

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

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

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 4

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 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

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 separates the storage units from the servers and the user network.

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

Answer: A

NEW QUESTION 9

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 10

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 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. Faster restoration
- C. Slower than a full backup
- D. Faster than a full backup
- E. Less expensive than full backup

Answer: AD

NEW QUESTION 14

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 17

John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network. Which of the following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt?

- A. `Tcp.flags==0x2b`
- B. `Tcp.flags=0x00`
- C. `Tcp.options.mss_val<1460`
- D. `Tcp.options.wscale_val==20`

Answer: ABC

NEW QUESTION 21

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 25

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 26

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 27

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 30

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 32

Geon Solutions INC., had only 10 employees when it started. But as business grew, the organization had to increase the amount of staff. The network administrator is finding it difficult to accommodate an increasing number of employees in the existing network topology. So the organization is planning to implement a new topology where it will be easy to accommodate an increasing number of employees. Which network topology will help the administrator solve the problem of needing to add new employees and expand?

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

Answer: B

NEW QUESTION 37

Harry has sued the company claiming they made his personal information public on a social networking site in the United States. The company denies the allegations and consulted a/an _____ for legal advice to defend them against this allegation.

- A. PR Specialist
- B. Attorney
- C. Incident Handler

D. Evidence Manager

Answer: B

NEW QUESTION 39

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 40

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 42

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 44

-----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

Harry has successfully completed the vulnerability scanning process and found serious vulnerabilities exist in the organization's network. Identify the vulnerability management phases through which he will proceed to ensure all the detected vulnerabilities are addressed and eradicated. (Select all that apply)

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

Answer: ACD

NEW QUESTION 48

James is a network administrator working at a student loan company in Minnesota. This company processes over 20,000 student loans a year from colleges all over the state. Most communication between the company schools, and lenders is carried out through emails. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, James wants to utilize email encryption. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt emails. What should James use?

- A. James could use PGP as a free option for encrypting the company's emails.
- B. James should utilize the free OTP software package.
- C. James can use MD5 algorithm to encrypt all the emails
- D. James can enforce mandatory HTTPS in the email clients to encrypt emails

Answer: A

NEW QUESTION 51

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 56

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 58

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 60

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 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 68

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 69

-----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 72

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 76

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 77

Kyle is an IT consultant working on a contract for a large energy company in Houston. Kyle was hired on to do contract work three weeks ago so the company could prepare for an external IT security audit. With suggestions from upper management, Kyle has installed a network-based IDS system. This system checks for abnormal behavior and patterns found in network traffic that appear to be dissimilar from the traffic normally recorded by the IDS. What type of detection is this network-based IDS system using?

- A. This network-based IDS system is using anomaly detection.
- B. This network-based IDS system is using dissimilarity algorithms.
- C. This system is using misuse detection.
- D. This network-based IDS is utilizing definition-based detection.

Answer: A

NEW QUESTION 80

Which IEEE standard does wireless network use?

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

Answer: A

NEW QUESTION 83

The-----protocol works in the network layer and is responsible for handling the error codes during the delivery of packets. This protocol is also responsible for providing communication in the TCP/IP stack.

