Course Outline

EC-Council Certified Ethical Hacker v12 (CEHv12)

Course Summary

Description

C|EH is divided into 20 modules and delivered through a carefully curated training plan that typically spans across 5 days. As you progress through your training, each module offers extensive hands-on lab components that allow you to practice the techniques and procedures taught in the program in real-time on live machines.

Ethical Hacking Labs: With over 220 hands-on labs, conducted in our cyber range environment, you will have the opportunity to practice every learning objective in the course on live machines and vulnerable targets. Pre-loaded with over 3,500 hacking tools and a variety of operating systems, you will gain unprecedented exposure to and hands-on experience with the most common security tools, latest vulnerabilities, and widely used operating systems on the market. Our range is web accessible, allowing you to study and practice from anywhere with a connection.

Topics

- Introduction to Ethical Hacking
- Foot Printing and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

Audience

This course is designed for:

- Mid-Level Information Security Auditor
- Cybersecurity Auditor
- Security Administrator
- IT Security Administrator
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- Information Security Analyst 1
- Security Analyst L1
- Infosec Security Administrator
- Cybersecurity Analyst level 1, level 2, & level 3
- Network Security Engineer
- SOC Security Analyst
- Security Analyst
- Network Engineer
- Senior Security Consultant
- Information Security Manager
- Senior SOC Analyst
- Solution Architect
- Cybersecurity Consultant

Prerequisites

Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent. Not anyone can be a student - the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Duration

Five days

EC-Council Certified Ethical Hacker v12 (CEHv12)

Course Outline

I. Introduction to Ethical Hacking

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

A. Elements of Information Security, Cyber Kill Chain Methodology, MITRE ATT&CK Framework, Hacker Classes, Ethical Hacking, Information Assurance (IA), Risk Management, Incident Management, PCI DSS, HIPPA, SOX, GDPR

II. Foot Printing and Reconnaissance

Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

A. Hands-On Lab Exercises:
   1. Over 30 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform foot printing on the target network using search engines, web services, and social networking sites
   3. Perform website, email, whois, DNS, and network foot printing on the target network

III. Scanning Networks

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

A. Hands-On Lab Exercises:
   1. Over 10 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform host, port, service, and OS discovery on the target network
   3. Perform scanning on the target network beyond IDS and firewall

IV. Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, plus associated countermeasures.

A. Hands-On Lab Exercises:
   1. Over 20 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform NetBIOS, SNMP, LDAP, NFS, DNS, SMTP, RPC, SMB, and FTP Enumeration

V. Vulnerability Analysis

Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems.

A. Hands-On Lab Exercises:
   1. Over 5 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform vulnerability research using vulnerability scoring systems and databases
   3. Perform vulnerability assessment using various vulnerability assessment tools

VI. System Hacking

Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

VII. Hands-On Lab Exercises:
   1. Over 25 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform Online active online attack to crack the system's password
   3. Perform buffer overflow attack to gain access to a remote system
   4. Escalate privileges using privilege escalation tools
   5. Escalate privileges in linux machine
   6. Hide data using steganography
   7. Clear Windows and Linux machine logs using various utilities
   8. Hiding artifacts in Windows and Linux machines

EC-Council Certified Ethical Hacker v12 (CEHv12)

Course Outline (cont'd)

VIII. Malware Threats

Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for malware attacks, malware analysis, and countermeasures.

