

## Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

<https://www.2passeasy.com/dumps/312-38/>



#### NEW QUESTION 1

Daniel is monitoring network traffic with the help of a network monitoring tool to detect any abnormalities. What type of network security approach is Daniel adopting?

- A. Preventative
- B. Reactive
- C. Retrospective
- D. Defense-in-depth

**Answer: B**

#### NEW QUESTION 2

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 3

Assume that you are working as a network administrator in the head office of a bank. One day a bank employee informed you that she is unable to log in to her system. At the same time, you get a call from another network administrator informing you that there is a problem connecting to the main server. How will you prioritize these two incidents?

- A. Based on approval from management
- B. Based on a first come first served basis
- C. Based on a potential technical effect of the incident
- D. Based on the type of response needed for the incident

**Answer: C**

#### NEW QUESTION 4

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 5

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 6

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 7

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 8

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 9

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 10

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 10

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 15

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 17

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

Jason has set a firewall policy that allows only a specific list of network services and deny everything else. This strategy is known as a \_\_\_\_\_.

- A. Default allow
- B. Default deny
- C. Default restrict
- D. Default access

**Answer:** B

#### NEW QUESTION 25

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 27

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 28

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 29

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 32

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 37

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 40

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 43

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 47

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 52

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 57

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 62

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 66

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 70

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 72

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 74

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 75

John has implemented \_\_\_\_\_ in the network to restrict the limit of public IP addresses in his organization and to enhance the firewall filtering technique.

- A. DMZ
- B. Proxies
- C. VPN
- D. NAT

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

**Answer:** D

#### NEW QUESTION 79

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 83

Which of the information below can be gained through network sniffing? (Select all that apply)

- A. Telnet Passwords
- B. Syslog traffic
- C. DNS traffic
- D. Programming errors

**Answer:** ABC



#### NEW QUESTION 88

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 92

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 93

Management asked their network administrator to suggest an appropriate backup medium for their backup plan that best suits their organization's need. Which of the following factors will the administrator consider when deciding on the appropriate backup medium?

- A. Capability
- B. Accountability
- C. Extensibility
- D. Reliability

**Answer:** ACD

#### NEW QUESTION 94

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 95

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 100

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 103

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 108

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 109

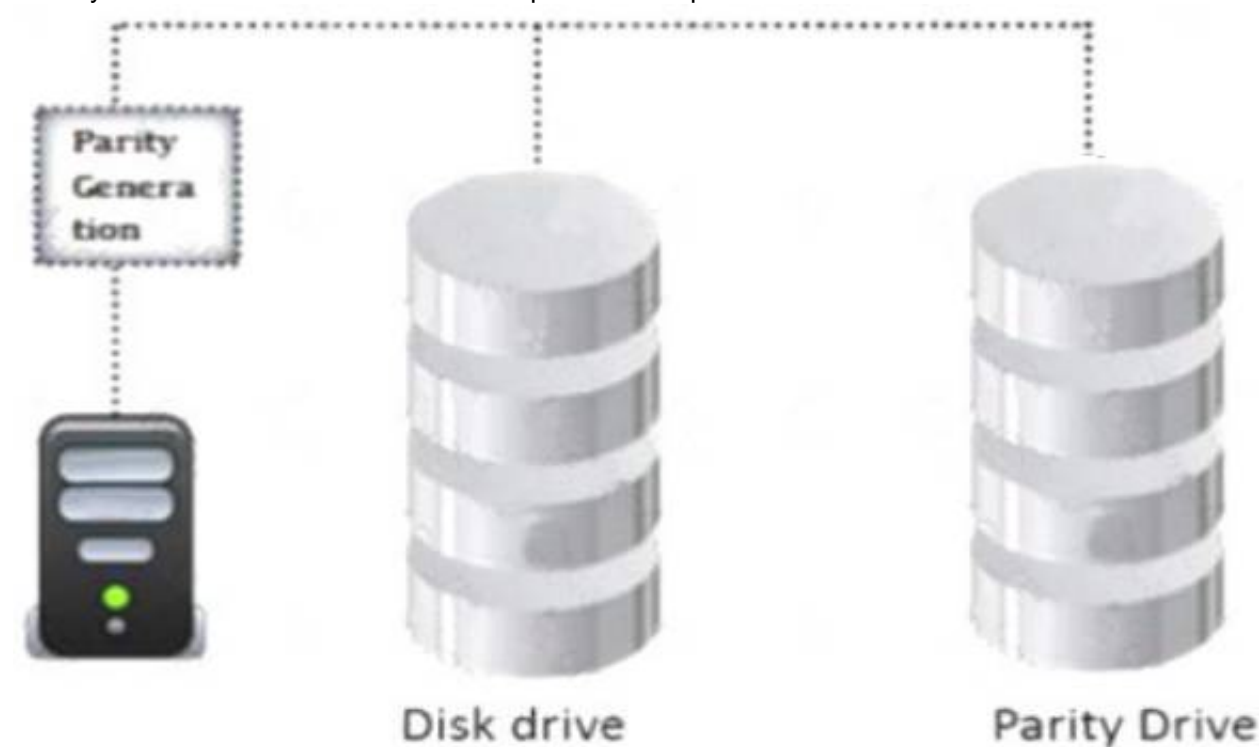
If a network is at risk from unskilled individuals, what type of threat is this?

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

**Answer: C**

#### NEW QUESTION 110

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



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

**Answer: B**

#### NEW QUESTION 114

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 116

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 117

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 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 124

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 128

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 spoofing
- D. ARP Poisoning

**Answer:** A

#### NEW QUESTION 131

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 133

Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered. What tool could Simon and his administrators implement to accomplish this?

- A. Snort is the best tool for their situation
- B. They can implement Wireshark
- C. They could use Tripwire
- D. They need to use Nessus

**Answer:** C

#### NEW QUESTION 136

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 137

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-38 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-38 Product From:

<https://www.2passeasy.com/dumps/312-38/>

## Money Back Guarantee

### 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 FirstTry
- \* 312-38 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year