

EC-Council

Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)



NEW QUESTION 1

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 2

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 3

The bank where you work has 600 windows computers and 400 Red Hat computers which primarily serve as bank teller consoles. You have created a plan and deployed all the patches to the Windows computers and you are now working on updating the Red Hat computers. What command should you run on the network to update the Red Hat computers, download the security package, force the package installation, and update all currently installed packages?

- A. You should run the `up2date -d -f -u` command
- B. You should run the `up2data -u` command
- C. You should run the `WSUS -d -f -u` command.
- D. You should type the `sysupdate -d` command

Answer: A

NEW QUESTION 4

Chris is a senior network administrator. Chris wants to measure the Key Risk Indicator (KRI) to assess the organization. Why is Chris calculating the KRI for his organization? It helps Chris to:

- A. Identifies adverse events
- B. Facilitates backward
- C. Facilitates post Incident management
- D. Notifies when risk has reached threshold levels

Answer: AD

NEW QUESTION 5

Fred is a network technician working for Johnson Services, a temporary employment agency in Boston. Johnson Services has three remote offices in New England and the headquarters in Boston where Fred works.

The company relies on a number of customized applications to perform daily tasks and unfortunately these applications require users to be local administrators. Because of this, Fred's supervisor wants to implement tighter security measures in other areas to compensate for the inherent risks in making those users local admins. Fred's boss wants a solution that will be placed on all computers throughout the company and monitored by Fred. This solution will gather information on all network traffic to and from the local computers without actually affecting the traffic. What type of solution does Fred's boss want to implement?

- A. Fred's boss wants a NIDS implementation.
- B. Fred's boss wants Fred to monitor a NIPS system.
- C. Fred's boss wants to implement a HIPS solution.
- D. Fred's boss wants to implement a HIDS solution.

Answer: D

NEW QUESTION 6

Daniel is giving training on designing and implementing a security policy in the organization. He is explaining the hierarchy of the security policy which demonstrates how policies are drafted, designed and implemented.

What is the correct hierarchy for a security policy implementation?

- A. Laws, Policies, Regulations, Procedures and Standards
- B. Regulations, Policies, Laws, Standards and Procedures
- C. Laws, Regulations, Policies, Standards and Procedures
- D. Procedures, Policies, Laws, Standards and Regulations

Answer: C

NEW QUESTION 7

Sam wants to implement a network-based IDS in the network. Sam finds out the one IDS solution which works is based on patterns matching. Which type of network-based IDS is Sam implementing?

- A. Behavior-based IDS
- B. Anomaly-based IDS
- C. Stateful protocol analysis
- D. Signature-based IDS

Answer: D

NEW QUESTION 8

Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user's email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures. What is Stephanie working on?

- A. Usability
- B. Data Integrity
- C. Availability
- D. Confidentiality

Answer: B

NEW QUESTION 9

Tom works as a network administrator in a multinational organization having branches across North America and Europe. Tom wants to implement a storage technology that can provide centralized data storage and provide free data backup on the server. He should be able to perform data backup and recovery more efficiently with the selected technology. Which of the following storage technologies best suits Tom's requirements?

- A. DAS
- B. PAS
- C. RAID
- D. NAS

Answer: D

NEW QUESTION 10

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 10

A company has the right to monitor the activities of their employees on different information systems according to the _____ policy.

- A. Information system
- B. User access control
- C. Internet usage
- D. Confidential data

Answer: B

NEW QUESTION 11

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 12

Which of the following acts as a verifier for the certificate authority?

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

Answer: D

NEW QUESTION 14

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 18

Identify the spread spectrum technique that multiplies the original data signal with a pseudo random noise spreading code.

- A. FHSS
- B. DSSS
- C. OFDM
- D. ISM

Answer: B

NEW QUESTION 19

Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. Which step should Malone list as the last step in the incident response methodology?

- A. Malone should list a follow-up as the last step in the methodology
- B. Recovery would be the correct choice for the last step in the incident response methodology
- C. He should assign eradication to the last step.
- D. Containment should be listed on Malone's plan for incident response.

Answer: B

NEW QUESTION 21

An US-based organization decided to implement a RAID storage technology for their data backup plan. John wants to setup a RAID level that require a minimum of six drives but will meet high fault tolerance and with a high speed for the data read and write operations. What RAID level is John considering to meet this requirement?

- A. RAID level 1
- B. RAID level 10
- C. RAID level 5
- D. RAID level 50

Answer: D

NEW QUESTION 23

The IR team and the network administrator have successfully handled a malware incident on the network. The team is now preparing countermeasure guideline to avoid a future occurrence of the malware incident.

