



EC-Council

**Certified Ethical Hacker (CEH) - Practical
Exam Blueprint v1**

Domain	Sub Domain	Description	Weightage(%)
1. Information Security and Ethical Hacking Overview	Introduction to EthicalHacking	<ul style="list-style-type: none">▪ Information Security Overview▪ Cyber Kill Chain Concepts▪ Hacking Concepts▪ Ethical Hacking Concepts▪ Information Security Controls▪ Information Security Laws and Standards	6%
2. Reconnaissance Techniques	Footprinting and Reconnaissance	<ul style="list-style-type: none">▪ 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	21%
	Scanning Networks	<ul style="list-style-type: none">▪ 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	

	Enumeration	<ul style="list-style-type: none"> ▪ 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 BGPenumeration) ▪ Enumeration Countermeasures 	
3. System Hacking Phases and Attack Techniques	Vulnerability Analysis	<ul style="list-style-type: none"> ▪ Vulnerability Assessment Concepts ▪ Vulnerability Classification and AssessmentTypes ▪ Vulnerability Assessment Solutions and Tools ▪ Vulnerability Assessment Reports 	17%
	System Hacking	<ul style="list-style-type: none"> ▪ System Hacking Concepts ▪ Gaining Access ▪ Cracking Passwords ▪ Vulnerability Exploitation ▪ Escalating Privileges ▪ Maintaining Access ▪ Executing Applications ▪ Hiding Files ▪ Clearing Logs 	
	Malware Threats	<ul style="list-style-type: none"> ▪ Malware Concepts ▪ APT Concepts ▪ Trojan Concepts ▪ Virus and Worm Concepts ▪ File-less Malware Concepts ▪ Malware Analysis ▪ Malware Countermeasures ▪ Anti-Malware Software 	

4. Network and Perimeter Hacking	Sniffing	<ul style="list-style-type: none"> ▪ 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 	14%
	Social Engineering	<ul style="list-style-type: none"> ▪ Social Engineering Concepts ▪ Social Engineering Techniques ▪ Insider Threats ▪ Impersonation on Social ▪ Networking Sites ▪ Identity Theft ▪ Social Engineering Countermeasures 	
	Denial-of-Service	<ul style="list-style-type: none"> ▪ DoS/DDoS Concepts ▪ DoS/DDoS Attack Techniques ▪ Botnets ▪ DDoS ▪ Case Study ▪ DoS/DDoS Attack Tools ▪ DoS/DDoS Countermeasures ▪ DoS/DDoS Protection Tools 	
	Session Hijacking	<ul style="list-style-type: none"> ▪ Session Hijacking Concepts ▪ Application-Level Session Hijacking ▪ Network Level Session Hijacking ▪ Session Hijacking Tools ▪ Session Hijacking Countermeasures 	

	Evading IDS, Firewalls, and Honeypots	<ul style="list-style-type: none"> ▪ 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. Web Application Hacking	Hacking Web Servers	<ul style="list-style-type: none"> ▪ Web Server Concepts ▪ Web Server Attacks ▪ Web Server Attack Methodology ▪ Web Server Attack Tools ▪ Web Server Countermeasures ▪ Patch Management ▪ Web Server Security Tools 	16%
	Hacking Web Applications	<ul style="list-style-type: none"> ▪ 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 	

		<ul style="list-style-type: none"> ▪ Web API, Webhooks and Web Shell ▪ Web App Security 	
	SQL Injection	<ul style="list-style-type: none"> ▪ SQL Injection Concepts ▪ Types of SQL Injection ▪ SQL Injection Methodology ▪ SQL Injection Tools ▪ Evasion Techniques ▪ SQL Injection Countermeasures 	
6. Wireless Network Hacking	Hacking Wireless Networks	<ul style="list-style-type: none"> ▪ Wireless Concepts ▪ Wireless Encryption ▪ Wireless Threats ▪ Wireless Hacking Methodology ▪ Wireless Hacking Tools ▪ Bluetooth Hacking ▪ Wireless Countermeasures ▪ Wireless Security Tools 	6%
7. Mobile Platform, IoT, and OT Hacking	Hacking Mobile Platforms	<ul style="list-style-type: none"> ▪ Mobile Platform Attack Vectors ▪ Hacking Android OS ▪ Hacking iOS ▪ Mobile Device Management ▪ Mobile Security Guidelines and Tools 	8%
	IoT and OT Hacking	<ul style="list-style-type: none"> ▪ IoT Concepts ▪ IoT Attacks ▪ IoT Hacking Methodology ▪ IoT Hacking Tools ▪ IoT Countermeasures ▪ OT Concepts ▪ OT Attacks ▪ OT Hacking Methodology ▪ OT Hacking Tools ▪ OT Countermeasures 	
8. Cloud Computing	Cloud Computing	<ul style="list-style-type: none"> ▪ Cloud Computing Concepts ▪ Container Technology ▪ Serverless Computing 	6%

		<ul style="list-style-type: none">▪ Cloud Computing Threats▪ Cloud Hacking▪ Cloud Security	
9. Cryptography	Cryptography	<ul style="list-style-type: none">▪ Cryptography Concepts▪ Encryption Algorithms▪ Cryptography Tools▪ Public Key Infrastructure (PKI)▪ Email Encryption▪ Disk Encryption▪ Cryptanalysis▪ Countermeasures	6%