EC-Council CEH: Certified Ethical Hacker v12

Content

Here's the formatted version of the course outline you provided, keeping all the details intact:

Course Outline

1. Introduction to Ethical Hacking

- Information Security Overview
- Hacking Methodologies and Frameworks
- Hacking Concepts
- Ethical Hacking Concepts
- Information Security Controls
- Information Security Laws and Standards

2. Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures

3. Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Host Discovery
- Port and Service Discovery
- OS Discovery (Banner Grabbing/OS Fingerprinting)
- Scanning Beyond IDS and Firewall
- Network Scanning Countermeasures

4. Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration

- NTP and NFS Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques
- Enumeration Countermeasures

5. Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment Types
- Vulnerability Assessment Tools
- Vulnerability Assessment Reports

6. System Hacking

- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

7. Malware Threats

- Malware Concepts
- APT Concepts
- Trojan Concepts
- Worm Makers
- Fileless Malware Concepts
- Malware Analysis
- Malware Countermeasures
- Anti-Malware Software

8. Sniffing

- Sniffing Concepts
- Sniffing Technique: MAC Attacks
- Sniffing Technique: DHCP Attacks
- Sniffing Technique: ARP Poisoning
- Sniffing Technique: Spoofing Attacks
- Sniffing Technique: DNS Poisoning
- Sniffing Tools

9. Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures

10. Denial-of-Service

- DoS/DDoS Concepts
- Botnets
- DoS/DDoS Attack Techniques
- DDoS Case Study
- DoS/DDoS Attack Countermeasures

11. Session Hijacking

- Session Hijacking Concepts
- Application-Level Session Hijacking
- Network-Level Session Hijacking
- Session Hijacking Tools
- Session Hijacking Countermeasures

12. Evading IDS, Firewalls, and Honeypots

- IDS, IPS, Firewall, and Honeypot Concepts
- IDS, IPS, Firewall, and Honeypot Solutions
- Evading IDS
- Evading Firewalls
- Evading NAC and Endpoint Security
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures

13. Hacking Web Servers

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Countermeasures

14. Hacking Web Applications

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web API, Webhooks, and Web Shell
- Web Application Security

15. SQL Injection

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- SQL Injection Countermeasures

16. Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Wireless Attack Countermeasures
- Wireless Security Tools

17. Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Management
- Mobile Security Guidelines and Tools

18. IoT and OT Hacking

- IoT Hacking
- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- OT Hacking
- OT Concepts
- OT Attacks
- OT Hacking Methodology

19. Cloud Computing

- Cloud Computing Concepts
- Container Technology
- Manipulating CloudTrial Service
- Cloud Security

20. Cryptography

- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Cryptography Attack Countermeasures