Which of the following countermeasure(s) should be added to deal with future malware incidents? (Select all that apply)

- A. Complying with the company's security policies
- B. Implementing strong authentication schemes
- C. Implementing a strong password policy
- D. Install antivirus software

Answer: D

NEW QUESTION 24

Larry is responsible for the company's network consisting of 300 workstations and 25 servers. After using a hosted email service for a year, the company wants to control the email internally. Larry likes this idea because it will give him more control over the email. Larry wants to purchase a server for email but does not want the server to be on the internal network due to the potential to cause security risks. He decides to place the server outside of the company's internal firewall. There is another firewall connected directly to the Internet that will protect traffic from accessing the email server. The server will be placed between the two firewalls. What logical area is Larry putting the new email server into?

- A. He is going to place the server in a Demilitarized Zone (DMZ)
- B. He will put the email server in an IPsec zone.
- C. Larry is going to put the email server in a hot-server zone.
- D. For security reasons, Larry is going to place the email server in the company's Logical Buffer Zone (LBZ).

Answer: A

NEW QUESTION 29

Identify the network topology where each computer acts as a repeater and the data passes from one computer to the other in a single direction until it reaches the destination.

- A. Ring
- B. Mesh
- C. Bus
- D. Star

Answer: A

NEW QUESTION 34

Mark is monitoring the network traffic on his organization's network. He wants to detect a TCP and UDP ping sweep on his network. Which type of filter will be used to detect this on the network?

- A. Tcp.srcport==7 and udp.srcport==7
- B. Tcp.srcport==7 and udp.dstport==7
- C. Tcp.dstport==7 and udp.srcport==7
- D. Tcp.dstport==7 and udp.dstport==7

Answer: D

NEW QUESTION 35

Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. What is the last step he should list?

- A. Assign eradication.
- B. Recovery
- C. Containment
- D. A follow-up.

Answer: D

NEW QUESTION 38

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 41

Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user's email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures. What is Stephanie working on?

- A. Confidentiality
- B. Availability
- C. Data Integrity
- D. Usability

Answer: C

NEW QUESTION 44

Brendan wants to implement a hardware based RAID system in his network. He is thinking of choosing a suitable RAM type for the architectural setup in the system. The type he is interested in provides access times of up to 20 ns. Which type of RAM will he select for his RAID system?

- A. NVRAM
- B. SDRAM
- C. NAND flash memory
- D. SRAM

Answer: D

NEW QUESTION 48

During a security awareness program, management was explaining the various reasons which create threats to network security. Which could be a possible threat to network security?

- A. Configuring automatic OS updates
- B. Having a web server in the internal network
- C. Implementing VPN
- D. Patch management

Answer: B

NEW QUESTION 53

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 55

A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other function(s) of the device? (Select all that apply)

- A. Provides access memory, achieving high efficiency
- B. Assigns user addresses
- C. Enables input/output (I/O) operations
- D. Manages security keys

Answer: BCD

NEW QUESTION 59

Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?

- A. Their first step is to analyze the data they have currently gathered from the company or interviews.
- B. Their first step is to make a hypothesis of what their final findings will be.
- C. Their first step is to create an initial Executive report to show the management team.
- D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.

Answer: D

NEW QUESTION 60

Bryson is the IT manager and sole IT employee working for a federal agency in California. The agency was just given a grant and was able to hire on 30 more employees for a new extended project. Because of this, Bryson has hired on two more IT employees to train up and work. Both of his new hires are straight out of college and do not have any practical IT experience. Bryson has spent the last two weeks teaching the new employees the basics of computers, networking, troubleshooting techniques etc. To see how these two new hires are doing, he asks them at what layer of the OSI model do Network Interface Cards (NIC) work on. What should the new employees answer?

- A. NICs work on the Session layer of the OSI model.
- B. The new employees should say that NICs perform on the Network layer.
- C. They should tell Bryson that NICs perform on the Physical layer
- D. They should answer with the Presentation layer.

Answer: C

NEW QUESTION 65

Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. What is the last step he should list?

- A. Containment
- B. Assign eradication
- C. A follow-up
- D. Recovery

Answer: C

NEW QUESTION 69

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 72

Sean has built a site-to-site VPN architecture between the head office and the branch office of his company. When users in the branch office and head office try to communicate with each other, the traffic is encapsulated. As the traffic passes through the gateway, it is encapsulated again. The header and payload both are encapsulated. This second encapsulation occurs only in the _____ implementation of a VPN.

