethical Hacking and Penetration Testing	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?
Understanding Ethical Hacking and Penetration Testingt	Overview
	Why Do We Need to Do Penetration Testing?
	Lab - Researching PenTesting Careers
	Threat Actors
Exploring Penetration Testing Methodologies	Overview
	Why Do We Need to Follow a Methodology for Penetration Testing?
	Environmental Considerations
	Practice - Types of Penetration Tests
	Surveying Different Standards and Methodologies
	Lab - Compare Pentesting Methodologies
Building Your Own Lab	Overview
	Requirements and Guidelines for Penetration Testing Labs
	What Tools Should You Use in Your Lab?

	Practice - Requirements and Guidelines for Penetration Testing Labs
	What If You Break Something?
	Lab - Deploy a Pre-Built Kali Linux Virtual Machine (VM)
	Lab - Investigate Kali Linux
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Introduction to Ethical Hacking and Penetration Testing

Module 2: Planning and Scoping a Penetration Testing Assessment	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?
Comparing and Contrasting Governance, Risk, and Compliance Concepts	Overview
	Regulatory Compliance Considerations
	Local Restrictions
	Practice - Regulations
	Legal Concepts
	Contracts
	Disclaimers
	Practice - Legal Concepts
	Lab - Compliance Requirements and Local Restrictions
Explaining the Importance of Scoping and Organizational or Customer Requirements	Overview
	Rules of Engagement
	Practice - Rules of Engagement
	Target List and In-Scope Assets

	Practice - Target List and In-Scope Assets
	Validating the Scope of Engagement
	Strategy: Unknown vs. Known Environment Testing
	Practice - Strategy: Unknown vs. Known Environment Testing
	Lab - Pre-Engagement Scope and Planning
	Lab - Create a Pentesting Agreement
Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and Integrity	Overview
	Practice - Demonstrate an Ethical Hacking Mindset
	Lab - Personal Code of Conduct
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Planning and Scoping a Penetration Testing Assessment
Module 3: Information Gathering and Vulnerability Scanning	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?
Performing Passive Reconnaissance	Overview
	Active Reconnaissance vs. Passive Reconnaissance
	Practice - Active Reconnaissance vs. Passive Reconnaissance
	Lab - Using OSINT Tools
	DNS Lookups
	Practice - DNS Lookups
	Identification of Technical and Administrative Contacts

	Practice - Identification of Technical and Administrative Contracts
	Lab - DNS Lookups
	Cloud vs. Self-Hosted Applications and Related Subdomains
	Social Media Scraping
	Lab - Employee Intelligence Gathering
	Cryptographic Flaws
	Lab - Finding Information from SSL Certificates
	Company Reputation and Security Posture
	Practice - File Metadata
	Practice - Web Archiving, Caching, and Public Code Repositories
	Lab - Finding Out About the Organization
	Lab - Advanced Searches
	Open-Source Intelligence (OSINT) Gathering
	Lab - Shodan Searches
Performing Active Reconnaissance	Overview
	Nmap Scan Types
	Practice - Nmap Scan Types
	Types of Enumeration
	Practice - Exploring Enumeration via Packet Crafting with Scapy
	Lab - Enumeration with Nmap
	Packet Inspection and Eavesdropping
	Practice - Packet Inspection and Eavesdropping
	Lab - Packet Crafting with Scapy

	Lab - Network Sniffing with Wireshark
Performing Active Reconnaissance	Overview
	How a Typical Automated Vulnerability Scanner Works
	Practice - How a Typical Automated Vulnerability Scanner Works
	Types of Vulnerability Scans
	Practice - Types of Vulnerability Scans
	Lab - Vulnerability Scanning with Kali Tools
	Challenges to Consider When Running a Vulnerability Scan
Understanding How to Analyze Vulnerability Scan Results	Overview
	Sources for Further Investigation of Vulnerabilities
	Lab - Investigate Vulnerability Information Sources
	How to Deal with a Vulnerability
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Information Gathering and Vulnerability Scanning
Module 4: Social Engineering Attacks	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?
Pretexting for an Approach and Impersonation	Overview
	Practice - Pretexting and Impersonation
Social Engineering Attacks	Overview
	Email Phishing
	Vishing
	Short Message Service (SMS) Phishing

	Universal Serial Bus (USB) Drop Key
	Watering Hole Attacks
	Practice - Pivot Attack
	Practice - Social Engineering Attacks
Physical Attacks	Overview
	Tailgating
	Dumpster Diving
	Shoulder Surfing
	Badge Cloning
	Practice - Physical Attacks
Social Engineering Tools	Overview
	Social-Engineer Toolkit (SET)
	Browser Exploitation Framework (BeEF)
	Practice - Browser Exploitation Framework
	Call Spoofing Tools
	Practice - Call Spoofing Tools
	Lab - Explore the Social Engineer Toolkit (SET)
	Lab - Using the Browser Exploitation Framework (BeEF)
Module 5: Exploiting Wired and Wireless Networks	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?
Exploiting Network-Based Vulnerabilities	Overview
	Windows Name Resolution and SMB Attacks
	Practice - Windows Name Resolution and SMB Attacks

