

EC-Council

Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)



NEW QUESTION 1

The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

- A. Bollards
- B. Fence
- C. Video surveillance
- D. Mantrap

Answer: B

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

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 4

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 5

You are responsible for network functions and logical security throughout the corporation. Your company has over 250 servers running Windows Server 2012, 5000 workstations running Windows 10, and 200 mobile users working from laptops on Windows 8. Last week 10 of your company's laptops were stolen from a salesman, while at a conference in Barcelona. These laptops contained proprietary company information.

While doing a damage assessment, a news story leaks about a blog post containing information about the stolen laptops and the sensitive information. What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?

- A. You should have used 3DES.
- B. You should have implemented the Distributed File System (DFS).
- C. If you would have implemented Pretty Good Privacy (PGP).
- D. You could have implemented the Encrypted File System (EFS)

Answer: D

NEW QUESTION 6

Kyle, a front office executive, suspects that a Trojan has infected his computer. What should be his first course of action to deal with the incident?

- A. Contain the damage
- B. Disconnect the five infected devices from the network
- C. Inform the IRT about the incident and wait for their response
- D. Inform everybody in the organization about the attack

Answer: C

NEW QUESTION 7

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 8

Management wants to calculate the risk factor for their organization. Kevin, a network administrator in the organization knows how to calculate the risk factor. Certain parameters are required before calculating risk factor. What are they? (Select all that apply) Risk factor =.....X.....X.....

- A. Vulnerability
- B. Impact
- C. Attack
- D. Threat

Answer: ABD

NEW QUESTION 9

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. `icmp.type==0 and icmp.type==16`
- B. `icmp.type==8 or icmp.type==16`
- C. `icmp.type==8 and icmp.type==0`
- D. `icmp.type==8 or icmp.type==0`

Answer: D

NEW QUESTION 10

The risk assessment team in Southern California has estimated that the probability of an incident that has potential to impact almost 80% of the bank's business is very high. How should this risk be categorized in the risk matrix?

- A. High
- B. Medium
- C. Extreme
- D. Low

Answer: C

NEW QUESTION 10

Ross manages 30 employees and only 25 computers in the organization. The network the company uses is a peer-to-peer. Ross configures access control measures allowing the employees to set their own control measures for their files and folders. Which access control did Ross implement?

- A. Discretionary access control
- B. Mandatory access control
- C. Non-discretionary access control
- D. Role-based access control

Answer: A

NEW QUESTION 15

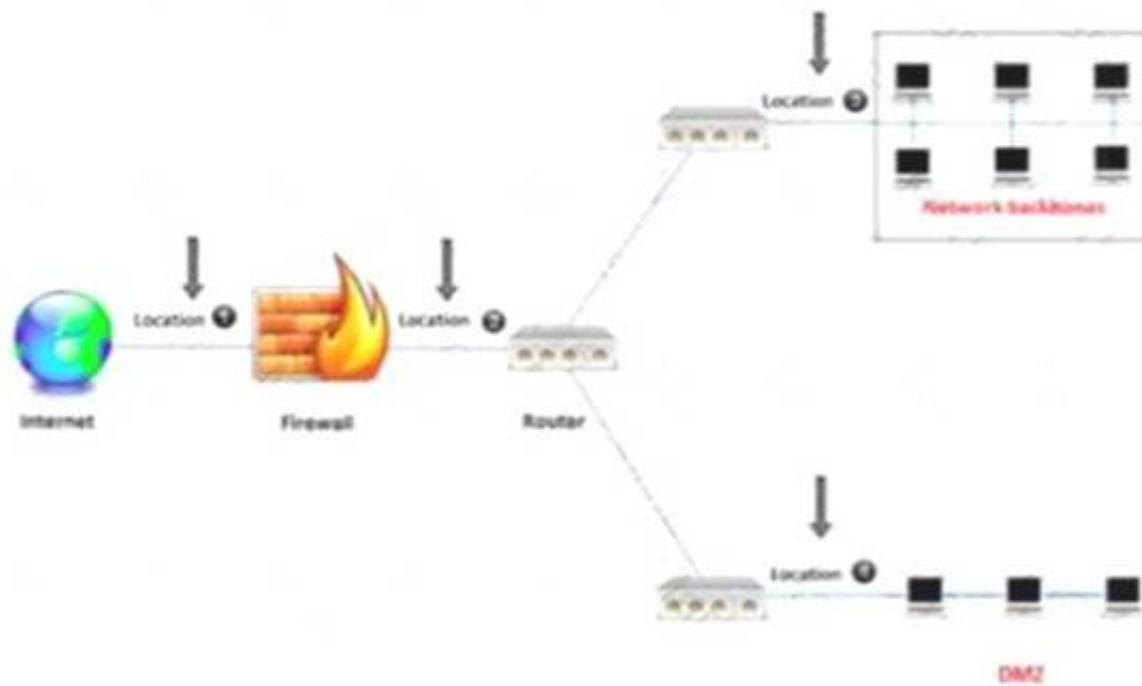
An US-based organization decided to implement a RAID storage technology for their data backup plan. John wants to setup a RAID level that require a minimum of six drives but will meet high fault tolerance and with a high speed for the data read and write operations. What RAID level is John considering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