A. Hands-On Lab Exercises:
   1. Over 20 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Gain control over a victim machine using Trojan
   3. Infect the target system using a virus
   4. Perform static and dynamic malware analysis

B. Key topics covered:
   1. Malware, Components of Malware, APT, Trojan, Types of Trojans, Exploit Kits, Virus, Virus Lifecycle, Types of Viruses, Ransomware, Computer Worms, Fileless Malware, Malware Analysis, Static Malware Analysis, Dynamic Malware Analysis, Virus Detection Methods, Trojan Analysis, Virus Analysis, Fileless Malware Analysis, Anti-Trojan Software, Antivirus Software, Fileless Malware Detection Tools

IX. Sniffing

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

A. Hands-On Lab Exercises:
   1. Over 10 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform MAC flooding, ARP poisoning, MITM and DHCP starvation attack
   3. Spoof a MAC address of Linux machine
   4. Perform network sniffing using various sniffing tools
   5. Detect ARP poisoning in a switch-based network

B. Key topics covered:
   1. Network Sniffing, Wiretapping, MAC Flooding, DHCP Starvation Attack, ARP Spoofing Attack, ARP Poisoning, ARP Poisoning Tools, MAC Spoofing, STP Attack, DNS Poisoning, DNS Poisoning Tools, Sniffing Tools, Sniffer Detection Techniques, Promiscuous Detection Tools

X. Social Engineering

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

A. Hands-On Lab Exercises:
   1. Over 4 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform social engineering using Various Techniques
   3. Spoof a MAC address of a Linux machine
   4. Detect a phishing attack
   5. Audit an organization's security for phishing attacks

B. Key topics covered:
   1. Social Engineering, Types of Social Engineering, Phishing, Phishing Tools, Insider Threats/Insider Attacks, Identity Theft

XI. Denial-of-Service

Learn about different Denial-of-Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

A. Hands-On Lab Exercises:
   1. Over 5 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform a DoS and DDoS attack on a target host
   3. Detect and protect against DoS and DDoS attacks

B. Key topics covered:
   1. DoS Attack, DDoS Attack, Botnets, DoS/DDoS Attack Techniques, DoS/DDoS Attack Tools, DoS/DDoS Attack Detection Techniques, DoS/DDoS Protection Tools

Course Outline (cont'd)

XII. Session Hijacking

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

A. Hands-On Lab Exercises:
   1. Over 4 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform session hijacking using various tools
   3. Detect session hijacking

B. Key topics covered:
   1. Session Hijacking, Types of Session Hijacking, Spoofing, Application-Level Session Hijacking, Man-in-the-Browser Attack, Client-side Attacks, Session Replay Attacks, Session Fixation Attack, CRIME Attack, Network Level Session Hijacking, TCP/IP Hijacking, Session Hijacking Tools, Session Hijacking Detection Methods, Session Hijacking Prevention Tools

XIII.Evading IDS, Firewalls, and Honeypots

Get introduced to firewall, intrusion detection system, and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

A. Hands-On Lab Exercises:
   1. Over 7 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Bypass Windows Firewall
   3. Bypass firewall rules using tunneling
   4. Bypass antivirus

XIV. Hacking Web Servers

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

A. Hands-On Lab Exercises:
   1. Over 8 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform web server reconnaissance using various tools
   3. Enumerate web server information
   4. Crack FTP credentials using a dictionary attack

B. Key topics covered:
   1. Web Server Operations, Web Server Attacks, DNS Server Hijacking, Website Defacement, Web Cache Poisoning Attack, Web Server Attack Methodology, Web Server Attack Tools, Web Server Security Tools, Patch Management, Patch Management Tools

XV. Hacking Web Applications

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

A. Hands-On Lab Exercises:
   1. Over 15 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform web application reconnaissance using various tools
   3. Perform web spidering
   4. Perform web application vulnerability scanning
   5. Perform a brute-force attack
   6. Perform Cross-Site Request Forgery (CSRF) Attack
   7. Identify XSS vulnerabilities in web applications
   8. Detect web application vulnerabilities using various web application security tools

B. Key topics covered:
   1. Web Application Architecture, Web Application Threats, OWASP Top 10 Application Security Risks – 2021, Web Application Hacking Methodology, Web API, Webhooks, and Web Shell, Web API Hacking Methodology, Web Application Security

Course Outline (cont'd)

XVI. SQL Injection

Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.

