EC-COUNCIL 312-50

EC-Council CEH Certification Questions & Answers

Exam Summary – Syllabus –Questions

312-50

[EC-Council Certified Ethical Hacker (CEH)]

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

Table of Contents:

Know Your 312-50 Certification Well:

The 312-50 is best suitable for candidates who want to gain knowledge in the EC-Council Cyber Security. Before you start your 312-50 preparation you may struggle to get all the crucial CEH materials like 312-50 syllabus, sample questions, study guide.

But don't worry the 312-50 PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the 312-50 syllabus?
- How many questions are there in the 312-50 exam?
- Which Practice test would help me to pass the 312-50 exam at the first attempt?

Passing the 312-50 exam makes you EC-Council Certified Ethical Hacker (CEH). Having the CEH certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

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 - 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
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
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 - 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 - 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 - Cryptanalysis - Countermeasures

EC-Council 312-50 Sample Questions:

Question: 1

Which one of the following scanning techniques do attackers use to bypass firewall rules, logging mechanism, and also hide themselves as usual network traffic?

a) Stealth scanning technique
b) TCP connect scanning technique
c) Xmas scanning technique
d) Maintaining Access
e) FIN scanning technique

Answer: a

Question: 2

CAM table in switch stores information such as MAC addresses available on physical ports with their associated VLAN parameters. What happens when the CAM table is full?

a) Additional ARP request traffic will not be forwarded to any port on the switch
b) The switch will stop functioning and get disconnected from network
c) Additional ARP request traffic will flood every port on the switch
d) It does not affect the switch functioning

Answer: c

Question: 3

Consider the attack scenario given below:

Step 1: User browses a web page
Step 2: Web server replies with requested page and sets a cookie on the user's browser
Step 3: Attacker steals cookie (Sniffing, XSS, phishing attack)
Step 4: Attacker orders for product using modified cookie
Step 5: Product is delivered to attacker's address

Identify the web application attack.

a) Session fixation attack
b) Unvalidated redirects attack
c) Cookie poisoning attack
d) Denial-of-Service (DoS) attack

Answer: c

Question: 4

Which of the following is a mutation technique used for writing buffer overflow exploits in order to avoid IDS and other filtering mechanisms?

a) Assuming that a string function is exploited, send a long string as the input
b) Randomly replace the NOPs with functionally equivalent segments of the code (e.g.: x++; x-; ? NOP NOP)
c) Pad the beginning of the intended buffer overflow with a long run of NOP instructions (a NOP slide or sled) so the CPU will do nothing until it gets to the "main event"
d) Make a buffer to overflow on the lower part of heap, overwriting other dynamic variables, which can have unexpected and unwanted effects

Answer: b

Question: 5

A wireless antenna is an electrical device which converts electric currents into radio waves, and vice versa. Which antenna is used in wireless base stations and provides a 360 degree horizontal radiation pattern?

a) Omnidirectional antenna
b) Parabolic grid antenna
c) Yagi antenna
d) Dipole antenna

Answer: a

Question: 6

Which cryptographic attack refers to the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture?

a) Ciphertext-only Attack
b) Chosen-ciphertext Attack
c) Adaptive Chosen-plaintext Attack
d) Rubber Hose Attack

Answer: d

Question: 7

Which of the following Wi-Fi chalking method refers to drawing symbols in public places to advertise open Wi-Fi networks?

a) WarWalking
b) WarFlying
c) WarChalking
d) WarDriving

Answer: c

Question: 8

Which of the following scan only works if an operating system's TCP/IP implementation is based on RFC 793?

a) NULL scan
b) IDLE scan
c) TCP connect scan
d) Maintaining Access
e) FTP bounce scan

Answer: a

Question: 9

Which following OSI layer is responsible for encoding and decoding data packets into bits?

a) Application layer
b) Session layer
c) Data link layer
d) Network layer

Answer: c

Question: 10

Network Time Protocol (NTP) is designed to synchronize clocks of networked computers. Which of the following ports does NTP use as its primary means of communication?

a) UDP port 123
b) UDP port 113
c) UDP port 161
d) UDP port 320

Answer: a

Study Guide to Crack EC-Council CEH 312-50 Exam:

- Getting details of the 312-50 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 312-50 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the EC-Council provided training for 312-50 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 312-50 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 312-50 practice tests is must. Continuous practice will make you an expert in all syllabus areas.