Certified Ethical Hacker - CEH v12 Syllabus

Module 01: Introduction to Ethical Hacking 2 Hours - 11 Topics

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.

Key topics covered:

- **Elements of Information Security (Day 1)**
- **Cyber Kill Chain Methodology (Day 1)**
- **MITRE ATT&CK Framework (Day 1)**
- **Hacker Classes, Ethical Hacking (Day 1)**
- **Information Assurance (IA) (Day 1)**
- **Risk Management (Day 1)**
- **Incident Management (Day 1)**
- **PCI DSS (Day 1)**
- **HIPPA (Day 1)**
- **SOX (Day 1)**
- **GDPR (Day 1)**

Module 02: Foot Printing and Reconnaissance 2 Hours - 2 Topics

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.

Hands-On Lab Exercises:

Over 30 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform foot printing on the target network using search engines, web services, and social networking sites (Day 2)**
- **Perform website, email, whois, DNS, and network foot printing on the target network (Day 2)**

Module 03: Scanning Networks 2 Hours - 2 Topics

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.

Hands-On Lab Exercises:

Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform host, port, service, and OS discovery on the target network (Day 3)**
- **Perform scanning on the target network beyond IDS and firewall (Day 3)**

Module 04: Enumeration 2 Hours - 1 Topic

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

Hands-On Lab Exercises:

Over 20 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform NetBIOS, SNMP, LDAP, NFS, DNS, SMTP, RPC, SMB, and FTP Enumeration (Day 4)**

Module 05: Vulnerability Analysis — 2 Hours - 2 Topics

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

Hands-On Lab Exercises:

Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform vulnerability research using vulnerability scoring systems and databases (Day 5)**
- **Perform vulnerability assessment using various vulnerability assessment tools (Day 5)**

Module 06: System Hacking — 2 Hours - 7 Topics

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

Hands-On Lab Exercises:

Over 25 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform Online active online attack to crack the system's password (Day 6)**
- **Perform buffer overflow attack to gain access to a remote system (Day 6)**
- **Escalate privileges using privilege escalation tools (Day 6)**
- **Escalate privileges in linux machine (Day 6)**
- **Hide data using steganography (Day 6)**
- **Clear Windows and Linux machine logs using various utilities (Day 6)**
- **Hiding artifacts in Windows and Linux machines (Day 6)**

Module 07: Malware Threats — 2 Hours - 22 Topics

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.

Hands-On Lab Exercises:

Over 20 hands-on exercises with real-life simulated targets to build skills on how to:

- **Gain control over a victim machine using Trojan (Day 7)**
- **Infect the target system using a virus (Day 7)**
- **Perform static and dynamic malware analysis (Day 7)**

Key topics covered:

- **Malware (Day 7)**
- **Components of Malware (Day 7)**
- **APT (Day 7)**
- **Trojan (Day 7)**
- **Types of Trojans (Day 7)**
- **Exploit Kits (Day 7)**
- **Virus (Day 7)**

- **Virus Lifecycle (Day 7)**
- **Types of Viruses (Day 7)**
- **Ransomware (Day 7)**
- **Computer Worms (Day 7)**
- **Fileless Malware (Day 7)**
- **Malware Analysis (Day 7)**
- **Static Malware Analysis (Day 7)**
- **Dynamic Malware Analysis (Day 7)**
- **Virus Detection Methods (Day 7)**
- **Trojan Analysis (Day 7)**
- **Virus Analysis (Day 7)**
- **Fileless Malware Analysis (Day 7)**
- **Anti-Trojan Software (Day 7)**
- **Antivirus Software (Day 7)**
- **Fileless Malware Detection Tools (Day 7)**

Module 08: Sniffing 2 Hours - 14 Topics

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

Hands-On Lab Exercises:

Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform MAC flooding, ARP poisoning, MITM and DHCP starvation attack (Day 8)**
- **Spoof a MAC address of Linux machine (Day 8)**
- **Perform network sniffing using various sniffing tools (Day 8)**
- **Detect ARP poisoning in a switch-based network (Day 8)**

Key topics covered:

- **Network Sniffing (Day 8)**
- **SWiretapping (Day 8)**
- **MAC Flooding (Day 8)**
- **DHCP Starvation Attack (Day 8)**
- **ARP Spoofing Attack (Day 8)**
- **ARP Poisoning (Day 8)**
- **ARP Poisoning Tools (Day 8)**
- **MAC Spoofing (Day 8)**
- **STP Attack (Day 8)**
- **DNS Poisoning (Day 8)**
- **DNS Poisoning (Day 8) Tools**
- **Sniffing Tools (Day 8)**
- **Sniffer Detection Techniques (Day 8)**
- **Promiscuous Detection Tools (Day 8)**

Module 09: Social Engineering 2 Hours - 6 Topics

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

Hands-On Lab Exercises:

Over 4 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform social engineering using Various Techniques (Day 9)**
- **Spoof a MAC address of a Linux machine (Day 9)**
- **Detect a phishing attack (Day 9)**
- **Audit an organization's security for phishing attacks (Day 9)**

Key topics covered:

- **Social Engineering (Day 9)**
- **Types of Social Engineering (Day 9)**
- **Phishing (Day 9)**
- **Phishing Tools (Day 9)**
- **Insider Threats/Insider Attacks (Day 9)**
- **Identity Theft (Day 9)**

Module 10: Denial-of-Service 2 Hours - 7 Topics

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.

