CYBERIUM

Learn ETHICAL HACKING

Online Training

INTRODUCTION

With the rapid growth of technology, cyber threats have become more sophisticated, making cybersecurity a critical concern for individuals, businesses, and governments. Ethical hacking plays a vital role in securing digital assets by proactively identifying and addressing vulnerabilities before malicious hackers can exploit them. This comprehensive Ethical Hacking course, designed for aspiring cybersecurity professionals, security analysts, and IT enthusiasts, provides an in-depth understanding of hacking methodologies, security tools, and best practices to protect networks, systems, and applications.

The course begins with an introduction to cybersecurity, covering the fundamental concepts of information security, attack vectors, and the importance of ethical hacking. Participants will learn about different cyber threats, including malware, ransomware, phishing, and denial-of-service (DoS) attacks, along with the legal and ethical considerations involved in penetration testing. Setting up a controlled and legal lab environment for ethical hacking practice is also a crucial part of the initial phase.

A key focus of the course is on the phases of ethical hacking, which mirror real-world cyberattack strategies. The first phase, reconnaissance, teaches information gathering techniques using open-source intelligence (OSINT) and footprinting tools. This is followed by scanning, where students learn to identify vulnerabilities in networks and systems through active scanning, enumeration, and fingerprinting.

Once vulnerabilities are identified, the course moves to gaining access, where students explore various exploitation techniques, including password cracking, privilege escalation, and exploiting system misconfigurations. After gaining access, maintaining access is covered, explaining methods used by attackers to create backdoors and persist within compromised systems. The final phase, covering tracks, delves into anti-forensics techniques and log manipulation, demonstrating how attackers attempt to erase evidence of their intrusion.

The course also covers malware analysis and denial-of-service (DoS) attacks, where students explore different types of malware, including viruses, trojans, and worms, as well as DoS and DDoS attack methodologies. Understanding these threats enables learners to implement effective mitigation strategies.

INTRODUCTION

A crucial part of the course is social engineering, which examines the psychological manipulation tactics used by attackers to deceive individuals into revealing sensitive information. From phishing scams to impersonation techniques, students will learn how to recognize and prevent social engineering attacks.

The sniffing and network security section introduces packet analysis techniques, including the use of tools like Wireshark. Students will explore network attacks like ARP poisoning and Man-in-the-Middle (MITM) attacks, alongside best practices for securing networks.

Web applications are a common attack target, and the course dedicates a section to web application security, focusing on vulnerabilities such as SQL injection, cross-site scripting (XSS), and security misconfigurations. Students will learn how to test and secure web applications effectively.

Additionally, the course includes cryptography and secure communication, covering encryption techniques, hashing algorithms, and SSL/TLS protocols to ensure data confidentiality and integrity.

Finally, the course concludes with wireless and mobile hacking, where students explore wireless security weaknesses, WPA2 cracking, and mobile application vulnerabilities. Practical hands-on labs, Capture The Flag (CTF) challenges, and penetration testing projects ensure that participants gain real-world experience.

By the end of the course, learners will have a solid foundation in ethical hacking, enabling them to pursue careers in cybersecurity, conduct penetration tests, and contribute to strengthening digital security.

Course Duration - 40 Hours

ETHICAL HACKING SYLLABUS

Module 01- Introduction to Ethical Hacking

1. What is Hacking?
2. Types of Hackers (White Hat, Black Hat, Grey Hat)
3. What is Ethical Hacking?
4. Importance of Cyber Security
5. Phases of Ethical Hacking
6. Setting Up a Hacking Lab (Kali Linux, Virtual Machines, Windows, Metasploitable, OWASP-BWA)
7. How to use your Kali Linux for Ethical Hacking
8. Basics commands of Kali Linux OS

Module 02- Cyber Security Fundamentals

1. What is Cyber Security?
2. What is Information Security?
3. Elements of Information Security
4. Essential Networking Concepts for Hackers (IP, MAC, DNS, ARP, OSI & TCP/IP Models)
5. Understanding Cyber Threats
6. Common Cyber Attacks
7. Vulnerabilities, and Exploits

Module 03- Reconnaissance & Footprinting

1. **What is Reconnaissance?**
2. **Types of Footprinting (Active & Passive)**
3. **Gathering Information from Open Sources (OSINT)**
    a. **Google Hacking (Google Dorking)**
    b. **Google Hacking Database**
    c. **WHOIS Lookups**
    d. **DNS Footprinting (NSLookup, Dig)**
    e. **Social Media Intelligence (SOCMINT)**
4. **Practical Lab: OSINT & Google Dorking Techniques**

