# 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**
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**
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 5**
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 6**
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 7**
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 8**
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 9**
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 10**
The company has implemented a backup plan. James is working as a network administrator for the company and is taking full backups of the data every time a backup is initiated. Alex who is a senior security manager talks to him about using a differential backup instead and asks him to implement this once a full backup of the data is completed. What is/are the reason(s) Alex is suggesting that James use a differential backup? (Select all that apply)

A. Less storage space is required
B. Father restoration
C. Slower than a full backup
D. Faster than a full backup
E. Less expensive than full backup

**Answer:** AD

**NEW QUESTION 10**
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 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 16**
Sam, a network administrator is using Wireshark to monitor the network traffic of the organization. He wants to detect TCP packets with no flag set to check for a specific attack attempt. Which filter will he use to view the traffic?

A. Tcp.flags==0x000
B. Tcp.flags==0000x
C. Tcp.flags==000x0
D. Tcp.flags==x0000

**Answer:** A

**NEW QUESTION 20**
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 24**
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

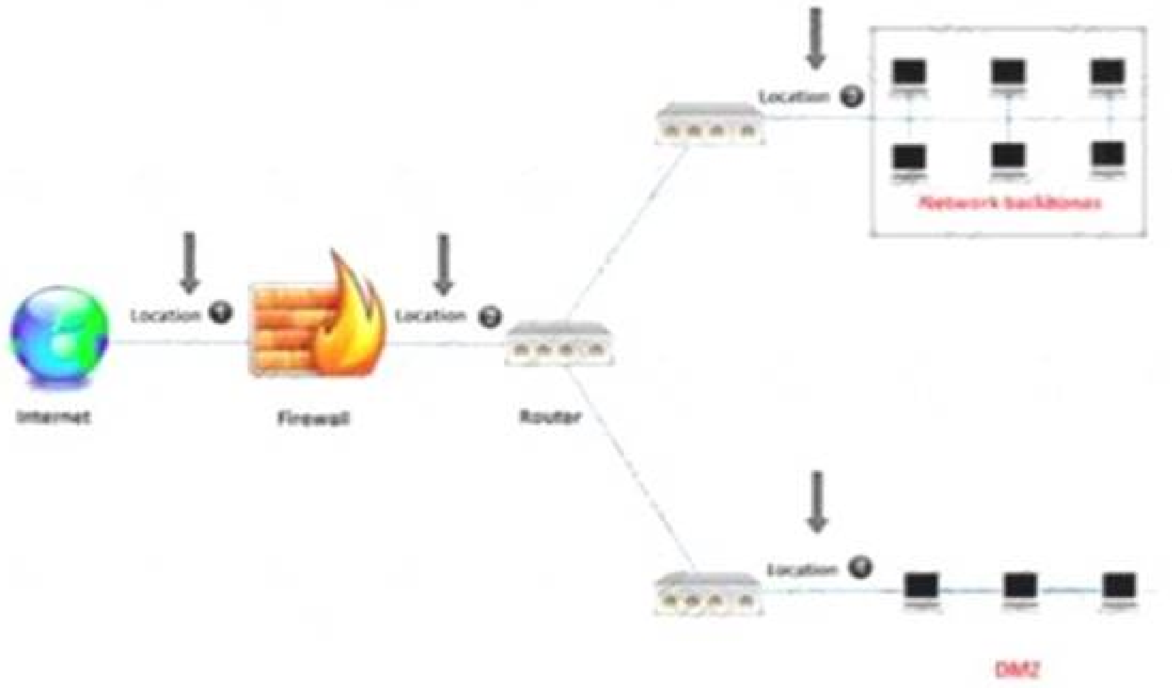
**Answer:** A

**NEW QUESTION 27**
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 28**
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 30**
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 31**
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 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 36**
A company wants to implement a data backup method which allows them to encrypt the data ensuring its security as well as access at any time and from any location. What is the appropriate backup method that should be implemented?

A. Onsite backup
B. Hot site backup
C. Offsite backup
D. Cloud backup

**Answer:** D

**NEW QUESTION 40**
------------is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs)

A. 802.15
B. 802.16
C. 802.15.4
D. 802.12

**Answer:** B

**NEW QUESTION 45**
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 49**
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 53**
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 57**

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 59**
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 64**
Alex is administrating the firewall in the organization's network. What command will he use to check all the remote addresses and ports in numerical form?

A. Netstat -o
B. Netstat -a
C. Netstat -ao
D. Netstat -an

**Answer:** D

**NEW QUESTION 65**
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 70**
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 71**
-----------is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs)

A. 802.15.4
B. 802.15
C. 802.12
D. 802.16

**Answer:** D

**NEW QUESTION 74**
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 76**
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 79**
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 83**
Michael decides to view the-----------------to track employee actions on the organization's network.