Hands-On Lab Exercises:

Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform a DoS and DDoS attack on a target host (Day 10)**
- **Detect and protect against DoS and DDoS attacks (Day 10)**

Key topics covered:

- **DoS Attack (Day 10)**
- **DDoS Attack**
- **Botnets**
- **DoS/DDoS Attack Techniques**
- **DoS/DDoS Attack Tools**
- **DoS/DDoS Attack Detection Techniques**
- **DoS/DDoS Protection Tools**

Module 11: Session Hijacking 2 Hours - 14 Topics

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

Hands-On Lab Exercises:

Over 4 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform session hijacking using various tools (Day 11)**
- **Detect session hijacking (Day 11)**

Key topics covered:

- **Session Hijacking (Day 11)**
- **Types of Session Hijacking (Day 11)**
- **Spoofing (Day 11)**
- **Application-Level Session Hijacking (Day 11)**
- **Man-in-the-Browser Attack (Day 11)**
- **Client-side Attacks (Day 11)**
- **Session Replay Attacks (Day 11)**
- **Session Fixation Attack (Day 11)**
- **CRIME Attack (Day 11)**
- **Network Level Session Hijacking (Day 11)**
- **TCP/IP Hijacking (Day 11)**
- **Session Hijacking Tools (Day 11)**
- **Session Hijacking Detection Methods (Day 11)**
- **Session Hijacking Prevention Tools (Day 11)**

Module 12: Evading IDS, Firewalls, and Honeypots — 2 Hours - 3 Topics

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

Hands-On Lab Exercises:

Over 7 hands-on exercises with real-life simulated targets to build skills on how to:

- **Bypass Windows Firewall (Day 12)**
- **Bypass firewall rules using tunneling (Day 12)**
- **Bypass antivirus (Day 12)**

Module 13: Hacking Web Servers — 2 Hours - 10 Topics

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

Hands-On Lab Exercises:

Over 8 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform web server reconnaissance using various tools (Day 13)**
- **Enumerate web server information (Day 13)**
- **Crack FTP credentials using a dictionary attack (Day 13)**

Key topics covered:

- **Web Server Operations (Day 13)**
- **Web Server Attacks (Day 13)**
- **DNS Server Hijacking (Day 13)**
- **Website Defacement (Day 13)**
- **Web Cache Poisoning Attack (Day 13)**
- **Web Server Attack Methodology (Day 13)**
- **Web Server Attack Tools (Day 13)**
- **Web Server Security Tools (Day 13)**
- **Patch Management (Day 13)**

- Patch Management Tools (Day 13)

Module 14: Hacking Web Applications — 2 Hours - 8 Topics

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

Hands-On Lab Exercises:

Over 15 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform web application reconnaissance using various tools (Day 14)
- Perform web spidering (Day 14)
- Perform web application vulnerability scanning (Day 14)
- Perform a brute-force attack (Day 14)
- Perform Cross-Site Request Forgery (CSRF) Attack (Day 14)
- Identify XSS vulnerabilities in web applications (Day 14)
- Detect web application vulnerabilities using various web application security tools (Day 14)

Key topics covered:

- Web Application Architecture (Day 14)
- Web Application Threats (Day 14)
- OWASP Top 10 Application Security Risks – 2021 (Day 14)
- Web Application Hacking Methodology (Day 14)
- Web API (Day 14)
- Webhooks and Web Shell (Day 14)
- Web API Hacking Methodology (Day 14)
- Web Application Security (Day 14)

Module 15: SQL Injection — 2 Hours - 7 Topics

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

Hands-On Lab Exercises:

Over 4 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform an SQL injection attack against MSSQL to extract databases (Day 15)
- Detect SQL injection vulnerabilities using various SQL injection detection tools (Day 15)

Key topics covered:

- SQL Injection (Day 15)
- Types of SQL injection (Day 15)
- Blind SQL Injection (Day 15)
- SQL Injection Methodology (Day 15)
- SQL Injection Tools (Day 15)
- Signature Evasion Techniques (Day 15)
- SQL Injection Detection Tools (Day 15)

Module 16: Hacking Wireless Networks — 2 Hours - 11 Topics

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

Hands-On Lab Exercises:

Over 3 hands-on exercises with real-life simulated targets to build skills on how to:

- **Foot Print a wireless network (Day 16)**
- **Perform wireless traffic analysis (Day 16)**
- **Crack WEP, WPA, and WPA2 networks (Day 16)**
- **Create a rogue access point to capture data packets (Day 16)**

Key topics covered:

- **Wireless Terminology (Day 16)**
- **Wireless Networks (Day 16)**
- **Wireless Encryption (Day 16)**
- **Wireless Threats (Day 16)**
- **Wireless Hacking Methodology (Day 16)**
- **Wi-Fi Encryption Cracking (Day 16)**
- **WEP/WPA/WPA2 Cracking Tools (Day 16)**
- **Bluetooth Hacking (Day 16)**
- **Bluetooth Threats (Day 16)**
- **Wi-Fi Security Auditing Tools (Day 16)**
- **Bluetooth Security Tools (Day 16)**

Module 17: Hacking Mobile Platforms — 2 Hours - 12 Topics

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

Hands-On Lab Exercises:

Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- **Hack an Android device by creating binary payloads (Day 17)**
- **Exploit the Android platform through ADB (Day 17)**
- **Hack an Android device by creating APK file (Day 17)**
- **Secure Android devices using various Android security tools (Day 17)**

Key topics covered:

- **Mobile Platform Attack Vectors (Day 17)**
- **OWASP Top 10 Mobile Risks (Day 17)**
- **App Sandboxing, SMS Phishing Attack (SMiShing) (Day 17)**
- **Android Rooting (Day 17)**
- **Hacking Android Devices (Day 17)**
- **Android Security Tools (Day 17)**
- **Jailbreaking iOS (Day 17)**
- **Hacking iOS Devices (Day 17)**
- **iOS Device Security Tools (Day 17)**
- **Mobile Device Management (MDM) (Day 17)**
- **OWASP Top 10 Mobile Controls (Day 17)**
- **Mobile Security Tools (Day 17)**

Module 18: IoT and OT Hacking 2 Hours - 13 Topics

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

Hands-On Lab Exercises:

Over 2 hands-on exercises with real-life simulated targets to build skills on how to:

- **Gather information using Online foot printing tools (Day 18)**
- **Capture and analyze IoT device traffic (Day 18)**

Key topics covered:

- **IoT Architecture (Day 18)**
- **IoT Communication Models (Day 18)**
- **OWASP Top 10 IoT Threats (Day 18)**
- **IoT Vulnerabilities (Day 18)**
- **IoT Hacking Methodology (Day 18)**
- **IoT Hacking Tools (Day 18)**
- **IoT Security Tools (Day 18)**
- **IT/OT Convergence (IIOT) (Day 18)**
- **ICS/SCADA, OT Vulnerabilities (Day 18)**
- **OT Attacks (Day 18)**
- **OT Hacking Methodology (Day 18)**
- **OT Hacking Tools (Day 18)**
- **OT Security Tools (Day 18)**

Module 19: Cloud Computing 2 Hours - 16 Topics

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.

Hands-On Lab Exercises:

Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- **Perform S3 Bucket enumeration using various S3 bucket enumeration tools (Day 19)**
- **Exploit open S3 buckets (Day 19)**
- **Escalate IAM user privileges by exploiting misconfigured user policy (Day 19)**

Key topics covered:

- **Cloud Computing (Day 19)**
- **Types of Cloud Computing Services (Day 19)**
- **Cloud Deployment Models (Day 19)**
- **Fog and Edge Computing (Day 19)**
- **Cloud Service Providers (Day 19)**
- **Container (Day 19)**
- **Docker (Day 19)**
- **Kubernetes (Day 19)**
- **Serverless Computing (Day 19)**
- **OWASP Top 10 Cloud Security Risks (Day 19)**
- **Container and Kubernetes Vulnerabilities (Day 19)**

- Cloud Attacks (Day 19)
- Cloud Hacking (Day 19)
- Cloud Network Security (Day 19)
- Cloud Security Controls (Day 19)
- Cloud Security Tools (Day 19)

Module 20: Cryptography **2 Hours - 10 Topics**

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

Hands-On Lab Exercises:

Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

- **Calculate MD5 hashes (Day 20)**
- **Perform file and text message encryption (Day 20)**
- **Create and use self-signed certificates (Day 20)**
- **Perform email and disk encryption (Day 20)**
- **Perform cryptanalysis using various cryptanalysis tools (Day 20)**

Key topics covered:

- **Cryptography (Day 20)**
- **Encryption Algorithms (Day 20)**
- **MD5 and MD6 Hash Calculators (Day 20)**
- **Cryptography Tools (Day 20)**
- **Public Key Infrastructure (PKI) (Day 20)**
- **Email Encryption (Day 20)**
- **Disk Encryption (Day 20)**
- **Cryptanalysis (Day 20)**
- **Cryptography Attacks (Day 20)**
- **Key Stretching (Day 20)**