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

Answer: D

NEW QUESTION 19

An administrator wants to monitor and inspect large amounts of traffic and detect unauthorized attempts from inside the organization, with the help of an IDS. They are not able to recognize the exact location to deploy the IDS sensor. Can you help him spot the location where the IDS sensor should be placed?



- A. Location 2
- B. Location 3
- C. Location 4
- D. Location 1

Answer: A

NEW QUESTION 21

An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

- A. Install a CCTV with cameras pointing to the entrance doors and the street
- B. Use fences in the entrance doors
- C. Use lights in all the entrance doors and along the company's perimeter
- D. Use an IDS in the entrance doors and install some of them near the corners

Answer: A

NEW QUESTION 25

Which OSI layer does a Network Interface Card (NIC) work on?

- A. Physical layer
- B. Presentation layer
- C. Network layer
- D. Session layer

Answer: A

NEW QUESTION 26

Henry needs to design a backup strategy for the organization with no service level downtime. Which backup method will he select?

- A. Normal backup
- B. Warm backup
- C. Hot backup
- D. Cold backup

Answer: C

NEW QUESTION 30

Liza was told by her network administrator that they will be implementing IPsec VPN tunnels to connect the branch locations to the main office. What layer of the OSI model do IPsec tunnels function on?

- A. The data link layer
- B. The session layer
- C. The network layer
- D. The application and physical layers

Answer: C

NEW QUESTION 32

The network admin decides to assign a class B IP address to a host in the network. Identify which of the following addresses fall within a class B IP address range.

- A. 255.255.255.0
- B. 18.12.4.1
- C. 172.168.12.4

D. 169.254.254.254

Answer: C

NEW QUESTION 34

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 38

David is working in a mid-sized IT company. Management asks him to suggest a framework that can be used effectively to align the IT goals to the business goals of the company. David suggests the _____ framework, as it provides a set of controls over IT and consolidates them to form a framework.

- A. RMIS
- B. ITIL
- C. ISO 27007
- D. COBIT

Answer: D

NEW QUESTION 42

Consider a scenario consisting of a tree network. The root Node N is connected to two main nodes N1 and N2. N1 is connected to N11 and N12. N2 is connected to N21 and N22. What will happen if any one of the main nodes fail?

- A. Failure of the main node affects all other child nodes at the same level irrespective of the main node.
- B. Does not cause any disturbance to the child nodes or its transmission
- C. Failure of the main node will affect all related child nodes connected to the main node
- D. Affects the root node only

Answer: C

NEW QUESTION 43

Blake is working on the company's updated disaster and business continuity plan. The last section of the plan covers computer and data incidence response. Blake is outlining the level of severity for each type of incident in the plan. Unsuccessful scans and probes are at what severity level?

- A. Extreme severity level
- B. Low severity level
- C. Mid severity level
- D. High severity level

Answer: B

NEW QUESTION 47

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 48

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 53

Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start

scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session. She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?

- A. The type of scan she is using is called a NULL scan.
- B. Cindy is using a half-open scan to find live hosts on her network.
- C. Cindy is attempting to find live hosts on her company's network by using a XMAS scan.
- D. She is utilizing a RST scan to find live hosts that are listening on her network.