- A. Full Mesh Mode
- B. Point-to-Point Mode
- C. Transport Mode
- D. Tunnel Mode

Answer: D

NEW QUESTION 76

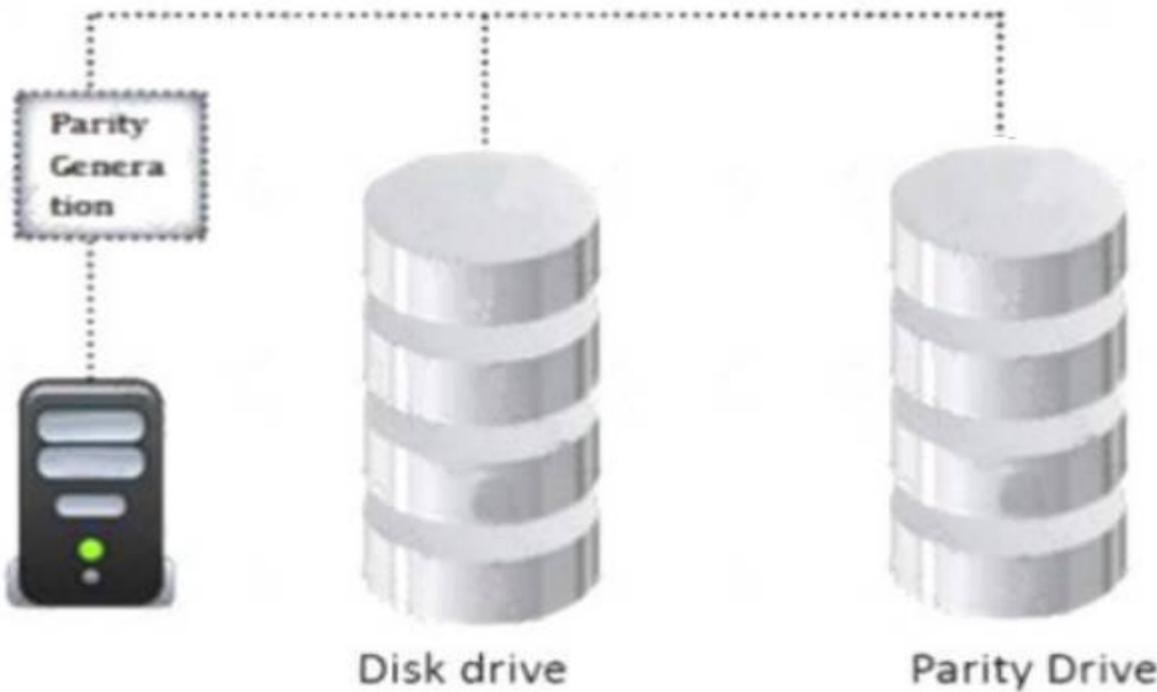
If a network is at risk from unskilled individuals, what type of threat is this?

- A. External Threats
- B. Structured Threats
- C. Unstructured Threats
- D. Internal Threats

Answer: C

NEW QUESTION 79

Identify the minimum number of drives required to setup RAID level 5.



- A. Multiple
- B. 3
- C. 4
- D. 2

Answer: B

NEW QUESTION 82

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 84

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

Answer: C

NEW QUESTION 88

John, the network administrator and he wants to enable the NetFlow feature in Cisco routers to collect and monitor the IP network traffic passing through the router. Which command will John use to enable NetFlow on an interface?

- A. Router(Config-if) # IP route - cache flow
- B. Router# Netmon enable
- C. Router IP route
- D. Router# netflow enable

Answer: A

NEW QUESTION 89

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 90

Ivan needs to pick an encryption method that is scalable even though it might be slower. He has settled on a method that works where one key is public and the other is private. What encryption method did Ivan settle on?

- A. Ivan settled on the private encryption method.
- B. Ivan settled on the symmetric encryption method.
- C. Ivan settled on the asymmetric encryption method
- D. Ivan settled on the hashing encryption method

Answer: C

NEW QUESTION 91

Which of the following is a best practice for wireless network security?

- A. Enabling the remote router login
- B. Do not changing the default SSID
- C. Do not placing packet filter between the AP and the corporate intranet
- D. Using SSID cloaking

Answer: D

NEW QUESTION 94

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

312-38 Practice Exam Features:

- * 312-38 Questions and Answers Updated Frequently
- * 312-38 Practice Questions Verified by Expert Senior Certified Staff
- * 312-38 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 312-38 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-38 Practice Test Here](#)