

# EC-Council

## Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)



#### NEW QUESTION 1

John wants to implement a packet filtering firewall in his organization's network. What TCP/IP layer does a packet filtering firewall work on?

- A. Application layer
- B. Network Interface layer
- C. TCP layer
- D. IP layer

**Answer: D**

#### NEW QUESTION 2

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 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

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 8

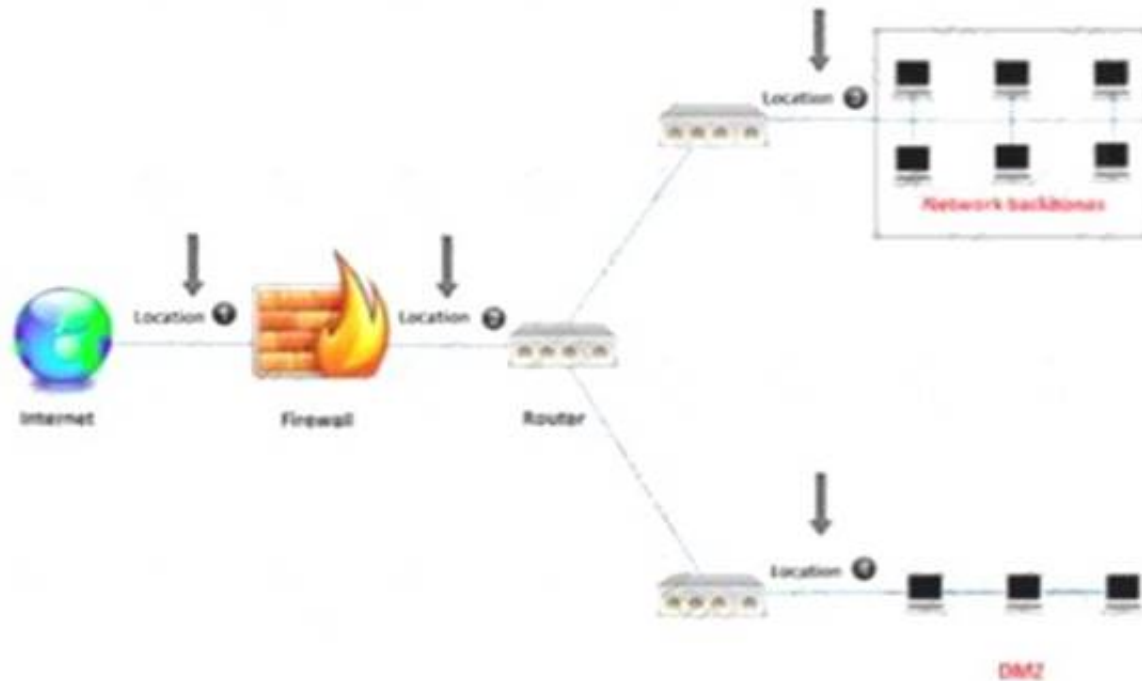
Ross manages 30 employees and only 25 computers in the organization. The network the company uses is a peer-to-peer. Ross configures access control measures allowing the employees to set their own control measures for their files and folders. Which access control did Ross implement?

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

**Answer: A**

#### NEW QUESTION 9

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 10

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 10

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 14

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 18

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 22

-----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 27

You are an IT security consultant working on a contract for a large manufacturing company to audit their entire network. After performing all the tests and building your report, you present a number of recommendations to the company and what they should implement to become more secure. One recommendation is to install a network-based device that notifies IT employees whenever malicious or questionable traffic is found. From your talks with the company, you know that they do not want a device that actually drops traffic completely, they only want notification. What type of device are you suggesting?

- A. The best solution to cover the needs of this company would be a HIDS device.
- B. A NIDS device would work best for the company
- C. You are suggesting a NIPS device
- D. A HIPS device would best suite this company

**Answer:** B

#### NEW QUESTION 29

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 32

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 33

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 34

Which IEEE standard does wireless network use?

