EC-COUNCIL 312-38

EC-Council CND Certification Questions & Answers

Exam Summary – Syllabus –Questions

312-38
EC-Council Certified Network Defender (CND)
100 Questions Exam – 70% Cut Score – Duration of 240 minutes

Table of Contents:

Know Your 312-38 Certification Well:

The 312-38 is best suitable for candidates who want to gain knowledge in the EC-Council Cyber Security. Before you start your 312-38 preparation you may struggle to get all the crucial CND materials like 312-38 syllabus, sample questions, study guide.

But don't worry the 312-38 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 312-38 syllabus?
- How many questions are there in the 312-38 exam?
- Which Practice test would help me to pass the 312-38 exam at the first attempt?

Passing the 312-38 exam makes you EC-Council Certified Network Defender (CND). Having the CND 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 312-38 CND Certification Details:

Exam Name	EC-Council Certified Network Defender (CND)
Exam Code	312-38
Exam Price	$450 (USD)
Duration	240 mins
Number of Questions	100
Passing Score	70%
Books / Training	**Courseware**
Schedule Exam	**Pearson VUE OR ECC Exam Center**
Sample Questions	**EC-Council CND Sample Questions**
Practice Exam	**EC-Council 312-38 Certification Practice Exam**

312-38 Syllabus:

Topic	Details	Weights
Computer Network and Defense Fundamentals	- Understanding computer network - Describing OSI and TCP/IP network Models - Comparing OSI and TCP/IP network Models - Understanding different types of networks - Describing various network topologies - Understanding various network components - Explaining various protocols in TCP/IP protocol stack - Explaining IP addressing concept - Understanding Computer Network Defense (CND) - Describing fundamental CND attributes - Describing CND elements - Describing CND process and Approaches	5%
Network Security Threats, Vulnerabilities, and Attacks	- Understanding threat, attack, and vulnerability - Discussing network security concerns - Reasons behind network security concerns - Effect of network security breach on business continuity - Understanding different types of network threats - Understanding different types of network security vulnerabilities - Understanding different types of network attacks - Describing various network attacks	5%
Network Security Controls, Protocols, and Devices	- Understanding fundamental elements of network security - Explaining network access control mechanism - Understanding different types of access controls - Explaining network Authentication, Authorization and Auditing (AAA) mechanism - Explaining network data encryption mechanism - Describing Public Key Infrastructure (PKI) - Describing various network security protocols - Describing various network security devices	8%
Network Security Policy Design and Implementation	- Understanding security policy - Need of security policies - Describing the hierarchy of security policy - Describing the characteristics of a good security policy - Describing typical content of security policy - Understanding policy statement - Describing steps for creating and implementing security policy - Designing of security policy - Implementation of security policy - Describing various types of security policy - Designing of various security policies	6%

Topic	Details	Weights
	- Discussing various information security related standards, laws and acts	
Physical Security	- Understanding physical security - Importance of physical security - Factors affecting physical security - Describing various physical security controls - Understanding the selection of Fire Fighting Systems - Describing various access control authentication techniques - Understanding workplace security - Understanding personnel security - Describing Environmental Controls - Importance of physical security awareness and training	6%
Host Security	- Understanding host security - Understanding the importance of securing individual hosts - Understanding threats specific to hosts - Identifying paths to host threats - Purpose of host before assessment - Describing host security baselining - Describing OS security baselining - Understanding and describing security requirements for different types of servers - Understanding security requirements for hardening of routers - Understanding security requirements for hardening of switches - Understanding data security concerns when data is at rest, in use, and in motion - Understanding virtualization security	7%
Secure Firewall Configuration and Management	- Understanding firewalls - Understanding firewall security concerns - Describing various firewall technologies - Describing firewall topologies - Appropriate selection of firewall topologies - Designing and configuring firewall ruleset - Implementation of firewall policies - Explaining the deployment and implementation of firewall - Factors to considers before purchasing any firewall solution - Describing the configuring, testing and deploying of firewalls - Describing the management, maintenance and administration of firewall implementation - Understanding firewall logging	8%

Topic	Details	Weights
	- Measures for avoiding firewall evasion - Understanding firewall security best practices	
Secure IDS Configuration and Management	- Understanding different types of intrusions and their indications - Understanding IDPS - Importance of implementing IDPS - Describing role of IDPS in network defense - Describing functions, components, and working of IDPS - Explaining various types of IDS implementation - Describing staged deployment of NIDS and HIDS - Describing fine-tuning of IDS by minimizing false positive and false negative rate - Discussing characteristics of good IDS implementation - Discussing common IDS implementation mistakes and their remedies - Explaining various types of IPS implementation - Discussing requirements for selecting appropriate IDSP product - Technologies complementing IDS functionality	8%
Secure VPN Configuration and Management	- Understanding Virtual Private Network (VPN) and its working - Importance of establishing VPN - Describing various VPN components - Describing implementation of VPN concentrators and its functions - Explaining different types of VPN technologies - Discussing components for selecting appropriate VPN technology - Explaining core functions of VPN - Explaining various topologies for implementation of VPN - Discussing various VPN security concerns - Discussing various security implications to ensure VPN security and performance	6%
Wireless Network Defense	- Understanding wireless network - Discussing various wireless standards - Describing various wireless network topologies - Describing possible use of wireless networks - Explaining various wireless network components - Explaining wireless encryption (WEP, WPA,WPA2) technologies - Describing various authentication methods for wireless networks - Discussing various types of threats on wireless networks - Creation of inventory for wireless network	6%

