



# Certified Ethical Hacker (CEH) v12

## Module 1 - Introduction To Ethical Hacking

- 1.0 Introduction to CEH v12
- 1.1 Elements of Security
- 1.2 Cyber Kill Chain
- 1.3 MITRE ATT&CK Framework
  - 1.3.1 Activity - Researching the MITRE ATTACK Framework
- 1.4 Hacking
- 1.5 Ethical Hacking
- 1.6 Information Assurance
- 1.7 Risk Management
- 1.8 Incident Management
- 1.9 Information Security Laws and Standards
- 1.10 Introduction to Ethical Hacking Review

## Module 2: Footprinting and Reconnaissance

- 2.1 Footprinting Concepts
- 2.2 OSINT Tools
  - 2.2.1 Activity - Conduct OSINT with OSR Framework
  - 2.2.2 Activity - OSINT with theHarvester
  - 2.2.3 Activity - Add API Keys to theHarvester
  - 2.2.4 Activity - Extract Document Metadata with FOCA
  - 2.2.5 Activity - Extract Document Metadata with FOCA
- 2.3 Advanced Google Search
  - 2.3.1 Activity - Google Hacking
- 2.4 Whois Footprinting
  - 2.4.1 Activity - Conducting Whois Research
- 2.5 DNS Footprinting
  - 2.5.1 Activity - Query DNS with NSLOOKUP
- 2.6 Website Footprinting
  - 2.6.1 Activity - Fingerprint a Webserver with ID Serve
  - 2.6.2 Activity - Extract Data from Websites
  - 2.6.3 Activity - Mirror a Website with HTTrack
- 2.7 Email Footprinting
  - 2.7.1 Activity - Trace a Suspicious Email
- 2.8 Network Footprinting
- 2.9 Social Network Footprinting
- 2.10 Footprinting and Reconnaissance Countermeasures
- 2.11 Footprinting and Reconnaissance Review

## Module 3: Scanning Networks

- 3.1 Scanning Concepts
- 3.2 Discovery Scans
  - 3.2.1 Activity - ICMP ECHO and ARP Pings
  - 3.2.2 Activity - Host Discovery with Angry IP Scanner
- 3.3 Port Scans
  - 3.3.1 Activity - Port Scan with Angry IP Scanner
- 3.4 Other Scan Types
- 3.5 Scanning Tools
  - 3.5.1 Activity - Hping3 Packet Crafting
  - 3.5.2 Activity - Fingerprinting with Zenmap
- 3.6 NMAP
  - 3.6.1 Activity - Nmap Basic Scans
  - 3.6.2 Activity - Host Discovery with Nmap
  - 3.6.3 - Activity - Nmap Version Detection
  - 3.6.4 Activity - Nmap Idle (Zombie) Scan
  - 3.6.5 Activity - Nmap FTP Bounce Scan
  - 3.6.6 - Activity - NMAP Scripts
- 3.7 Firewall and IDS Evasion
  - 3.7.1 Activity - Nmap Advanced Scans
- 3.8 Proxies
- 3.9 Scanning Countermeasures
- 3.10 Scanning Networks Review

## **Module 4: Enumeration**

- 4.1 Enumeration Overview
- 4.2 SMB\_NetBIOS\_Enumeration
  - 4.2.1 Activity - Enumerate NetBIOS Information with Hyena
- 4.3 File Transfer Enumeration
- 4.4 WMI Enumeration
  - 4.4.1 - Activity - Enumerating WMI with Hyena
- 4.5 SNMP Enumeration
  - 4.5.1 Activity - Enumerate WMI, SNMP and Other Information Using SoftPerfect
- 4.6 LDAP Enumeration
- 4.7 DNS Enumeration
- 4.8 SMTP Enumeration
  - 4.8.1 Activity - Enumerate Email Users with SMTP
- 4.9 Remote Connection Enumeration
- 4.10 Website Enumeration
  - 4.10.1 Activity - Enumerate a Website with DirBuster
- 4.11 Other Enumeration Types
- 4.12 Enumeration Countermeasures and Review