Answer: B

NEW QUESTION 54

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 59

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 61

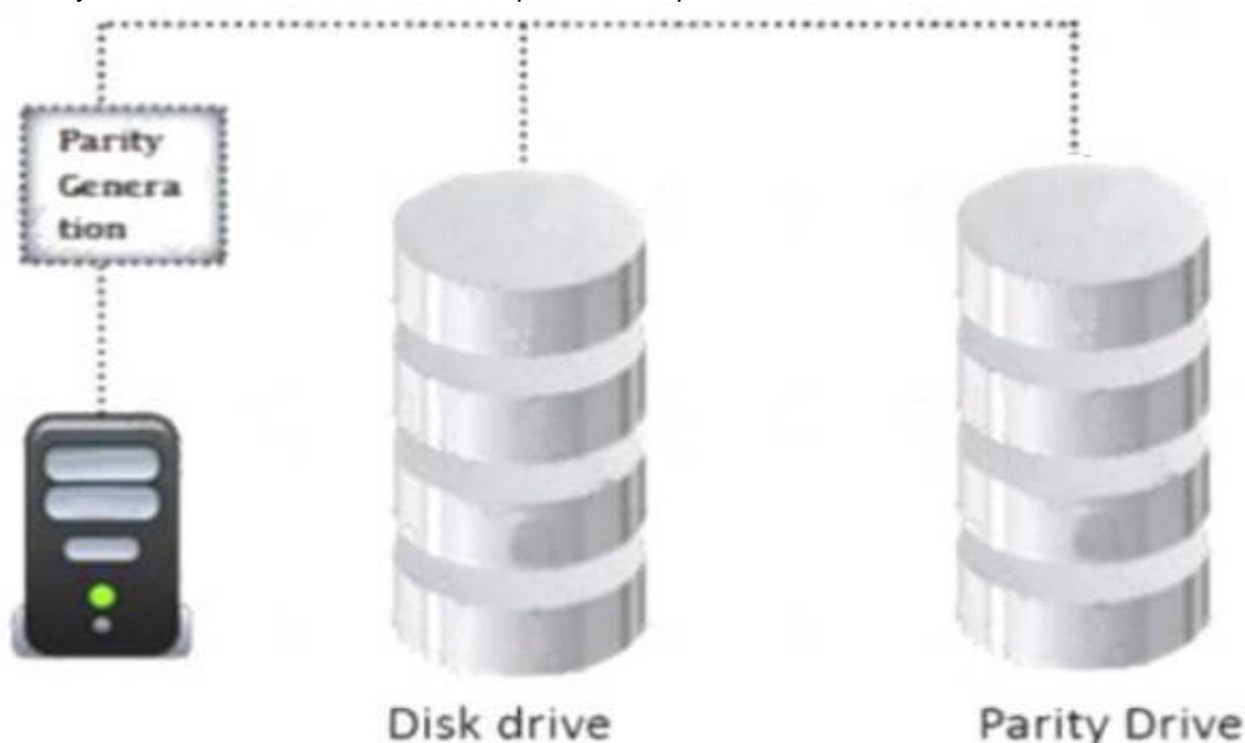
If a network is at risk from unskilled individuals, what type of threat is this?

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

Answer: C

NEW QUESTION 65

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



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

Answer: B

NEW QUESTION 70

Lyle is the IT director for a medium-sized food service supply company in Nebraska. Lyle's company employs over 300 workers, half of which use computers. He recently came back from a security training seminar on logical security. He now wants to ensure his company is as secure as possible. Lyle has many network nodes and workstation nodes across the network. He does not have much time for implementing a network-wide solution. He is primarily concerned about preventing any external attacks on the network by using a solution that can drop packets if they are found to be malicious. Lyle also wants this solution to be easy to implement and be network-wide. What type of solution would be best for Lyle?

- A. A NEPT implementation would be the best choice.
- B. To better serve the security needs of his company, Lyle should use a HIDS system.
- C. Lyle would be best suited if he chose a NIPS implementation
- D. He should choose a HIPS solution, as this is best suited to his needs.

Answer: C

NEW QUESTION 73

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 78

A network is setup using an IP address range of 0.0.0.0 to 127.255.255.255. The network has a default subnet mask of 255.0.0.0. What IP address class is the network range a part of?

- A. Class C
- B. Class A
- C. Class B
- D. Class D

Answer: B

NEW QUESTION 80

.....

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](#)