EC-COUNCIL 312-50

EC-Council CEH Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

312-50

EC-Council Certified Ethical Hacker (CEH)

125 Questions Exam – 70% Cut Score – Duration of 240 minutes

Table of Contents:

Discover More about the 312-50 Certification

Are you interested in passing the EC-Council 312-50 exam? First discover, who benefits from the 312-50 certification. The 312-50 is suitable for a candidate if he wants to learn about Cyber Security. Passing the 312-50 exam earns you the EC-Council Certified Ethical Hacker (CEH) title.

While preparing for the 312-50 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The 312-50 PDF contains some of the most valuable preparation tips and the details and instant access to useful **312-50 study materials just at one click**.

EC-Council 312-50 CEH Certification Details:

Exam Name	EC-Council Certified Ethical Hacker (CEH)
Exam Code	312-50
Exam Price	$950 (USD)
Duration	240 mins
Number of Questions	125
Passing Score	70%
Books / Training	**Courseware**
Schedule Exam	**Pearson VUE**
Sample Questions	**EC-Council CEH Sample Questions**
Practice Exam	**EC-Council 312-50 Certification Practice Exam**

312-50 Syllabus:

Topic	**Details**
Information Security and Ethical Hacking Overview - 6%	
Introduction to Ethical Hacking	- Information Security Overview - Cyber Kill Chain Concepts - Hacking Concepts - Ethical Hacking Concepts

Topic	Details
	- Information Security Controls - Information Security Laws and Standards
Reconnaissance Techniques - 21%	
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
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
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

Topic	**Details**
System Hacking Phases and Attack Techniques - 17%	
Vulnerability Analysis	- Vulnerability Assessment Concepts - Vulnerability Classification and Assessment Types - Vulnerability Assessment Solutions and Tools - Vulnerability Assessment Reports
System Hacking	- System Hacking Concepts - Gaining Access - Cracking Passwords - Vulnerability Exploitation - Escalating Privileges - Maintaining Access - Executing Applications - Hiding Files - Clearing Logs
Malware Threats	- Malware Concepts - APT Concepts - Trojan Concepts - Virus and Worm Concepts - File-less Malware Concepts - Malware Analysis - Malware Countermeasures - Anti-Malware Software
Network and Perimeter Hacking - 14%	
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

Topic	Details
Social Engineering	- Social Engineering Concepts - Social Engineering Techniques - Insider Threats - Impersonation on Social - Networking Sites - Identity Theft - Social Engineering Countermeasures
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
Session Hijacking	- Session Hijacking Concepts - Application Level Session Hijacking - Network Level Session Hijacking - Session Hijacking Tools - Session Hijacking Countermeasures
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
Web Application Hacking - 16%	
Hacking Web Servers	- Web Server Concepts - Web Server Attacks - Web Server Attack Methodology - Web Server Attack Tools - Web Server Countermeasures

Topic	Details
	- Patch Management - Web Server Security Tools
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
SQL Injection	- SQL Injection Concepts - Types of SQL Injection - SQL Injection Methodology - SQL Injection Tools - Evasion Techniques - SQL Injection Countermeasures
Wireless Network Hacking - 6%	
Hacking Wireless Networks	- Wireless Concepts - Wireless Encryption - Wireless Threats - Wireless Hacking Methodology - Wireless Hacking Tools - Bluetooth Hacking

Topic	Details
	- Wireless Countermeasures - Wireless Security Tools
Mobile Platform, IoT, and OT Hacking - 8%	
Hacking Mobile Platforms	- Mobile Platform Attack Vectors - Hacking Android OS - Hacking iOS - Mobile Device Management - Mobile Security Guidelines and Tools
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
Cloud Computing - 6%	
Cloud Computing	- Cloud Computing Concepts - Container Technology - Serverless Computing - Cloud Computing Threats - Cloud Hacking - Cloud Security
Cryptography - 6%	
Cryptography	- Cryptography Concepts - Encryption Algorithms - Cryptography Tools - Public Key Infrastructure (PKI) - Email Encryption - Disk Encryption

Topic	Details
	- Cryptanalysis - Countermeasures

Broaden Your Knowledge with EC-Council 312-50 Sample Questions:

Question: 1

The DNS server where records for a domain belonging to an organization or enterprise reside is called the ____________ server.

a) Authoritative
b) Recursive
c) Caching
d) Local

Answer: a

Question: 2

If you wanted a lightweight protocol to send real-time data over, which of these would you use?

a) TCP
b) HTTP
c) ICMP
d) UDP

Answer: d

Question: 3

You've installed multiple files and processes on the compromised system. What should you also look at installing?

a) Registry keys
b) Alternate data streams
c) Root login
d) Rootkit

Answer: d

Question: 4

Which of these devices would not be considered part of the Internet of Things?

a) Smartphone
b) Thermostat
c) Light bulb
d) Set-top cable box

Answer: a

Question: 5

You see the following text written down—port:502. What does that likely reference?

a) Shodan search
b) I/O search
c) p0f results
d) RIR query

Answer: a

Question: 6

What piece of software could you use to recover from a ransomware attack?

a) Decryptor
b) Encryptor
c) Anti-malware
d) Endpoint detection and response

Answer: a

Question: 7

How would you ensure that confidentiality is implemented in an organization?

a) Watchdog processes
b) Encryption
c) Cryptographic hashes
d) Web servers

Answer: b

Question: 8

Why is it important to store system logs remotely?

a) Local systems can't handle it.
b) Bandwidth is faster than disks.
c) Attackers might delete local logs.
d) It will defend against attacks.

Answer: c

Question: 9

An intrusion detection system can perform which of the following functions?

a) Block traffic
b) Filter traffic based on headers
c) Generate alerts on traffic
d) Log system messages

Answer: c

Question: 10

What order, from bottom to top, does the TCP/IP architecture use?

a) Network Access, Network, Transport, Application
b) Link, Internet, Transport, Application
c) Physical, Network, Session, Application
d) Data Link, Internet, Transport, Application

Answer: b

Avail the Study Guide to Pass EC-Council 312-50 CEH Exam:

- Find out about the 312-50 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **312-50 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the 312-50 training. Joining the EC-Council provided training for 312-50 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **312-50 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. 312-50 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the 312-50 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.