CyberGate ACADEMY

EC-COUNCIL

CERTIFIED ETHICAL HACKER COURSE

Course Overview

A Certified Ethical Hacker (CEH) is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems. A Ethical Hacker uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident. CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.

Course Duration

5 Days (40 Hours).

Target Audience

The Certified Ethical Hacking training course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

During this course you should learn

- Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
- Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
- Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
- Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
- Social engineering techniques and how to identify theft attacks to audit humanlevel vulnerabilities and suggest social engineering countermeasures.
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
- Session hijacking techniques to discover network-level session management, authentication/ authorization, cryptographic weaknesses, and countermeasures.
- Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
- Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
- SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
- Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.

- Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
- Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Course Content

Module 1: Introduction to Ethical Hacking

Lesson 1: Information Security Overview

Lesson 2: Cyber Kill Chain Concepts

Lesson 3: Hacking Concepts

Lesson 4: Ethical Hacking Concepts

Lesson 5: Information Security Controls

Lesson 6: Information Security Laws and Standards

Module 2: Footprinting and Reconnaissance

Lesson 1: Footprinting Concepts

Lesson 2: Footprinting through Search Engines

Lesson 3: Footprinting through Web Services

Lesson 4: Footprinting through Social Networking Sites

Lesson 5: Website Footprinting

Lesson 6: Email Footprinting

Lesson 7: Whois Footprinting

Lesson 8: DNS Footprinting

Lesson 9: Network Footprinting

Lesson 10: Footprinting through Social Engineering

Lesson 11: Footprinting Tools

Lesson 12: Footprinting Countermeasures

Module 3: Scanning Networks

Lesson 1: Network Scanning Concepts

Lesson 2: Scanning Tools

Lesson 3: Host Discovery

Lesson 4: Port and Service Discovery

Lesson 5: OS Discovery (Banner Grabbing/OS Fingerprinting)

Lesson 6: Scanning Beyond IDS and Firewall

Lesson 7: Banner Grabbing

Lesson 8: Draw Network Diagrams

Module 4: Enumeration

- Lesson 1: Enumeration Concepts
- Lesson 2: NetBIOS Enumeration
- Lesson 3: SNMP Enumeration
- Lesson 4: LDAP Enumeration
- Lesson 5: NTP and NFS Enumeration
- Lesson 6: SMTP and DNS Enumeration
- Lesson 7: Other Enumeration Techniques
- Lesson 8: Enumeration Countermeasures

Module 5: Vulnerability Analysis

- Lesson 1: Vulnerability Assessment Concepts
- Lesson 2: Vulnerability Classification and Assessment Types
- Lesson 3: Vulnerability Assessment Solutions and Tools
- Lesson 4: Vulnerability Assessment Reports

Module 6: System Hacking

- Lesson 1: System Hacking Concepts
- Lesson 2: Gaining Access
- Lesson 3: Escalating Privileges
- Lesson 4: Maintaining Access
- Lesson 5: Clearing Logs

Module 7: Malware Threats

- Lesson 1: Malware Concepts
- Lesson 2: APT Concepts
- Lesson 3: Trojan Concepts
- Lesson 4: Virus and Worm Concepts
- Lesson 5: Fileless Malware Concepts
- Lesson 6: Malware Analysis
- Lesson 7: Countermeasures
- Lesson 8: Anti-Malware Software

Module 8: Sniffing

- Lesson 1: Sniffing Concepts
- Lesson 2: Sniffing Technique: MAC Attacks
- Lesson 3: Sniffing Technique: DHCP Attacks
- Lesson 4: Sniffing Technique: ARP Poisoning
- Lesson 5: Sniffing Technique: Spoofing Attacks
- Lesson 6: Sniffing Technique: DNS Poisoning
- Lesson 7: Sniffing Tools
- Lesson 8: Countermeasures
- Lesson 9: Sniffing Detection Techniques

Module 9: Social Engineering

- Lesson 1: Social Engineering Concepts
- Lesson 2: Social Engineering Techniques
- Lesson 3: Insider Threats
- Lesson 4: Impersonation on Social Networking Sites
- Lesson 5: Identity Theft
- Lesson 6: Countermeasures

Module 10: Denial-of-Service

- Lesson 1: DoS/DDoS Concepts
- Lesson 2: DoS/DDoS Attack Techniques
- Lesson 3: Botnets
- Lesson 4: DDoS Case Study
- Lesson 5: DoS/DDoS Attack Tools
- Lesson 6: Countermeasures
- Lesson 7: DoS/DDoS Protection Tools

Module 11: Session Hijacking

- Lesson 1: Session Hijacking Concepts
- Lesson 2: Application Level Session Hijacking
- Lesson 3: Network Level Session Hijacking
- Lesson 4: Session Hijacking Tools
- Lesson 5: Countermeasures

