EC-Council

Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

NEW QUESTION 1
Identify the correct statements regarding a DMZ zone:

A. It is a file integrity monitoring mechanism
B. It is a Neutral zone between a trusted network and an untrusted network
C. It serves as a proxy
D. It includes sensitive internal servers such as database servers

Answer: B

NEW QUESTION 2
According to the company's security policy, all access to any network resources must use Windows Active Directory Authentication. A Linux server was recently installed to run virtual servers and it is not using Windows Authentication. What needs to happen to force this server to use Windows Authentication?

A. Edit the ADLIN file.
B. Edit the shadow file.
C. Remove the /var/bin/localauth.conf file.
D. Edit the PAM file to enforce Windows Authentication

Answer: D

NEW QUESTION 3
Assume that you are a network administrator and the company has asked you to draft an Acceptable Use Policy (AUP) for employees. Under which category of an information security policy does AUP fall into?

A. System Specific Security Policy (SSSP)
B. Incident Response Policy (IRP)
C. Enterprise Information Security Policy (EISP)
D. Issue Specific Security Policy (ISSP)

Answer: A

NEW QUESTION 4
Kelly is taking backups of the organization's data. Currently, he is taking backups of only those files which are created or modified after the last backup. What type of backup is Kelly using?

A. Full backup
B. Incremental backup
C. Differential Backup
D. Normal Backup

Answer: B

NEW QUESTION 5
Timothy works as a network administrator in a multinational organization. He decides to implement a dedicated network for sharing storage resources. He uses a _______ as it seperates the storage units from the servers and the user network.

A. SAN
B. SCSA
C. NAS
D. SAS

Answer: A

NEW QUESTION 6
A local bank wants to protect their card holder data. The bank should comply with the ________ standard to ensure the security of card holder data.

A. HIPAA
B. ISEC
C. PCI DSS
D. SOAX

Answer: C

NEW QUESTION 7
George was conducting a recovery drill test as a part of his network operation. Recovery drill tests are conducted on the _________.

A. Archived data
B. Deleted data
C. Data in transit
D. Backup data

Answer: D

NEW QUESTION 8
What is the name of the authority that verifies the certificate authority in digital certificates?

A. Directory management system
B. Certificate authority
C. Registration authority
D. Certificate Management system

Answer: D

NEW QUESTION 9
James wants to implement certain control measures to prevent denial-of-service attacks against the organization. Which of the following control measures can help James?

A. Strong passwords
B. Reduce the sessions time-out duration for the connection attempts
C. A honeypot in DMZ
D. Provide network-based anti-virus

Answer: B

NEW QUESTION 10
James is working as a Network Administrator in a reputed company situated in California. He is monitoring his network traffic with the help of Wireshark. He wants to check and analyze the traffic against a PING sweep attack. Which of the following Wireshark filters will he use?

A. lcmp.type==0 and icmp.type==16
B. lcmp.type==8 or icmp.type==16
C. lcmp.type==8 and icmp.type==0
D. lcmp.type==8 or icmp.type==0

Answer: D

NEW QUESTION 10
Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the data.
Which RAID level is used here?

A. RAID 3
B. RAID 1
C. RAID 5
D. RAID 0

Answer: B

NEW QUESTION 13
The agency Jacob works for stores and transmits vast amounts of sensitive government data that cannot be compromised. Jacob has implemented Encapsulating Security Payload (ESP) to encrypt IP traffic. Jacob wants to encrypt the IP traffic by inserting the ESP header in the IP datagram before the transport layer protocol header. What mode of ESP does Jacob need to use to encrypt the IP traffic?

A. He should use ESP in transport mode.
B. Jacob should utilize ESP in tunnel mode.
C. Jacob should use ESP in pass-through mode.
D. He should use ESP in gateway mode

Answer: B

NEW QUESTION 14
What command is used to terminate certain processes in an Ubuntu system?

