THROUGHSEC

Penetration Testing and Ethical Hacking

This course is designed to provide participants with a comprehensive understanding of penetration testing methodologies, tools, and techniques. Covering foundational concepts to advanced exploitation and post-exploitation tactics, the course emphasizes real-world scenarios, preparing students for professional roles in cybersecurity.

Module 1: Fundamentals of Ethical Hacking and Information Gathering

Overview:
This module introduces students to the ethical hacking landscape, emphasizing the importance of methodology and legal considerations. It provides a solid foundation in reconnaissance techniques, enabling students to gather technical and organizational information about targets using open-source intelligence (OSINT) and active discovery methods.

Content:

1. **Introduction to Ethical Hacking**
    - Understanding the Penetration Testing Lifecycle
    - Legal and Ethical Considerations
    - Overview of Tools and Methodologies
2. **Information Gathering & Reconnaissance**
    - Host Discovery and Network Mapping
    - Port Scanning Techniques (TCP/UDP/Service Version Scans)
    - OS Fingerprinting and Service Enumeration
    - Extracting Technical Information from Public Sources
    - Email and Metadata Analysis
    - Tools: Nmap, Netcat, Recon-ng

Module 2: Host and Network Penetration Testing

Overview:
This module equips students with skills to test and exploit host and network infrastructures. It focuses on auditing techniques, leveraging tools like Metasploit for exploitation, and advanced network pivoting techniques to demonstrate lateral movement.

Content:

1. **Host and Networking Auditing**
    - System and Network Enumeration
    - Identifying Vulnerabilities in Services
    - Extracting Hashes and Passwords from Systems
    - Transferring Files to and from Targets
2. **Host and Network Exploitation**
    - Exploit Development and Modification
    - Using Metasploit for Exploitation
    - Pivoting Techniques (Port Forwarding and Adding Routes)
    - Tools: Metasploit, Mimikatz, ProxyChains

Module 3: Web Application Penetration Testing

Overview:
This module focuses on assessing web applications for vulnerabilities, including classic and modern attack vectors. Students will learn how to identify weaknesses, exploit them, and extract valuable data from compromised web applications.

Content:

1. **Introduction to Web Application Testing**
    - Understanding HTTP, Cookies, and Sessions
    - Web Application Reconnaissance Techniques
2. **Identifying and Exploiting Web Vulnerabilities**
    - SQL Injection, Cross-Site Scripting (XSS), Command Injection
    - Exploiting Vulnerable and Outdated Components
    - Brute-Forcing Login Forms
    - Identifying Hidden Files and Directories
3. **Data Exfiltration and Database Attacks**
    - Stealing Credentials from Compromised Applications
    - Tools: Burp Suite, OWASP ZAP

Module 4: Active Directory Penetration Testing

Overview:
Active Directory (AD) environments are central to most organizations. This module trains students to identify weaknesses in AD configurations, perform lateral movement, and escalate privileges to achieve domain administrator access.

Content:

1. **Introduction to Active Directory**
    - Understanding Domain Structures and AD Components
    - Enumeration of AD Accounts, Policies, and Groups
2. **Exploitation Techniques in AD Environments**
    - AS-REP Roasting and Stealing Kerberos Tickets
    - Lateral Movement (Pass-the-Hash, Pass-the-Ticket)
    - Privilege Escalation to Domain Admin
    - Tools: BloodHound, PowerView, Impacket

Module 5: Exploitation and Post-Exploitation Techniques

Overview:
This module dives deep into exploiting vulnerabilities and post-exploitation activities. It covers advanced tactics for maintaining access, extracting sensitive information, and developing custom exploits to fit unique scenarios.

Content:

1. **Vulnerability Exploitation**
    - Identifying and Exploiting Service Misconfigurations
    - Exploiting Privilege Escalation Vulnerabilities
2. **Post-Exploitation Tactics**
    - Dumping Password Hashes and Cracking Passwords
    - Extracting Locally Stored Credentials
    - Persisting Access and Cleaning Tracks
3. **Exploit Development**
    - Modifying Exploit Code for Specific Scenarios
    - Understanding Memory Corruption (Buffer Overflows, Stack Overflows)

- Tools: Immunity Debugger, GDB

Module 6: Capstone Project and Exam Preparation

Overview:
This final module consolidates all prior knowledge into practical, hands-on labs and a capstone project. Students will simulate real-world penetration tests in a controlled environment, preparing them for professional engagements and certification exams.

Content:

1. **Comprehensive Penetration Testing Lab**
    - Conduct End-to-End Assessment of a Simulated Enterprise Environment
    - Combine Network, Web, and AD Penetration Testing Skills
2. **Exam Preparation and Strategies**
    - Review Common Pitfalls in eCPPT , eJPT, CRTP and OSCP Exams

---

The audience for the **Penetration Testing and Ethical Hacking** course includes:

1. **Aspiring Penetration Testers**: Individuals looking to enter the field of ethical hacking and cybersecurity, with an interest in learning real-world penetration testing methodologies, tools, and techniques.
2. **Cybersecurity Enthusiasts**: Those with a passion for cybersecurity who want to expand their skillset in offensive security, particularly in ethical hacking and penetration testing.
3. **IT Professionals**: Professionals in IT roles, such as network administrators, system administrators, and security officers, who want to gain deeper knowledge of penetration testing to improve their organization's security posture.
4. **Security Consultants**: Cybersecurity consultants seeking to enhance their technical skills to provide more thorough assessments and recommendations for clients in terms of vulnerability identification and remediation.
5. **Students in Cybersecurity**: Undergraduate or graduate students who are studying cybersecurity and wish to gain practical, hands-on experience in penetration testing to complement their academic knowledge.
6. **Certified Ethical Hackers**: Individuals already certified in ethical hacking (CEH, OSCP) who want to further enhance their skills in advanced exploitation and post-exploitation techniques, including Active Directory testing and web application security.
7. **Professionals Seeking Certification**: Individuals preparing for industry-recognized certifications such as eCPPT, eJPT, CRTP, or OSCP and who need to refine their penetration testing skills through practical labs and capstone projects.