Module 04- Scanning & Enumeration

1. **Understanding Scanning & Enumeration**
2. **Types of Scanning**
    a. **Network Scanning (TCP, UDP)**
    b. **Port Scanning (Nmap, Zenmap)**
    c. **Vulnerability Scanning (Nessus)**
3. **Banner Grabbing & Service Fingerprinting**
4. **Operating System Detection**
5. **Enumeration Techniques**
    a. **FTP, SMB, SSH Enumeration**
6. **Practical Lab: Using Nmap & Nessus for Scanning & Enumeration**

Module 05- Gaining Access

1. **Exploiting Vulnerabilities**
2. **Types of Exploits (Zero-Day, Known Vulnerabilities)**
3. **Exploiting Vulnerabilities with Metasploit Framework (MSFconsole)**
4. **Exploiting Vulnerabilities with Exploit Database**
5. **Brute Force & Password Cracking (Hydra, John the Ripper, Hashcat)**
6. **Privilege Escalation**
7. **Practical Lab: Exploiting Vulnerabilities Using Metasploit & Hydra**

Module 06- Maintaining Access

1. **Backdoors, Spywares & Trojans**
2. **Netcat & Reverse Shells**
3. **Practical Lab: Using Trojans and Spywares**

Module 07- Covering Tracks

1. **Clearing Logs & Removing Traces**
2. **Clearing Commands**
3. **Practical Lab: Covering Tracks in Windows & Linux**

Module 08- Malware & Ransomware Analysis

1. **Types of Malware (Viruses, Trojans, Worms, Ransomware)**
2. **Working of a Ransomware**
3. **Working of Trojan Horse**
4. **Creating & Analyzing Malware**
5. **Practical Lab: Creating & Detecting Malware using SEToolkit**

Module 09- Denial of Service (DoS) & Distributed DoS (DDoS) Attacks

1. **Understanding DoS & DDoS Attacks**
2. **Types of DoS Attacks (SYN Flood, Ping of Death Flood, HTTP Flood)**
3. **Using LOIC and Hping3 for DoS Attacks**
4. **Mitigation Techniques (Firewalls, Rate Limiting, WAF)**
5. **Practical Lab: Simulating a DoS Attack using Hping3**

Module 10- Social Engineering Attacks

1. **Psychology Behind Social Engineering**
2. **Types of Social Engineering Attacks**
    a. **Phishing (Spear Phishing, Whaling, Smishing)**
    b. **Impersonation & Pretexting**
    c. **Baiting & Tailgating**
3. **Using Social Engineering Toolkit (SET)**
4. **How to protect against Phishing**
5. **Practical Lab: Conducting a Phishing Attack Simulation**

Module 11- Sniffing & Traffic Analysis

1. **What is Packet Sniffing?**
2. **Tools: Wireshark, TCPDump, Ettercap**
3. **MITM (Man-in-the-Middle) Attack**
4. **MAC Spoofing & ARP Poisoning**
5. **Practical Lab: Intercepting Network Traffic using Wireshark**

Module 12- Web Application Security & OWASP Top 10

1. **Understanding Web Architecture**
2. **Common Web App Vulnerabilities**
3. **OWASP Top 10 Web Application Vulnerabilities**
4. **Injection Attacks (SQL Injection, Command Injection)**
5. **Cross-Site Scripting (XSS)**
6. **Cross-Site Request Forgery (CSRF)**
7. **File Upload Vulnerability**
8. **Directory Traversal**
9. **Security Misconfigurations & Broken Authentication**
10. **Practical Lab: Exploiting SQLi & XSS on DVWA**

Module 13- Cryptography & Encryption Techniques

1. Basics of Cryptography (Symmetric & Asymmetric Encryption)
2. Hashing & Digital Signatures
3. Cracking Hashes with Hashcat
4. Encoding and Decoding
5. Practical Lab: Encryption, Hashing and Encoding

Module 14- Wireless Network Hacking

1. Wireless Network Fundamentals
2. Wireless Security Fundamentals
3. WEP, WPA, WPA2 & WPA3 Security
4. Evil Twin Attack
5. Cracking Wi-Fi Passwords (Aircrack-ng)
6. Deauthentication Attack
7. Practical Lab: Capturing & Cracking Wi-Fi Handshakes

Module 15- Mobile Hacking & Security

1. Understanding Mobile Devices
2. Understanding Mobile Vulnerabilities
3. Android Hacking with Kali Linux
4. Reverse Shell on Android using Metasploit
5. Practical Lab: Exploiting an Android Device using Metasploit

Module 16- Ethical Hacking Challenges & Real-World Scenarios

1. Bug Bounty Programs
2. CTF (Capture The Flag) Competitions
3. Legal & Ethical Responsibilities of an Ethical Hacker
4. Best Practices for Cyber Security
5. Career Paths in Ethical Hacking