A. #grep Kill [Target Process}
B. #kill-9[PID]
C. #ps ax Kill
D. # netstat Kill [Target Process]

Answer: C

NEW QUESTION 17
Rick has implemented several firewalls and IDS systems across his enterprise network. What should he do to effectively correlate all incidents that pass through these security controls?

A. Use firewalls in Network Address Transition (NAT) mode
B. Implement IPsec
C. Implement Simple Network Management Protocol (SNMP)
D. Use Network Time Protocol (NTP)

Answer:

D

NEW QUESTION 20
Heather has been tasked with setting up and implementing VPN tunnels to remote offices. She will most likely be implementing IPsec VPN tunnels to connect the offices. At what layer of the OSI model does an IPsec tunnel function on?

A. They work on the session layer.
B. They function on either the application or the physical layer.
C. They function on the data link layer
D. They work on the network layer

Answer: D

NEW QUESTION 23
An attacker uses different types of password cracking techniques to crack the password and gain unauthorized access to a system. An attacker uses a file containing a list of commonly used passwords. They then upload this file into the cracking application that runs against the user accounts. Which of the following password cracking techniques is the attacker trying?

A. Bruteforce
B. Rainbow table
C. Hybrid
D. Dictionary

Answer: D

NEW QUESTION 24
Which of the information below can be gained through network sniffing? (Select all that apply)

A. Telnet Passwords
B. Syslog traffic
C. DNS traffic
D. Programming errors

Answer: ABC

NEW QUESTION 25
Which IEEE standard does wireless network use?

A. 802.11
B. 802.18
C. 802.9
D. 802.10

Answer: A

NEW QUESTION 28
Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?

A. Mitigation
B. Assessment
C. Remediation
D. Verification

Answer: C

NEW QUESTION 29
John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a _______ and it has to adhere to the ________

A. Verification, Security Policies
B. Mitigation, Security policies
C. Vulnerability scanning, Risk Analysis
D. Risk analysis, Risk matrix

Answer: A

NEW QUESTION 30
As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2's _____ integrity check mechanism provides security against a replay attack

A. CBC-32
B. CRC-MAC
C. CRC-32
D. CBC-MAC

Answer:

D

NEW QUESTION 31
As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2's _______ integrity check mechanism provides security against a replay attack

A. CRC-32
B. CRC-MAC
C. CBC-MAC
D. CBC-32

Answer: C

NEW QUESTION 35
Frank is a network technician working for a medium-sized law firm in Memphis. Frank and two other IT employees take care of all the technical needs for the firm. The firm's partners have asked that a secure wireless network be implemented in the office so employees can move about freely without being tied to a network cable. While Frank and his colleagues are familiar with wired Ethernet technologies, 802.3, they are not familiar with how to setup wireless in a business environment. What IEEE standard should Frank and the other IT employees follow to become familiar with wireless?

A. The IEEE standard covering wireless is 802.9 and they should follow this.
B. 802.7 covers wireless standards and should be followed
C. They should follow the 802.11 standard
D. Frank and the other IT employees should follow the 802.1 standard.

Answer: C

NEW QUESTION 38
Identify the password cracking attempt involving precomputed hash values stored as plaintext and using these to crack the password.

A. Bruteforce
B. Rainbow table
C. Dictionary
D. Hybrid

Answer: B

NEW QUESTION 39
Management wants to bring their organization into compliance with the ISO standard for information security risk management. Which ISO standard will management decide to implement?

A. ISO/IEC 27004
B. ISO/IEC 27002
C. ISO/IEC 27006
D. ISO/IEC 27005

Answer: D

NEW QUESTION 43
Frank installed Wireshark at all ingress points in the network. Looking at the logs he notices an odd packet source. The odd source has an address of 1080:0:FF:0:8:800:200C:4171 and is using port 21. What does this source address signify?

A. This address means that the source is using an IPv6 address and is spoofed and signifies an IPv4 address of 127.0.0.1.
B. This source address is IPv6 and translates as 13.1.68.3
C. This source address signifies that the originator is using 802dot1x to try and penetrate into Frank's network
D. This means that the source is using IPv4

Answer: D

NEW QUESTION 47
......