CEH Exam Blueprint v4.0

EC-Council

Domain	Sub Domain	Description	Number of Questions	Weightage (%)
1. Information Security and Ethical Hacking Overview	Introduction to Ethical Hacking	• Information Security Overview • Cyber Kill Chain Concepts • Hacking Concepts • Ethical Hacking Concepts • Information Security Controls • Information Security Laws and Standards	8	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	10	21%
	Scanning Networks	• Network Scanning Concepts • Scanning Tools • Host Discovery • Port and Service Discovery • OS Discovery (Banner Grabbing/OS Fingerprinting) • Scanning Beyond IDS and Firewall • Draw Network Diagrams	10	
	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	6	
3. System Hacking Phases and Attack Techniques	Vulnerability Analysis	• Vulnerability Assessment Concepts • Vulnerability Classification and Assessment Types • Vulnerability Assessment Solutions and Tools • Vulnerability Assessment Reports	9	17%

	System Hacking	• System Hacking Concepts • Gaining Access • Cracking Passwords • Vulnerability Exploitation • Escalating Privileges • Maintaining Access • Executing Applications • Hiding Files • Clearing Logs	6	
	Malware Threats	• Malware Concepts • APT Concepts • Trojan Concepts • Virus and Worm Concepts • File-less Malware Concepts • Malware Analysis • Malware Countermeasures • Anti-Malware Software	6	
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	3	14%
	Social Engineering	• Social Engineering Concepts • Social Engineering Techniques • Insider Threats • Impersonation on Social • Networking Sites • Identity Theft • Social Engineering Countermeasures	5	
	Denial-of-Service	• DoS/DDoS Concepts • DoS/DDoS Attack Techniques • Botnets • DDoS • Case Study • DoS/DDoS Attack Tools • DoS/DDoS Countermeasures • DoS/DDoS Protection Tools	2	
	Session Hijacking	• Session Hijacking Concepts • Application Level Session Hijacking • Network Level Session Hijacking • Session Hijacking Tools • Session Hijacking Countermeasures	3	

	Evading IDS, Firewalls, and Honeypots	• IDS, IPS, Firewall, and Honeypot Concepts • IDS, IPS, Firewall, and Honeypot Solutions • Evading IDS • Evading Firewalls • IDS/Firewall Evading Tools • Detecting Honeypots • IDS/Firewall Evasion Countermeasures	5	
5. Web Application Hacking	Hacking Web Servers	• Web Server Concepts • Web Server Attacks • Web Server Attack Methodology • Web Server Attack Tools • Web Server Countermeasures • Patch Management • Web Server Security Tools	8	16%
	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 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	8	
	SQL Injection	• SQL Injection Concepts • Types of SQL Injection • SQL Injection Methodology • SQL Injection Tools • Evasion Techniques • SQL Injection Countermeasures	4	
6. Wireless Network Hacking	Hacking Wireless Networks	• Wireless Concepts • Wireless Encryption • Wireless Threats • Wireless Hacking Methodology • Wireless Hacking Tools • Bluetooth Hacking • Wireless Countermeasures • Wireless Security Tools	8	6%
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	4	8%

	IoT and OT Hacking	• IoT Concepts • IoT Attacks • IoT Hacking Methodology • IoT Hacking Tools • IoT Countermeasures • OT Concepts • OT Attacks • OT Hacking Methodology • OT Hacking Tools • OT Countermeasures	6	
8. Cloud Computing	Cloud Computing	• Cloud Computing Concepts • Container Technology • Serverless Computing • Cloud Computing Threats • Cloud Hacking • Cloud Security	7	6%
9. Cryptography	Cryptography	• Cryptography Concepts • Encryption Algorithms • Cryptography Tools • Public Key Infrastructure (PKI) • Email Encryption • Disk Encryption • Cryptanalysis • Countermeasures	7	6%