312-38 New Cram Materials | Latest 312-38 Dumps Pdf

2026 Latest ActualTorrent 312-38 PDF Dumps and 312-38 Exam Engine Free Share: https://drive.google.com/open?id=1hQwCOH136Ar5YRD0Logsi0CKCoxWu44f

You can save time and clear the 312-38 certification test in one sitting if you skip unnecessary material and focus on our EC-COUNCIL 312-38 actual questions. It's time to expand your knowledge and skills if you're committed to pass the EC-COUNCIL 312-38 Exam and get the certification badge to advance your profession.

EC-Council 312-38 Exam Syllabus Topics:

Topic	Details	Weights
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 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	9%

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%
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 - Discussing various information security related standards, laws and acts	6%
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 - Measures for avoiding firewall evasion - Understanding firewall security best practices	8%
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 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%
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%

The EC-Council Certified Network Defender CND certification exam is designed for IT professionals, network administrators, security analysts, and anyone interested in a career in network security. The EC-Council Certified Network Defender (CND) certification is globally recognized and provides a competitive edge in the job market. It demonstrates the candidate's proficiency in network security and validates their commitment to maintaining the highest security standards. Overall, the EC-Council Certified Network Defender (CND) certification is an excellent choice for individuals seeking a career in network security and is an essential requirement for many job roles in the field.

312-38 New Cram Materials - EC-Council Certified Network Defender CND Realistic Latest Dumps Pdf Free PDF

We are amenable to offer help by introducing our 312-38 real exam materials and they can help you pass the EC-Council Certified Network Defender CND practice exam efficiently. All knowledge is based on the real exam by the help of experts. By compiling the most important points of questions into our 312-38 guide prep our experts also amplify some difficult and important points. There is no doubt they are clear-cut and easy to understand to fulfill your any confusion about the exam. Our EC-Council Certified Network Defender CND exam question is applicable to all kinds of exam candidates who eager to pass the exam. Last but not the least, they help our company develop brand image as well as help a great deal of exam candidates pass the exam with passing rate over 98 percent of our 312-38 Real Exam materials.

EC-COUNCIL 312-38 (EC-Council Certified Network Defender CND) Exam is a certification program designed for individuals who aspire to become network security professionals. EC-Council Certified Network Defender CND certification is recognized globally and is specifically designed to test the knowledge and practical skills required to protect an organization's network infrastructure against cyber threats. The EC-COUNCIL 312-38 Exam covers a broad range of topics, including network security, risk management, and ethical hacking.

EC-COUNCIL EC-Council Certified Network Defender CND Sample

Questions (Q195-Q200):

NEW QUESTION # 195
Which of the following layers of the OSI model provides interhost communication?

- A. Transport layer
- B. Session layer
- C. Application layer
- D. Network layer

Answer: B

NEW QUESTION # 196
Steven's company has recently grown from 5 employees to over 50. Every workstation has a public IP address and navigated to the Internet with little to no protection. Steven wants to use a firewall. He also wants IP addresses to be private addresses, to prevent public Internet devices direct access to them. What should Steven implement on the firewall to ensure this happens?

- A. Steven should use IPsec
- B. Steven should enabled Network Address Translation(NAT)
- C. Steven should use Open Shortest Path First (OSPF)
- D. Steven should use a Demilitarized Zone (DMZ)

Answer: B

Explanation:
Steven should implement Network Address Translation (NAT) on the firewall to ensure that the IP addresses of the workstations are private and not directly accessible from the public Internet. NAT translates the private IP addresses of the workstations to a public IP address before they are sent out to the Internet, and vice versa for incoming traffic. This not only hides the internal IP addresses but also allows multiple devices to share a single public IP address, which is essential as the company grows.

NEW QUESTION # 197
Which of the following RAID storage techniques divides the data into multiple blocks, which are further written across the RAID system?

- A. Mirroring
- B. Parity
- C. Striping
- D. None of these

Answer: C

NEW QUESTION # 198
Nancy is working as a network administrator for a small company. Management wants to implement a RAID storage for their organization. They want to use the appropriate RAID level for their backup plan that will satisfy the following requirements:
1. It has a parity check to store all the information about the data in multiple drives
2. Help reconstruct the data during downtime.
3. Process the data at a good speed.
4.Should not be expensive.
The management team asks Nancy to research and suggest the appropriate RAID level that best suits their requirements. What RAID level will she suggest?

- A. RAID 10
- B. RAID 0
- C. RAID 3
- D. RAID 1

Answer: C

Explanation:
RAID 3 is a level of RAID that uses striping with a dedicated parity disk. This means that data is spread across multiple disks, and parity information is stored on one dedicated disk. RAID 3 allows for good read and write speeds and can reconstruct data if one drive fails, thanks to the parity information. It is also a cost-effective solution because it requires only one additional disk for parity, regardless of the size of the array. This makes it suitable for environments where data throughput and fault tolerance are important but budget constraints are a consideration.

NEW QUESTION # 199
Which of the following network monitoring techniques requires extra monitoring software or hardware?

- A. Non-router based
- B. Hub based
- C. Router based
- D. Switch based

Answer: A

NEW QUESTION # 200
.....