Module 12: Evading IDS, Firewalls, and Honeypots

- Lesson 1: IDS, IPS, Firewall and Honeypot Concepts
- Lesson 2: IDS, IPS, Firewall and Honeypot Solutions
- Lesson 3: Evading IDS
- Lesson 4: Evading Firewalls
- Lesson 5: IDS/Firewall Evading Tools
- Lesson 6: Detecting Honeypots
- Lesson 7: IDS/Firewall Evasion Countermeasures

Module 13: Hacking Web Servers

- Lesson 1: Web Server Concepts
- Lesson 2: Web Server Attacks
- Lesson 3: Web Server Attack Methodology
- Lesson 4: Web Server Attack Tools
- Lesson 5: Countermeasures
- Lesson 6: Patch Management
- Lesson 7: Web Server Security Tools.

Module 14: Hacking Web Applications

- Lesson 1: Web Application Concepts
- Lesson 2: Web Application Threats
- Lesson 3: Web Application Hacking Methodology
- Lesson 4: Web API, Webhooks and Web Shell
- Lesson 5: Web Application Security

Module 15: SQL Injection

- Lesson 1: SQL Injection Concepts
- Lesson 2: Types of SQL Injection
- Lesson 3: SQL Injection Methodology
- Lesson 4: SQL Injection Tools
- Lesson 5: Evasion Techniques
- Lesson 6: Countermeasures

Module 16: Hacking Wireless Networks

- Lesson 1: Wireless Concepts
- Lesson 2: Wireless Encryption
- Lesson 3: Wireless Threats
- Lesson 4: Wireless Hacking Methodology
- Lesson 5: Wireless Hacking Tools
- Lesson 6: Bluetooth Hacking
- Lesson 7: Countermeasures
- Lesson 8: Wireless Security Tools

Module 17: Hacking Mobile Platforms

- Lesson 1: Mobile Platform Attack Vectors
- Lesson 2: Hacking Android OS
- Lesson 3: Hacking iOS
- Lesson 4: Mobile Device Management
- Lesson 5: Mobile Security Guidelines and Tools

Module 18: IoT and OT Hacking

- Lesson 1: IoT Concepts
- Lesson 2: IoT Attacks
- Lesson 3: IoT Hacking Methodology
- Lesson 4: IoT Hacking Tools
- Lesson 5: Countermeasures
- Lesson 6: OT Concepts
- Lesson 7: OT Attacks
- Lesson 8: OT Hacking Methodology
- Lesson 9: OT Hacking Tools
- Lesson 10: Countermeasures

Module 19: Cloud Computing

Lesson 1: Cloud Computing Concepts
Lesson 2: Container Technology
Lesson 3: Serverless Computing
Lesson 4: Cloud Computing Threats
Lesson 5: Cloud Hacking
Lesson 6: Cloud Security

Module 20: Cryptography

Lesson 1: Cryptography Concepts
Lesson 2: Encryption Algorithms
Lesson 3: Cryptography Tools
Lesson 4: Public Key Infrastructure (PKI)
Lesson 5: Email Encryption
Lesson 6: Disk Encryption
Lesson 7: Cryptanalysis
Lesson 8: Countermeasures.

Prerequisites

Attendees should meet the following prerequisites:

- Have two years' IT work experience and a possess a basic familiarity of Linux and/or Unix.
- A strong working knowledge of:
  - TCP/IP
  - Windows Server

Course Agenda

Day 1	Module 1: Introduction to Ethical Hacking Module 2: Footprinting and Reconnaissance Module 3: Scanning Networks **Module 4: Enumeration**
Day 2	Module 5: Vulnerability Analysis Module 6: System Hacking Module 7: Malware Threats **Module 8: Sniffing**
Day 3	Module 9: Social Engineering Module 10: Denial-of-Service Module 11: Session Hijacking **Module 12: Evading IDS, Firewalls, and Honeypots**
Day 4	Module 13: Hacking Web Servers Module 14: Hacking Web Applications **Module 15: SQL Injection**
Day 5	Module 16: Hacking Wireless NetworksModule 17: Hacking Mobile Platforms Module 18: IoT and OT Hacking Module 19: Cloud Computing **Module 20: Cryptography**

Technical Requirement

1. Laptop with minimum 8GB Ram.
2. Connected Monitor for iLabs.
3. Hi speed Internet Connection as All the labs it will be accessed through EC-Council Cloud.

Exam Voucher Validity

It will be valid for 12month starting from the last day of the course.

Certification Expiry

It will be valid for 3 years.

CyberGate ACADEMY

YOUR TRUSTED DEFENDERS

ADDRESS

CyberGate Academy
ADPOLY, MBZ City

WEB

academy@cybergate.tech
training@cybergate.tech