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

**Answer:** A

#### NEW QUESTION 37

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 38

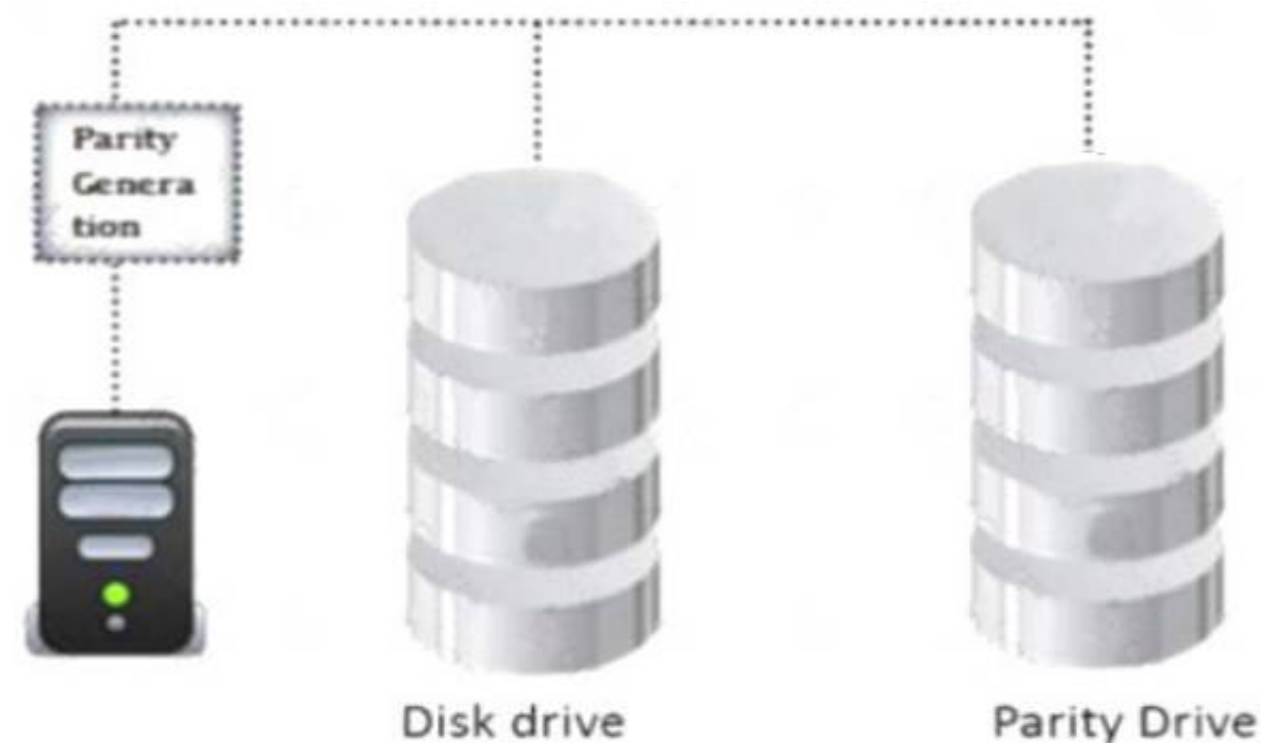
John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information. Which type of firewall service is John thinking of implementing?

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

**Answer:** B

#### NEW QUESTION 42

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



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

**Answer:** B

#### NEW QUESTION 45

A network administrator is monitoring the network traffic with Wireshark. Which of the following filters will she use to view the packets moving without setting a flag to detect TCP Null Scan attempts?

- A. TCRflags==0x000
- B. Tcp.flags==0X029
- C. Tcp.dstport==7
- D. Tcp.flags==0x003

**Answer:** A

#### NEW QUESTION 50

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 53**

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 58**

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 61**

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

**Answer:** C

**NEW QUESTION 67**

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 72**

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 75**

.....

## 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](#)**