A. Firewall policy
B. Firewall log
C. Firewall settings
D. Firewall rule set

**Answer:** B

**NEW QUESTION 86**
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 89**
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 though 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

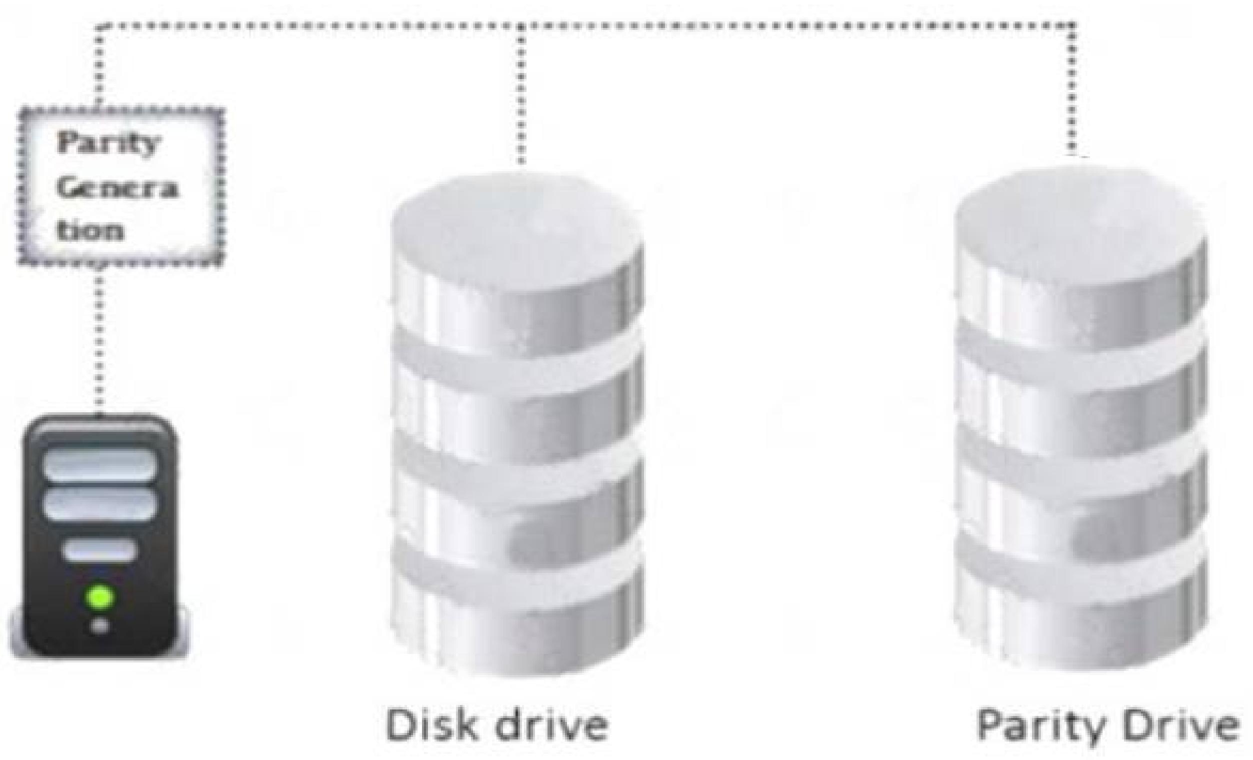
**Answer:** D

**NEW QUESTION 93**
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 95**
Identify the minimum number of drives required to setup RAID level 5.



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

**Answer:** B

**NEW QUESTION 99**
Management decides to implement a risk management system to reduce and maintain the organization's risk at an acceptable level. Which of the following is the correct order in the risk management phase?

A. Risk Identification, Risk Assessment, Risk Treatment, Risk Monitoring & Review
B. Risk Treatment, Risk Monitoring & Review, Risk Identification, Risk Assessment
C. Risk Assessment, Risk Treatment, Risk Monitoring & Review, Risk Identification
D. Risk Identificatio
E. Risk Assessmen
F. Risk Monitoring & Review, Risk Treatment

**Answer:** A

**NEW QUESTION 100**
Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A. Automated Field Correlation
B. Field-Based Approach
C. Rule-Based Approach
D. Graph-Based Approach

**Answer:** A

**NEW QUESTION 103**
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 108**
Alex is administrating the firewall in the organization's network. What command will he use to check the ports applications open?

A. Netstat -an
B. Netstat -o
C. Netstat -a
D. Netstat -ao

**Answer:** A

**NEW QUESTION 109**
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 112**
Which of the following VPN topologies establishes a persistent connection between an organization's main office and its branch offices using a third-party network or the Internet?

A. Star
B. Point-to-Point
C. Full Mesh
D. Hub-and-Spoke

**Answer:** D

**NEW QUESTION 113**
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 114**
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 117**
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 118**
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 121**
James was inspecting ARP packets in his organization's network traffic with the help of Wireshark. He is checking the volume of traffic containing ARP requests as well as the source IP address from which they are originating. Which type of attack is James analyzing?

A. ARP Sweep
B. ARP misconfiguration
C. ARP spoofinq

D. ARP Poisioning

**Answer:** A

**NEW QUESTION 124**
You are monitoring your network traffic with the Wireshark utility and noticed that your network is experiencing a large amount of traffic from a certain region. You suspect a DoS incident on the network. What will be your first reaction as a first responder?

A. Avoid Fear, Uncertainty and Doubt
B. Communicate the incident
C. Make an initial assessment
D. Disable Virus Protection

**Answer:** A

**NEW QUESTION 126**
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 130**
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 a Demilitarized Zone (DMZ)
B. Steven should use Open Shortest Path First (OSPF)
C. Steven should use IPsec
D. Steven should enabled Network Address Translation(NAT)

**Answer:** D

**NEW QUESTION 131**
An organization needs to adhere to the ________ rules for safeguarding and protecting the electronically stored health information of employees.

A. HI PA A
B. PCI DSS
C. ISEC
D. SOX

**Answer:** A

**NEW QUESTION 136**
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 139**
......