



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

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 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

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 5

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 6

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 7

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 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

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 10

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 10

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 12

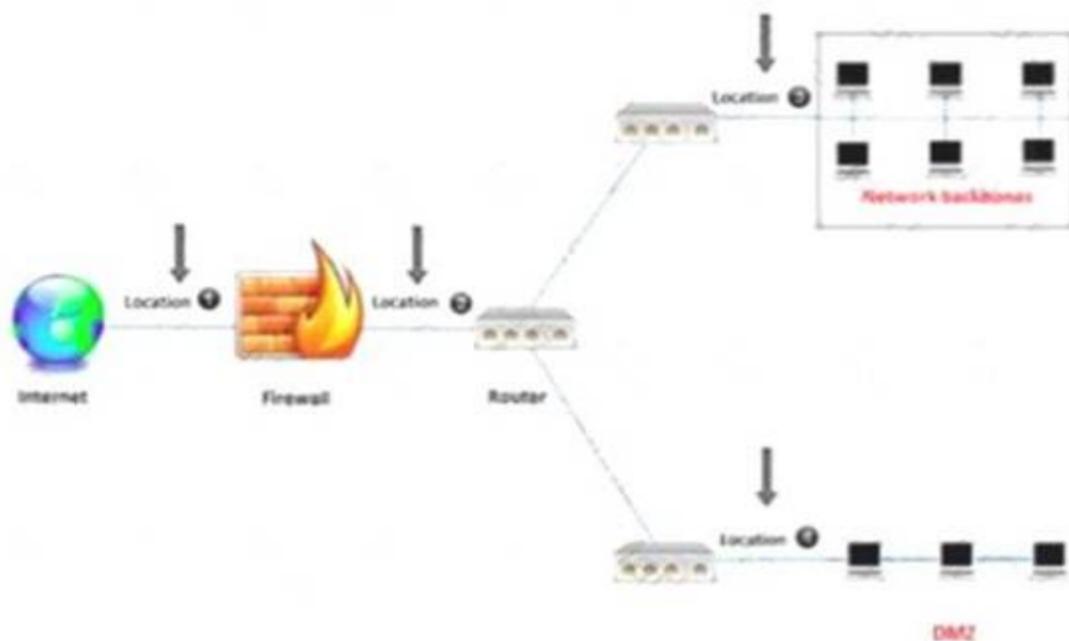
An US-based organization decided to implement a RAID storage technology for their data backup plan. John wants to setup a RAID level that require a minimum of six drives but will meet high fault tolerance and with a high speed for the data read and write operations. What RAID level is John considering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

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

Answer: D

NEW QUESTION 13

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 17

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 18

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 20

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 24

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 29

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 34

Management asked Adam to implement a system allowing employees to use the same credentials to access multiple applications. Adam should implement the-----authentication technique to satisfy the management request.

- A. Two-factor Authentication
- B. Smart Card Authentication
- C. Single-sign-on
- D. Biometric

Answer: C

NEW QUESTION 39

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 41

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 42

Paul is a network security technician working on a contract for a laptop manufacturing company in Chicago. He has focused primarily on securing network devices, firewalls, and traffic traversing in and out of the network. He just finished setting up a server a gateway between the internal private network and the outside public network. This server will act as a proxy, limited amount of services, and will filter packets. What is this type of server called?

- A. Bastion host
- B. Edge transport server
- C. SOCKS hshot
- D. Session layer firewall

Answer: A

NEW QUESTION 44

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 47

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 51

Dan and Alex are business partners working together. Their Business-Partner Policy states that they should encrypt their emails before sending to each other. How will they ensure the authenticity of their emails?

- A. Dan will use his public key to encrypt his mails while Alex will use Dan's digital signature to verify the authenticity of the mails.
- B. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.
- C. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.
- D. Dan will use his digital signature to sign his mails while Alex will use Dan's public key to verify the authenticity of the mails.

Answer: D

NEW QUESTION 53

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

Answer: D

NEW QUESTION 54

Which VPN QoS model guarantees the traffic from one customer edge (CE) to another?

- A. Pipe Model
- B. AAA model
- C. Hub-and-Spoke VPN model
- D. Hose mode

Answer: A

NEW QUESTION 56

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

Which IEEE standard does wireless network use?

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

Answer: A

NEW QUESTION 62

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

Answer: B

NEW QUESTION 65

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 70

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 72

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 73

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 77

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 82

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 Identification
- E. Risk Assessment
- F. Risk Monitoring & Review, Risk Treatment

Answer: A

NEW QUESTION 83

A newly joined network administrator wants to assess the organization against possible risk. He notices the organization doesn't have a _____ identified which helps measure how risky an activity is.

- A. Risk Severity
- B. Risk Matrix
- C. Key Risk Indicator
- D. Risk levels

Answer: C

NEW QUESTION 86

Justine has been tasked by her supervisor to ensure that the company's physical security is on the same level as their logical security measures. She installs video cameras at all entrances and exits and installs badge access points for all doors. The last item she wants to install is a method to prevent unauthorized people piggybacking employees. What should she install to prevent piggybacking?

- A. She should install a mantrap
- B. Justine needs to install a biometrics station at each entrance
- C. Justine will need to install a revolving security door
- D. She should install a Thompson Trapdoor.

Answer: A

NEW QUESTION 88

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 92

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 97

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 99

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 101

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 104

.....

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](#)