

CEH Exam Topics

1. Introduction to Ethical Hacking

- Information security fundamentals
- Cyber kill chain, MITRE ATT&CK framework
- Hacker types, attack vectors

2. Footprinting and Reconnaissance

- Footprinting concepts
- Passive vs active reconnaissance
- Tools for gathering information

3. Scanning Networks

- Network scanning techniques
- Port scanning, vulnerability scanning

- Tools (Nmap, Nessus, etc.)

4. Enumeration

- NetBIOS, SNMP, LDAP, DNS enumeration
- Tools and countermeasures

5. Vulnerability Analysis

- Vulnerability assessment concepts
- Tools for vulnerability scanning
- Interpreting reports

6. System Hacking

- Password cracking techniques
- Privilege escalation
- Maintaining access (backdoors, rootkits)

7. Malware Threats

- Viruses, worms, Trojans
- Fileless malware
- Countermeasures

8. Sniffing

- Packet sniffing concepts
- ARP poisoning, MAC flooding
- Detection and defenses

9. Social Engineering

- Human-based, computer-based, mobile-based
- Social engineering techniques & defenses

- 10. Denial-of-Service (DoS) and DDoS Attacks
- DoS/DDoS concepts
- Botnets
- Tools & countermeasures

11. Session Hijacking

- Session hijacking techniques (TCP, web)
- Countermeasures

12. Evading IDS, Firewalls, and Honeypots

- Techniques for evasion
- IDS/IPS/firewall detection evasion
- Honeypot evasion

13. Hacking Web Servers

- Web server attacks
- IIS/Apache vulnerabilities
- Hardening and countermeasures

14. Hacking Web Applications

- Web app threats (XSS, CSRF, etc.)
- Tools (Burp Suite, OWASP ZAP)

15. SQL Injection

- SQL injection types (in-band, blind, out-of-band)
- Detection and prevention

16. Hacking Wireless Networks

- Wireless encryption standards

- WPA/WPA2 cracking techniques
- Tools (Aircrack-ng, Kismet)

17. Hacking Mobile Platforms

- Mobile OS vulnerabilities (Android, iOS)
- Mobile device management (MDM) attacks

18. IoT and OT Hacking

- IoT ecosystem vulnerabilities
- SCADA/ICS attacks

19. Cloud Computing

- Cloud environment threats
- Cloud security tools and policies

20. Cryptography

- Encryption algorithms (symmetric, asymmetric)
- Hashing, PKI, SSL/TLS
- Cryptanalysis attacks