## **Module 5: Vulnerability Analysis**

- 5.1 Vulnerability Scanning
  - 5.1.1 Vulnerability Scanning with OpenVAS
- 5.2 Vulnerability Assessment
- 5.3 Vulnerability Analysis Review

## **Module 6: System Hacking**

- 6.1 System Hacking Concepts
- 6.2 Common OS Exploits
- 6.3 Buffer Overflows
  - 6.3.1 Activity - Performing a Buffer Overflow
- 6.4 System Hacking Tools and Frameworks
  - 6.4.1 Activity - Hack a Linux Target from Start to Finish
- 6.5 Metasploit
  - 6.5.1 Activity - Get Started with Metasploit
- 6.6 Meterpreter
- 6.7 Keylogging and Spyware
  - 6.7.1 Activity - Keylogging with Meterpreter
- 6.8 Netcat
  - 6.8.1 Activity - Using Netcat
- 6.9 Hacking Windows
  - 6.9.1 Activity - Hacking Windows with Eternal Blue
- 6.10 Hacking Linux
- 6.11 Password Attacks
  - 6.11.1 Activity - Pass the Hash
  - 6.11.2 Activity - Password Spraying
- 6.12 Password Cracking Tools
- 6.13 Windows Password Cracking
  - 6.13.1 Activity - Cracking Windows Passwords
  - 6.13.2 Activity - Cracking Password Hashes with Hashcat
- 6.14 Linux Password Cracking
- 6.15 Other Methods for Obtaining Passwords
- 6.16 Network Service Attacks
  - 6.16.1 Activity - Brute Forcing a Network Service with Medusa
- 6.17 Post Exploitation
- 6.18 Pivoting
  - 6.18.1 Activity - Pivoting Setup
- 6.19 Maintaining Access
  - 6.19.1 Activity - Persistence
- 6.20 Hiding Data
  - 6.20.1 Activity - Hiding Data Using Least Significant Bit Steganography
- 6.21 Covering Tracks
  - 6.21.1 Activity - Clearing Tracks in Windows
  - 6.21.2 Activity - View and Clear Audit Policies with Auditpol
- 6.22 System Hacking Countermeasures
- 6.23 System Hacking Review

## **Module 7: Malware Threats**

- 7.1 Malware Overview
- 7.2 Viruses
- 7.3 Trojans
  - 7.3.1 Activity - Deploying a RAT
- 7.4 Rootkits
- 7.5 Other Malware

- 7.6 Advanced Persistent Threat
- 7.7 Malware Makers
  - 7.7.1 Activity - Creating a Malware Dropper and Handler
- 7.8 Malware Detection
- 7.9 Malware Analysis
  - 7.9.1 Activity - Performing a Static Code Review
  - 7.9.2 Activity - Analyzing the SolarWinds Orion Hack
- 7.10 Malware Countermeasures
- 7.11 Malware Threats Review

## **Module 8: Sniffing**

- 8.1 Network Sniffing
- 8.2 Sniffing Tools
  - 8.2.1 Activity- Sniffing HTTP with Wireshark
  - 8.2.2 Activity - Capturing Files from SMB
- 8.3 ARP and MAC Attacks
  - 8.3.1 Activity - Performing an MITM Attack with Ettercap
- 8.4 Name Resolution Attacks
  - 8.4.1 Activity - Spoofing Responses with Responder
- 8.5 Other Layer 2 Attacks
- 8.6 Sniffing Countermeasures
- 8.7 Sniffing Review

## **Module 9: Social Engineering**

- 9.1 Social Engineering Concepts
- 9.2 Social Engineering Techniques
  - 9.2.1 Activity - Deploying a Baited USB Stick
  - 9.2.2 Activity - Using an O.MG Lightning Cable
- 9.3 Social Engineering Tools
  - 9.3.1 Activity - Phishing for Credentials
- 9.4 Social Media, Identity Theft, Insider Threats
- 9.5 Social Engineering Countermeasures
- 9.6 Social Engineering Review

