312-38 Guide Torrent: EC-Council Certified Network Defender CND & 312-38 Test Braindumps Files

2026 Latest PassTestking 312-38 PDF Dumps and 312-38 Exam Engine Free Share: https://drive.google.com/open?id=13GRWwJFviVK_Ub3DDHFupQ8c_TTb2tpt

How far is the word from the deed? If you are a man of strong will, victory is at hand. Since you want to pass EC-COUNCIL 312-38 Exam, you must get the EC-COUNCIL 312-38 certification. PassTestking provide you with the latest certification training information and the most accurate tests answers. Real questions and answers can make your dream come true.

EC-Council 312-38 Exam Syllabus Topics:

Topic	Details	Weights
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%

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%
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%
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%
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 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%

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%
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%
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%

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 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	6%
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%

Interactive EC-COUNCIL 312-38 Online Practice Test Engine

The PassTestking is a trusted and reliable platform that has been helping the EC-Council Certified Network Defender CND (312-38) certification exam candidates for many years. Over this long time period, the 312-38 Exam Practice questions have helped the 312-38 exam candidates in their preparation and enabled them to pass the challenging exam on the first attempt.

The EC-Council CND certification is recognized by many organizations and is considered an essential requirement for many cybersecurity roles. EC-Council Certified Network Defender CND certification provides candidates with the knowledge and skills required to identify and mitigate network threats, as well as the ability to design and implement effective network defense strategies. EC-Council Certified Network Defender CND certification is particularly valuable for professionals who work in industries that handle sensitive information, such as finance, healthcare, and government.

EC-COUNCIL EC-Council Certified Network Defender CND Sample Questions (Q101-Q106):

NEW QUESTION # 101
Xenon is a leading real estate firm located in Australia. Recently, the company had decided a bid amount for a prestigious construction project and was sure of being awarded the project.
Unfortunately, the company lost the tender to one of its competitors. A few days later, while performing a network scan, the network admin identified that somebody had captured the confidential e-mails conversions related to the tender. Upon further investigation, the admin discovered that one of the switch ports was left open and an employee had plugged into the network using an Ethernet cable.
Which attack did the employee perform in the above situation?

- A. Network Sniffing
- B. Password Attack
- C. Social Engineering Attack
- D. Man-in-the-Middle Attack

Answer: A

Explanation:
In the scenario described, the employee performed a Network Sniffing attack. This type of attack involves capturing and analyzing packets traveling through a network. Since the admin discovered that confidential emails related to the tender were captured and that an open switch port was used to connect to the network, it indicates that the data was intercepted as it traveled across the network, which is characteristic of a sniffing attack. Network sniffing can be either passive or active; however, the scenario suggests a passive approach where the packets were monitored and captured without altering the network traffic.

NEW QUESTION # 102
Dan and Alex are business partners working together. Their Business-Partner Policy states that they should encrypt their emails before sending to each other. How will they ensure the authenticity of their emails?

- A. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.
- B. Dan will use his digital signature to sign his mails while Alex will use Dan's public key to verify the authencity of the mails.
- C. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.
- D. Dan will use his public key to encrypt his mails while Alex will use Dan's digital signature to verify the authenticity of the mails.

Answer: B

NEW QUESTION # 103
Which command is used to change the permissions of a file or directory?

- A. chmod
- B. kill
- C. rmdir
- D. systemctl

Answer: A

Explanation:
The command used to change the permissions of a file or directory in Linux is chmod (change mode).
The chmod command allows users to set or modify the access permissions for file system objects (files and directories). These permissions determine the actions that can be performed by different classes of users: the file owner, members of the file's group, and others. The command syntax typically includes the permissions to be set, which can be expressed in either symbolic or numeric format, and the name of the target file or directory.
References: The use of the chmod command is a fundamental concept covered in the EC-Council's Certified Network Defender (CND) program, as it pertains to securing data by correctly setting file and directory permissions as part of system hardening practices123.

NEW QUESTION # 104
Which of the following data security technology can ensure information protection by obscuring specific areas of information?

- A. Data encryption
- B. Data masking
- C. Data hashing
- D. Data retention

Answer: B

NEW QUESTION # 105
You are an IT security consultant working on a contract for a large manufacturing company to audit their entire network. After performing all the tests and building your report, you present a number of recommendations to the company and what they should implement to become more secure. One recommendation is to install a network-based device that notifies IT employees whenever malicious or questionable traffic is found. From your talks with the company, you know that they do not want a device that actually drops traffic completely, they only want notification. What type of device are you suggesting?

- A. You are suggesting a NIPS device
- B. A NIDS device would work best for the company
- C. The best solution to cover the needs of this company would be a HIDS device.
- D. A HIPS device would best suite this company

Answer: B

Explanation:
The device suggested is a Network Intrusion Detection System (NIDS). A NIDS monitors network traffic for suspicious activity and alerts the system or network administrator. Unlike a Network Intrusion Prevention System (NIPS), which actively blocks traffic deemed malicious, a NIDS does not interfere with the flow of traffic, thus fulfilling the company's requirement for a device that only notifies rather than drops traffic.

NEW QUESTION # 106
.....

BONUS!!! Download part of PassTestking 312-38 dumps for free: https://drive.google.com/open?id=13GRWwJFviVK_Ub3DDHFupQ8c_TTb2tpt