CEH Exam Blueprint v5.0

EC-Council

Domain	Sub Domain	Description	Number of Questions	Weightage (%)
1. Information Security and Ethical Hacking Overview	Introduction to Ethical Hacking	▪ Information Security Overview ▪ Hacking Methodologies and Frameworks ▪ Hacking Concepts ▪ Ethical Hacking Concepts ▪ Information Security Controls ▪ Information Security Laws and Standards	**7**	**6%**
2. Reconnaissance Techniques	Footprinting and Reconnaissance	▪ Footprinting Concepts ▪ Footprinting Methodology ▪ 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	**7**	**17%**
	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	**7**	
	Enumeration	▪ Enumeration Concepts ▪ NetBIOS Enumeration ▪ SNMP Enumeration ▪ LDAP Enumeration ▪ NTP and NFS Enumeration ▪ SMTP and DNS Enumeration ▪ Other Enumeration Techniques (IPsec, VoIP, RPC, Unix/Linux, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration) ▪ Enumeration Countermeasures	**7**	
3. System Hacking Phases and Attack Techniques	Vulnerability Analysis	▪ Vulnerability Assessment Concepts ▪ Vulnerability Classification and Assessment Types ▪ Vulnerability Assessment Tools ▪ Vulnerability Assessment Reports	**6**	**15%**

	System Hacking	▪ System Hacking Concepts ▪ Gaining Access ▪ Password Cracking ▪ Vulnerability Exploitation ▪ Escalating Privileges ▪ Maintaining Access ▪ Executing Applications ▪ Hiding Files ▪ Establishing Persistence ▪ Clearing Logs	**6**	
	Malware Threats	▪ Malware Concepts ▪ APT Concepts ▪ Trojan Concepts ▪ Virus and Worm Concepts ▪ Fileless Malware Concepts ▪ Malware Analysis ▪ Malware Countermeasures ▪ Anti-Malware Software	**7**	
4. Network and Perimeter Hacking	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 ▪ Sniffing Countermeasures ▪ Sniffing Detection Techniques	**6**	**24%**
	Social Engineering	▪ Social Engineering Concepts ▪ Social Engineering Techniques ▪ Insider Threats ▪ Impersonation on Social Networking Sites ▪ Identity Theft ▪ Social Engineering Countermeasures	**6**	
	Denial-of-Service	▪ DoS/DDoS Concepts ▪ Botnets ▪ DoS/DDoS Attack Techniques ▪ DDoS Case Study ▪ DoS/DDoS Attack Countermeasures ▪ DoS/DDoS Protection Tools	**6**	
	Session Hijacking	▪ Session Hijacking Concepts ▪ Application-Level Session Hijacking ▪ Network-Level Session Hijacking ▪ Session Hijacking Tools ▪ Session Hijacking Countermeasures	**6**	

	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	**6**	
5. Web Application Hacking	Hacking Web Servers	▪ Web Server Concepts ▪ Web Server Attacks ▪ Web Server Attack Methodology ▪ Web Server Attack Countermeasures ▪ Patch Management	**6**	**14%**
	Hacking Web Applications	▪ Web App Concepts ▪ Web App Threats ▪ Web App Hacking Methodology ▪ Footprint Web Infrastructure ▪ Analyze Web Applications ▪ Bypass Client-Side Controls ▪ Attack Authentication Mechanism ▪ Attack Authorization Schemes ▪ Attack Access Controls ▪ Attack Session Management Mechanism ▪ Perform Injection/Input Validation Attacks ▪ Attack Application Logic Flaws ▪ Attack Shared Environments ▪ Attack Database Connectivity ▪ Attack Web App Client ▪ Attack Web Services ▪ Web API, Webhooks, and Web Shell ▪ Web App Security	**6**	
	SQL Injection	▪ SQL Injection Concepts ▪ Types of SQL Injection ▪ SQL Injection Methodology ▪ SQL Injection Tools ▪ Evasion Techniques ▪ SQL Injection Countermeasures	**6**	
6. Wireless Network Hacking	Hacking Wireless Networks	▪ Wireless Concepts ▪ Wireless Encryption ▪ Wireless Threats ▪ Wireless Hacking Methodology ▪ Wireless Hacking Tools ▪ Bluetooth Hacking ▪ Wireless Attack Countermeasures ▪ Wireless Security Tools	**6**	**5%**
7. Mobile Platform, IoT, and OT Hacking	Hacking Mobile Platforms	▪ Mobile Platform Attack Vectors ▪ Hacking Android OS ▪ Hacking iOS ▪ Mobile Device Management ▪ Mobile Security Guidelines and Tools	**6**	**10%**

	IoT and OT Hacking	▪ IoT Concepts ▪ IoT Attacks ▪ IoT Hacking Methodology ▪ IoT Attack Countermeasures ▪ OT Concepts ▪ OT Attacks ▪ OT Hacking Methodology ▪ OT Attack Countermeasures	**6**	
8. Cloud Computing	Cloud Computing	▪ Cloud Computing Concepts ▪ Container Technology ▪ Serverless Computing ▪ Cloud Computing Threats ▪ Cloud Hacking ▪ Cloud Security	**6**	**5%**
9. Cryptography	Cryptography	▪ Cryptography Concepts ▪ Encryption Algorithms ▪ Cryptography Tools ▪ Public Key Infrastructure (PKI) ▪ Email Encryption ▪ Disk Encryption ▪ Cryptanalysis ▪ Cryptography Attack Countermeasures	**6**	**5%**