## **Module 10: Denial-of-Service**

- 10.1 DoS-DDoS Concepts
- 10.2 Volumetric Attacks
- 10.3 Fragmentation Attacks
- 10.4 State Exhaustion Attacks
- 10.5 Application Layer Attacks
  - 10.5.1 Activity - Performing a LOIC Attack
  - 10.5.2 Activity - Performing a HOIC Attack
  - 10.5.3 Activity - Conducting a Slowloris Attack
- 10.6 Other Attacks
- 10.7 DoS Tools
- 10.8 DoS Countermeasures

10.9 DoS Review

## **Module 11: Session Hijacking**

- 11.1 Session Hijacking
- 11.2 Compromising a Session Token
- 11.3 XSS
- 11.4 CSRF
- 11.5 Other Web Hijacking Attacks
- 11.6 Network-Level Session Hijacking
  - 11.6.1 Activity - Hijack a Telnet Session
- 11.7 Session Hijacking Tools
- 11.8 Session Hijacking Countermeasures
- 11.9 Session Hijacking Review

## **Module 12: Evading IDS, Firewalls, and Honeypots**

- 12.1 Types of IDS
- 12.2 Snort
- 12.3 System Logs
- 12.4 IDS Considerations
- 12.5 IDS Evasion
  - 12.5.1 Activity - Fly Below IDS Radar
- 12.6 Firewalls
- 12.7 Packet Filtering Rules
- 12.8 Firewall Deployments
- 12.9 Split DNS
- 12.10 Firewall Product Types
- 12.11 Firewall Evasion
  - 12.11.1 Activity - Use Social Engineering to Bypass a Windows Firewall
  - 12.11.2 Activity - Busting the DOM for WAF Evasion
- 12.12 Honeypots
- 12.13 Honeypot Detection and Evasion
  - 12.13.1 Activity - Test and Analyze a Honey Pot
- 12.14 Evading IDS, Firewalls, and Honeypots Review

## **Module 13: Hacking Web Servers**

- 13.1 Web Server Operations
- 13.2 Hacking Web Servers
- 13.3 Common Web Server Attacks
  - 13.3.1 Activity - Defacing a Website
- 13.4 Web Server Attack Tools
- 13.5 Hacking Web Servers Countermeasures
- 13.6 Hacking Web Servers Review

## **Module 14: Hacking Web Applications**

- 14.1 Web Application Concepts

- 14.2 Attacking Web Apps
- 14.3 A01 Broken Access Control
- 14.4 A02 Cryptographic Failures
- 14.5 A03 Injection
  - 14.5.1 Activity - Command Injection
- 14.6 A04 Insecure Design
- 14.7 A05 Security Misconfiguration
- 14.8 A06 Vulnerable and Outdated Components
- 14.9 A07 Identification and Authentication Failures
- 14.10 A08 Software and Data integrity Failures
- 14.11 A09 Security Logging and Monitoring Failures
- 14.12 A10 Server-Side Request Forgery
- 14.13 XSS Attacks
  - 14.13.1 Activity - XSS Walkthrough
  - 14.13.2 Activity - Inject a Malicious iFrame with XSS
- 14.14 CSRF
- 14.15 Parameter Tampering
  - 14.15.1 Activity - Parameter Tampering with Burp
- 14.16 Clickjacking
- 14.17 SQL Injection
- 14.18 Insecure Deserialization Attacks
- 14.19 IDOR
  - 14.19.1 Activity - Hacking with IDOR
- 14.20 Directory Traversal
- 14.21 Session Management Attacks
- 14.22 Response Splitting
- 14.23 Overflow Attacks
- 14.24 XXE Attacks
- 14.25 Web App DoS
- 14.26 Soap Attacks
- 14.27 AJAX Attacks
- 14.28 Web API Hacking
- 14.29 Webhooks and Web Shells
- 14.30 Web App Hacking Tools
- 14.31 Hacking Web Applications Countermeasures
- 14.32 Hacking Web Applications Review