Topic	Details	Weights
	components - Appropriate placement of wireless Access Point (AP) - Appropriate placement of wireless antenna - Monitoring of wireless network traffic - Detection and locating of rogue access points - Prevention of wireless network from RF interference - Describing various security implications for wireless network	
Network Traffic Monitoring and Analysis	- Understanding network traffic monitoring - Importance of network traffic monitoring - Discussing techniques used for network monitoring and analysis - Appropriate position for network monitoring - Connection of network monitoring system with managed switch - Understanding network traffic signatures - Baselining for normal traffic - Disusing the various categories of suspicious traffic signatures - Various techniques for attack signature analysis - Understanding Wireshark components, working and features - Demonstrating the use of various Wireshark filters - Demonstrating the monitoring LAN traffic against policy violation - Demonstrating the security monitoring of network traffic - Demonstrating the detection of various attacks using Wireshark - Discussing network bandwidth monitoring and performance improvement	9%
Network Risk and Vulnerability Management	- Understanding risk and risk management - Key roles and responsibilities in risk management - Understanding Key Risk Indicators (KRI) in risk management - Explaining phase involves in risk management - Understanding enterprise network risk management - Describing various risk management frameworks - Discussing best practices for effective implementation of risk management - Understanding vulnerability management - Explaining various phases involve in vulnerability management - Understanding vulnerability assessment and its importance - Discussing requirements for effective network vulnerability assessment - Discussing internal and external vulnerability	9%

Topic	Details	Weights
	assessment - Discussing steps for effective external vulnerability assessment - Describing various phases involve in vulnerability assessment - Selection of appropriate vulnerability assessment tool - Discussing best practices and precautions for deploying vulnerability assessment tool - Describing vulnerability reporting, mitigation, remediation and verification	
Data Backup and Recovery	- Understanding data backup - Describing the data backup plan - Describing the identification of data to backup - Determining the appropriate backup medium for data backup - Understanding RAID backup technology and its advantages - Describing RAID architecture - Describing various RAID levels and their use - Selection of appropriate RAID level - Understanding Storage Area Network (SAN) backup technology and its advantages - Best practices of using SAN - Understanding Network Attached Storage (NAS) backup technology and its advantages - Describing various types of NAS implementation	9%
Network Incident Response and Management	- Understanding Incident Handling and Response (IH&R) - Roles and responsibilities of Incident Response Team (IRT) - Describing role of first responder - Describing first response activities for network administrators - Describing Incident Handling and Response (IH&R) process - Understanding forensic investigation - People involved in forensics investigation - Describing forensics investigation methodology	8%

EC-Council 312-38 Sample Questions:

Question: 1

Which of the following network security controls can an administrator use to detect, deflect or study attempts to gain unauthorized access to information systems?

a) IDS/IPS
b) Network Protocol Analyzer
c) Proxy Server
d) Honeypot

Answer: d

Question: 2

Which technique is used in RAID level 0 where the data is split into blocks and written evenly across multiple disks?

a) Disk mirroring
b) Disk stripping
c) Data splitting
d) Disk partition

Answer: b

Question: 3

Identify the Password Attack Technique in which the adversary attacks cryptographic hash functions based on the probability, that if a hashing process is used for creating a key, then the same is used for other keys?

a) Dictionary Attack
b) Brute Forcing Attack
c) Hybrid Attack
d) Birthday Attack

Answer: d

Question: 4

Which of the following Wireshark filters can a network administrator use to view the packets without any flags set in order to detect TCP Null Scan attempts?

a) TCP.flags==0x000
b) tcp.flags==0X029
c) tcp.flags==0x003
d) tcp.dstport==7

Answer: a

Question: 5

Which authentication technique involves mathematical pattern-recognition of the colored part of the eye behind the cornea?

a) Iris Scanning
b) Retinal Scanning
c) Facial Recognition
d) Vein Scanning

Answer: a

Question: 6

Under which of the following acts can an international financial institution be prosecuted if it fails to maintain the privacy of its customer's information?

a) GLBA
b) FISMA
c) DMCA
d) SOX

Answer: a

Question: 7

Which of the following VPN topologies establishes a persistent connection between an organizations main office and its branch offices using a third-party network or the Internet?

a) Hub-and-Spoke
b) Full Mesh
c) Star
d) Point-to-Point

Answer: a

Question: 8

Which of the following commands can be used to disable unwanted services on Debian, Ubuntu and other Debian-based Linux distributions?

a) # chkconfig [service name]off
b) # chkconfig [service name] –del
c) # service [service name] stop
d) # update-rc.d -f [service name] remove

Answer: d

Question: 9

What is a person, who offers formal experienced testimony in the court, called?

a) Expert Witness
b) Evidence Manager
c) Evidence Documenter
d) Attorney

Answer: a

Question: 10

In Public Key Infrastructure (PKI), which authority is responsible for issuing and verifying the certificates?

a) Registration authority
b) Certificate authority
c) Digital Certificate authority
d) Digital signature authority

Answer: b

Study Guide to Crack EC-Council CND 312-38 Exam:

- Getting details of the 312-38 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 312-38 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 312-38 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 312-38 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 312-38 practice tests is must. Continuous practice will make you an expert in all syllabus areas.