Exam Blueprint V4.0

14 December 2023 10:11

Exam Title	Certified Ethical Hacker
Exam Code	312-50 (ECC Exam Portal) / 312-50 (VUE)
No. of Questions	125
Duration	4 Hours
Availability	ECC Exam Portal / VUE
Passing score	69 - 84 %

Domain	No. of Questions (125)	Weightage	Covered in Matt Walker 5th Edition	Ric Messier CH V12
1. Information Security and Ethical Hacking Overview	8	6%	Yes - Ethical hacking fundamentals	Yes - Ch 1 n 2
2. Reconnaissance Techniques	**26**	**21%**	**Yes - Reconnaissance and footprinting**	**Yes - CH 4**
3. System Hacking Phases and Attack Techniques	**21**	**17%**	**May be not**	**Yes - CH 7**
4. Network and Perimeter Hacking	**18**	**14%**	**Yes - Sniffing and evasion ?**	**May be CH 2 n 5**
5. Web Application Hacking	**20**	**16%**	**Yes - Hacking web servers and applications**	**May be CH 12**
6. Wireless Network Hacking	8	6%	Yes - Wireless network hacking	Yes CH 11
7. Mobile Platform, IoT, and OT Hacking	**10**	**8%**	Yes - Mobile, IoT, and OT	NA
8.Cloud Computing	7	6%	Partial - Security in cloud computing	Yes CH 15
9. Cryptography	7	6%	Yes - Cryptography	Yes CH 13

- Passing Criteria is 70% i.e. 88 out of 125 questions
- 5 highlighted sections comprise of 95/125, i.e. 76% - which is more than passing criteria

Domain	Sub Domain	Description	No. of Questions	Covered in Matt Walker 5th Edition
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	Yes - Ethical hacking fundamentals
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 / 26	Yes - Reconnaissance and footprinting
	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 / 26	Yes - Scanning and enumeration
	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 / 26	Yes - Scanning and enumeration
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	9/21	May be not
	System Hacking	System Hacking Concepts • Gaining Access • Cracking Passwords • Vulnerability Exploitation • Escalating Privileges • Maintaining Access • Executing Applications • Hiding Files • Clearing Logs	6/21	Yes - Attacking a system ?

	Malware Threats	Malware Concepts • APT Concepts • Trojan Concepts • Virus and Worm Concepts • File-less Malware Concepts • Malware Analysis • Malware Countermeasures • Anti-Malware Software	6/21	Yes - Trojans and other attacks, including malware analysis ?
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	3/18	Yes - Sniffing and evasion ?
	Social Engineering	Social Engineering Concepts • Social Engineering Techniques • Insider Threats • Impersonation on Social • Networking Sites • Identity Theft • Social Engineering Countermeasures	5/18	Yes - Social engineering and physical security
	Denial-of-Service (DoS)	DoS/DDoS Concepts • DoS/DDoS Attack Techniques • Botnets • DDoS • Case Study • DoS/DDoS Attack Tools • DoS/DDoS Countermeasures • DoS/DDoS Protection Tools	2/18	No
	Session Hijacking	Session Hijacking Concepts • Application Level Session Hijacking • Network Level Session Hijacking • Session Hijacking Tools • Session Hijacking Countermeasures	3/18	Maybe - Hacking web servers and applications ?
	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	5/18	Not sure - may be Sniffing and evasion ?
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	8/20	Yes - Hacking web servers and applications
	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	8/20	Yes - Hacking web servers and applications
	SQL Injection	SQL Injection Concepts • Types of SQL Injection • SQL Injection Methodology • SQL Injection Tools • Evasion Techniques • SQL Injection Countermeasures	4/20	No
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	Yes - Wireless network hacking
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	4/10	Yes - Mobile, IoT, and OT
	IoT and OT Hacking	IoT Concepts • IoT Attacks	6/10	Yes - Mobile, IoT, and OT

		• 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	Cloud Computing Concepts • Container Technology • Serverless Computing • Cloud Computing Threats • Cloud Hacking • Cloud Security	7	Partial - Security in cloud computing
9. Cryptography	Cryptography	Cryptography Concepts • Encryption Algorithms • Cryptography Tools • Public Key Infrastructure (PKI) • Email Encryption • Disk Encryption • Cryptanalysis • Countermeasures	7	Yes - Cryptography