## **Module 15: SQL Injection**

- 15.1 SQL Injection Overview
- 15.2 Basic SQL Injection
- 15.3 Finding Vulnerable Websites
- 15.4 Error-based SQL Injection
- 15.5 Union SQL Injection
  - 15.5.1 Activity - Testing SQLi on a Live Website - Part 1
  - 15.5.2 Activity - Testing SQLi on a Live Website - Part 2
- 15.6 Blind SQL Injection
- 15.7 SQL Injection Tools
  - 15.7.1 Activity - SQL Injection Using SQLmap
- 15.8 Evading Detection

- 15.9 Analyzing SQL Injection
- 15.10 SQL Injection Countermeasures
- 15.11 SQL Injection Review

## **Module 16: Hacking Wireless Networks**

- 16.1 Wireless Concepts
- 16.2 Wireless Security Standards
- 16.3 WI-FI Discovery Tools
- 16.4 Common Wi-Fi Attacks
- 16.5 Wi-Fi Password Cracking
- 16.6 WEP Cracking
  - 16.6.1 Activity - Cracking WEP
- 16.7 WPA,WPA2,WPA3 Cracking
  - 16.7.1 Activity - WPA KRACK Attack
- 16.8 WPS Cracking
- 16.9 Bluetooth Hacking
- 16.10 Other Wireless Hacking
  - 16.10.1 Activity - Cloning an RFID badge
  - 16.10.2 Activity - Hacking with a Flipper Zero
- 16.11 Wireless Security Tools
- 16.12 Wireless Hacking Countermeasures
- 16.13 Hacking Wireless Networks Review

## **Module 17: Hacking Mobile Platforms**

- 17.1 Mobile Device Overview
- 17.2 Mobile Device Attacks
- 17.3 Android Vulnerabilities
- 17.4 Rooting Android
- 17.5 Android Exploits
  - 17.5.1 Activity - Hacking Android
  - 17.5.2 Activity - Using a Mobile Device in a DDoS Campaign
- 17.6 Android-based Hacking Tools
- 17.7 Reverse Engineering an Android App
- 17.8 Securing Android
- 17.9 iOS Overview
- 17.10 Jailbreaking iOS
- 17.11 iOS Exploits
- 17.12 iOS-based Hacking Tools
- 17.13 Reverse Engineering an iOS App
- 17.14 Securing iOS
- 17.15 Mobile Device Management
- 17.16 Hacking Mobile Platforms Countermeasures
- 17.17 Hacking Mobile Platforms Review

## **Module 18: IoT AND OT Hacking**

- 18.1 IoT Overview

- 18.2 IoT Infrastructure
- 18.3 IoT Vulnerabilities and Threats
  - 18.3.1 Activity - Searching for Vulnerable IoT Devices
- 18.4 IoT Hacking Methodology and Tools
- 18.5 IoT Hacking Countermeasures
- 18.6 OT Concepts
- 18.7 IT-OT Convergence
- 18.8 OT Components
- 18.9 OT Vulnerabilities
- 18.10 OT Attack Methodology and Tools
- 18.11 OT Hacking Countermeasures
- 18.12 IoT and OT Hacking Review

## **Module 19: Cloud Computing**

- 19.1 Cloud Computing Concepts
- 19.2 Cloud Types
- 19.3 Cloud Benefits and Considerations
- 19.4 Cloud Risks and Vulnerabilities
- 19.5 Cloud Threats and Countermeasures
  - 19.5.1 Activity - Hacking S3 Buckets
- 19.6 Cloud Security Tools And Best Practices
- 19.7 Cloud Computing Review

## **Module 20: Cryptography**

- 20.1 Cryptography Concepts
- 20.2 Symmetric Encryption
  - 20.2.1 Activity - Symmetric Encryption
- 20.3 Asymmetric Encryption
  - 20.3.1 Activity - Asymmetric Encryption
- 20.4 Public Key Exchange
- 20.5 PKI
  - 20.5.1 Activity - Generating and Using an Asymmetric Key Pair
- 20.6 Digital Signatures
- 20.7 Hashing
  - 20.7.1 Activity - Calculating Hashes
- 20.8 Common Cryptography Use Cases
- 20.9 Cryptography Tools
- 20.10 Cryptography Attacks
- 20.11 Cryptography Review
- 20.12 Course Conclusion