	Lab - Scanning for SMB Vulnerabilities with enum4linux
	DNS Cache Poisoning
	Practice - DNS Cache Poisoning
	SNMP Exploits
	SMTP Exploits
	Practice - SMTP Commands
	FTP Exploits
	Pass-the-Hash Attacks
	Kerberos and LDAP-Based Attacks
	Kerberoasting
	On-Path Attacks
	Practice - Kerberos, LDAP, and On-Path Attacks
	Lab - On-Path Attacks with Ettercap
	Route Manipulation Attacks
	DoS and DDoS Attacks
	Practice - DoS and DDoS Attacks
	Network Access Control (NAC) Bypass
	VLAN Hopping
	Practice - NAC Bypass and VLAN Hopping
	DHCP Starvation Attacks and Rogue DHCP Servers
	Practice - DHCP Starvation and Rogue DHCP Servers
Exploiting Wireless Vulnerabilities	Overview
	Rogue Access Points
	Evil Twin Attacks

	Disassociation (or Deauthentication) Attacks
	Preferred Network List Attacks
	Wireless Signal Jamming and Interference
	War Driving
	Initialization Vector (IV) Attacks and Unsecured Wireless Protocols
	KARMA Attacks
	Fragmentation Attacks
	Practice - IV, Unsecured Wireless, KARMA, and Fragmentation Attacks
	Credential Harvesting
	Bluejacking and Bluesnarfing
	Bluetooth Low Energy (BLE) Attacks
	Radio-Frequency Identification (RFID) Attacks
	Password Spraying
	Exploit Chaining
	Practice - Wireless Attacks
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Exploiting Wired and Wireless Networks

Module 6: Exploiting Application-Based Vulnerabilities

Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?

Overview of Web Application-Based Attacks for Security Professionals and the OWASP Top 10	Overview
	The HTTP Protocol
	Practice - The HTTP Protocol
	Web Sessions
	Practice - Web Sessions
	OWASP Top 10
	Lab - Website Vulnerability Scanning
	Lab - Using the GVM Vulnerability Scanner
How to Build Your Own Web Application Lab	Overview
Understanding Business Logic Flaws	Overview
	Practice - Business Logic Flaws
Understanding Injection-Based Vulnerabilities	Overview
	SQL Injection Vulnerabilities
	Practice - SQL Injection Attacks
	Command Injection Vulnerabilities
	Practice - Command Injection Vulnerabilities
	Lightweight Directory Access Protocol (LDAP) Injection Vulnerabilities
	Lab - Injection Attacks
Exploiting Authentication-Based Vulnerabilities	Overview
	Session Hijacking
	Practice - Session Hijacking
	Redirect Attacks
	Default Credentials

	Kerberos Vulnerabilities
	Practice - Kerberos Vulnerabilities
	Lab - Using Password Tools
Exploiting Authorization-Based Vulnerabilities	Overview
	Parameter Pollution
	Practice - Parameter Pollution
	Insecure Direct Object Reference Vulnerabilities
	Practice - Insecure Direct Object Reference Vulnerabilities
Understanding Cross-Site Scripting (XSS) Vulnerabilities	Overview
	Reflected XSS Attacks
	Practice - Reflected XSS Attacks
	Stored XSS Attacks
	Practice - Stored XSS Attacks
	XSS Evasion Techniques
	XSS Mitigations
	Lab - Cross Site Scripting
Understanding Cross-Site Request Forgery (CSRF/XSRF) and Server-Side Request Forgery Attacks	Overview
	Practice - CSRF/XSRF Attacks
Understanding Clickjacking	Overview
Exploiting Security Misconfigurations	Overview
	Exploiting Directory Traversal Vulnerabilities
	Practice - Directory Transversal
	Cookie Manipulation Attacks

Exploiting File Inclusion Vulnerabilities	Overview
	Local File Inclusion Vulnerabilities
	Remote File Inclusion Vulnerabilities
Exploiting Insecure Code Practices	Overview
	Comments in Source Code
	Lack of Error Handling and Overly Verbose Error Handling
	Practice - Insecure Code
	Hard-Coded Credentials
	Race Conditions
	Unprotected APIs
	Practice - Unprotected APIs
	Hidden Elements
	Lack of Code Signing
	Additional Web Application Hacking Tools
	Practice - Web Hacking Tools
	Lab - Use the OWASP Web Security Testing Guide
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Performing Post-Exploitation Techniques
Module 7: Cloud, Mobile, and IoT Security	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?