- A. RARP
- B. ICMP
- C. DHCP
- D. ARP

Answer: B

NEW QUESTION 86

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 87

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 90

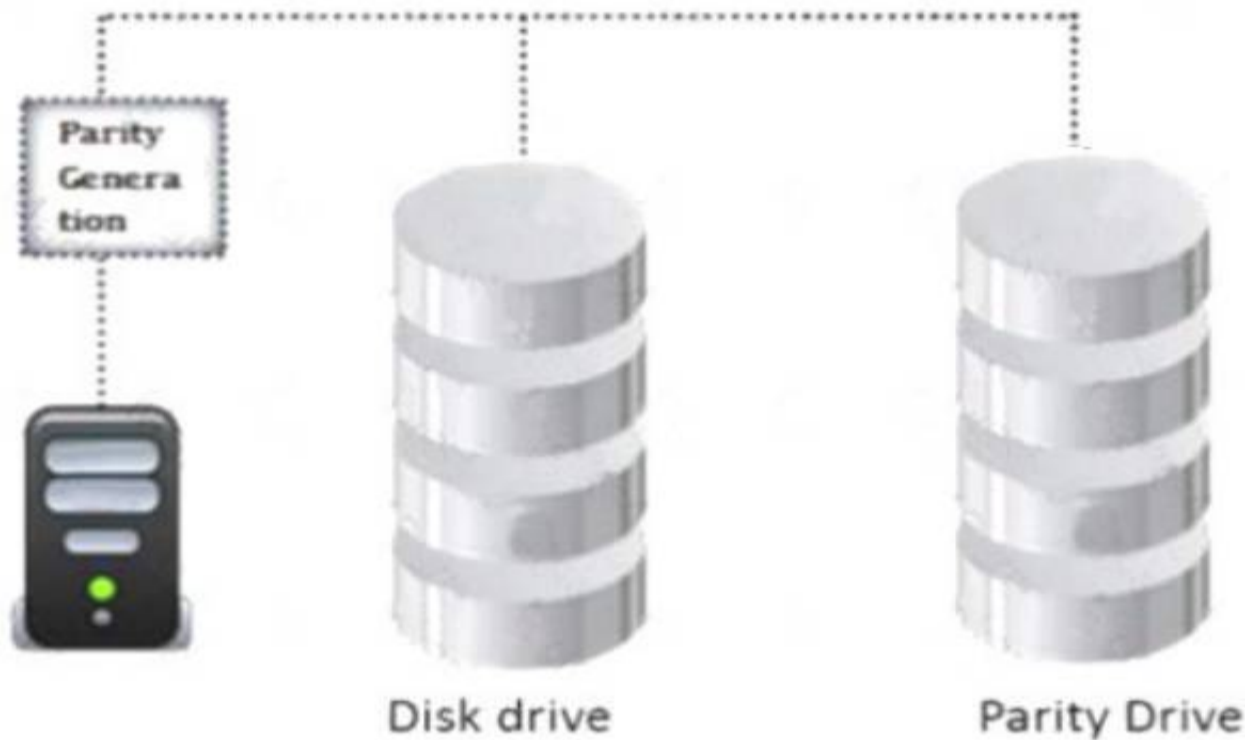
John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a _____ and it has to adhere to the _____

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

Answer: A

NEW QUESTION 92

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



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

Answer: B

NEW QUESTION 97

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 102

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 106

Katie has implemented the RAID level that split data into blocks and evenly write the data to multiple hard drives but does not provide data redundancy. This type of RAID level requires a minimum of _____ in order to setup.

- A. Four drives
- B. Three drives
- C. Two drives
- D. Six drives

Answer: C

NEW QUESTION 111

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 115

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 119

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 120

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 125

Kyle is an IT technician managing 25 workstations and 4 servers. The servers run applications and mostly store confidential data. Kyle must backup the server's data daily to ensure nothing is lost. The power in the company's office is not always reliable, Kyle needs to make sure the servers do not go down or are without power for too long. Kyle decides to purchase an Uninterruptible Power Supply (UPS) that has a pair of inverters and converters to charge the battery and provides power when needed. What type of UPS has Kyle purchased?

- A. Kyle purchased a Ferro resonant Standby UPS.
- B. Kyle purchased a Line-Interactive UPS
- C. He has bought a Standby UPS
- D. He purchased a True Online UPS.

Answer: C

NEW QUESTION 126

John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information. Which type of firewall service is John thinking of implementing?

- A. Application level gateway
- B. Stateful Multilayer Inspection
- C. Circuit level gateway
- D. Packet Filtering

Answer: C

NEW QUESTION 127

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 130

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 134

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 137

.....

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](#)