A. Hands-On Lab Exercises:
   1. Over 4 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform an SQL injection attack against MSSQL to extract databases
   3. Detect SQL injection vulnerabilities using various SQL injection detection tools

B. Key topics covered:
   1. SQL Injection, Types of SQL injection, Blind SQL Injection, SQL Injection Methodology, SQL Injection Tools, Signature Evasion Techniques, SQL Injection Detection Tools

XVII. Hacking Wireless Networks

Learn about wireless encryption, wireless hacking methodologies and tools, and Wi-Fi security tools

A. Hands-On Lab Exercises:
   1. Over 3 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Foot Print a wireless network
   3. Perform wireless traffic analysis
   4. Crack WEP, WPA, and WPA2 networks
   5. Create a rogue access point to capture data packets

B. Key topics covered:
   1. Wireless Terminology, Wireless Networks, Wireless Encryption, Wireless Threats, Wireless Hacking Methodology, Wi-Fi Encryption Cracking, WEP/WPA/WPA2 Cracking Tools, Bluetooth Hacking, Bluetooth Threats, Wi-Fi Security Auditing Tools, Bluetooth Security Tools

XVIII. Hacking Mobile Platforms

Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.

A. Hands-On Lab Exercises:
   1. Over 5 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Hack an Android device by creating binary payloads
   3. Exploit the Android platform through ADB
   4. Hack an Android device by creating APK file
   5. Secure Android devices using various Android security tools

B. Key topics covered:
   1. Mobile Platform Attack Vectors, OWASP Top 10 Mobile Risks, App Sandboxing, SMS Phishing Attack (SMiShing), Android Rooting, Hacking Android Devices, Android Security Tools, Jailbreaking iOS, Hacking iOS Devices, iOS Device Security Tools, Mobile Device Management (MDM), OWASP Top 10 Mobile Controls, Mobile Security Tools.

XIX. IoT and OT Hacking

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

A. Hands-On Lab Exercises:
   1. Over 2 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Gather information using Online foot printing tools
   3. Capture and analyze IoT device traffic

B. Key topics covered:
   1. IoT Architecture, IoT Communication Models, OWASP Top 10 IoT Threats, IoT Vulnerabilities, IoT Hacking Methodology, IoT Hacking Tools, IoT Security Tools, IT/OT Convergence (IIOT), ICS/SCADA,

Course Outline (cont'd)

2. OT Vulnerabilities, OT Attacks, OT Hacking Methodology, OT Hacking Tools, OT Security Tools

XX. Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud-based threats and attacks, and cloud security techniques and tools.

A. Hands-On Lab Exercises:
   1. Over 5 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Perform S3 Bucket enumeration using various S3 bucket enumeration tools
   3. Exploit open S3 buckets
   4. Escalate IAM user privileges by exploiting misconfigured user policy

B. Key topics covered:
   1. Cloud Computing, Types of Cloud Computing Services, Cloud Deployment Models, Fog and Edge Computing, Cloud Service Providers, Container, Docker, Kubernetes, Serverless Computing, OWASP Top 10 Cloud Security Risks, Container and Kubernetes Vulnerabilities, Cloud Attacks, Cloud Hacking, Cloud Network Security, Cloud Security Controls, Cloud Security Tools

XXI. Cryptography

In the final module, learn about cryptography and ciphers, public-key infrastructure, cryptography attacks, and cryptanalysis tools.

A. Hands-On Lab Exercises:
   1. Over 10 hands-on exercises with real-life simulated targets to build skills on how to:
   2. Calculate MD5 hashes
   3. Perform file and text message encryption
   4. Create and use self-signed certificates
   5. Perform email and disk encryption
   6. Perform cryptanalysis using various cryptanalysis tools

B. Key topics covered:
   1. Cryptography, Encryption Algorithms, MD5 and MD6 Hash Calculators, Cryptography Tools, Public Key Infrastructure (PKI), Email Encryption, Disk Encryption, Cryptanalysis, Cryptography Attacks, Key Stretching