Researching Attack Vectors and Performing Attacks on Cloud Technologies	Overview
	Practice - Types of Cloud Services
	Credential Harvesting
	Practice - Credential Harvesting
	Privilege Escalation
	Account Takeover
	Metadata Service Attacks
	Attacks Against Misconfigured Cloud Assets
	Resource Exhaustion and DoS Attacks
	Cloud Malware Injection Attacks
	Side-Channel Attacks
	Practice - Cloud Attack Types
	Tools and Software Development Kits (SDKs)
Explaining Common Attacks and Vulnerabilities Against Specialized Systems	Overview
	Attacking Mobile Devices
	Practice - Mobile Device Vulnerabilities
	Practice - Attacking Mobile Devices
	Attacking Internet of Things (IoT) Devices
	Analyzing IoT Protocols
	Practice - Analyzing IoT Protocols
	IoT Security Special Considerations
	Common IoT Vulnerabilities
	Practice - Common IoT Vulnerabilities
	Data Storage System Vulnerabilities

	Management Interface Vulnerabilities
	Practice - Management Interface Vulnerabilities
	Exploiting Virtual Machines
	Vulnerabilities Related to Containerized Workloads
	Practice - Vulnerabilities Related to Containerized Workloads
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Cloud, Mobile, and IoT Security
Module 8: Performing Post-Exploitation Techniques	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?
Creating a Foothold and Maintaining Persistence After Compromising a System	Overview
	Reverse and Bind Shells
	Practice - Reverse and Bind Shells
	Command and Control (C2) Utilities
	Practice - Types of C2 Utilities
	Scheduled Jobs and Tasks
	Custom Daemons, Processes, and Additional Backdoors
	New Users
Understanding How to Perform Lateral Movement, Detection Avoidance, and Enumeration	Overview
	Post-Exploitation Scanning
	Legitimate Utilities and Living-off-the-Land
	Practice - Post Exploitation
	Post-Exploitation Privilege Escalation

	Practice - Post Exploitation Privilege Escalation
	How to Cover Your Tracks
	Practice – Steganography
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Performing Post-Exploitation Techniques
Module 9: Reporting and Communication	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?
Comparing and Contrasting Important Components of Written Reports	Overview
	Report Contents
	Practice - Penetration Reporting
	Storage Time for Report and Secure Distribution
	Practice - Control and Distribution of Reports
	Note Taking
	Common Themes/Root Causes
	Practice - Common Themes/Root Causes
	Lab - Explore PenTest Reports
Analyzing the Findings and Recommending the Appropriate Remediation Within a Report	Overview
	Technical Controls
	Administrative Controls
	Operational Controls
	Physical Controls
	Practice - Recommended Controls

	Lab - Recommend Remediation Based on Findings
Explaining the Importance of Communication During the Penetration Testing Process	Overview
	Communication Triggers
	Practice - Communication Triggers
	Reasons for Communication
	Goal Reprioritization and Presentation of Findings
Explaining Post-Report Delivery Activities	Overview
	Post-Engagement Cleanup
	Additional Post-Report Delivery Activities
	Practice - Post Report Delivery
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Reporting and Communication
Module 10: Tools and Code Analysis	
Introduction	Why Should I Take This Module?
	What Will I Learn in This Module?
Understanding the Basic Concepts of Scripting and Software Development	Overview
	Logic Constructs
	Practice - Logic Constructs
	Data Structures
	Practice - Data Structures
	Libraries
	Procedures
	Functions

	Classes
	Analysis of Scripts and Code Samples for Use in Penetration Testing
	Practice - Scripting
	The Bash Shell
	Resources to Learn Python
	Resources to Learn Ruby
	Resources to Learn PowerShell
	Resources to Learn Perl
	Resources to Learn JavaScript
	Practice - Programming Languages
	Lab - Analyze Exploit Code
	Lab - Analyze Automation Code
Understanding the Different Use Cases of Penetration Testing Tools and Analyzing Exploit Code	Overview
	Penetration Testing - Focused Linux Distributions
	Common Tools for Reconnaissance and Enumeration
	Practice - Common Tools for Reconnaissance and Enumeration
	Common Tools for Vulnerability Scanning
	Practice - Common Tools for Vulnerability Scanning
	Common Tools for Credential Attacks
	Practice - Common Tools for Credential Attacks
	Common Tools for Persistence
	Practice - Common Tools for Persistence
	Common Tools for Evasion

	Practice - Common Tools for Evasion
	Exploitation Frameworks
	Practice - Exploitation Frameworks
	Common Decompilation, Disassembly, and Debugging Tools
	Practice - Common Decompilation, Disassembly, and Debugging Tools
	Common Tools for Forensics
	Practice - Common Tools for Forensics
	Common Tools for Software Assurance
	Practice - Common Tools for Software Assurance
	Wireless Tools
	Practice - Wireless Tools
	Steganography Tools
	Practice - Steganography Tools
	Cloud Tools
	Practice - Cloud Tools
Summary	What Did I Learn in this Module?
	Reflection Questions
	Quiz - Tools and Code Analysis
Final Capstone Activity	
Final Capstone Activity	Objectives
	Required Resources
Ethical Hacker: Course Final Exam	
Course Final Exam	