



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

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 3

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 4

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 5

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 6

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 7

Which of the following acts as a verifier for the certificate authority?

- A. Certificate Management system
- B. Certificate authority
- C. Directory management system
- D. Registration authority

Answer: D

NEW QUESTION 8

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 9

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 10

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 10

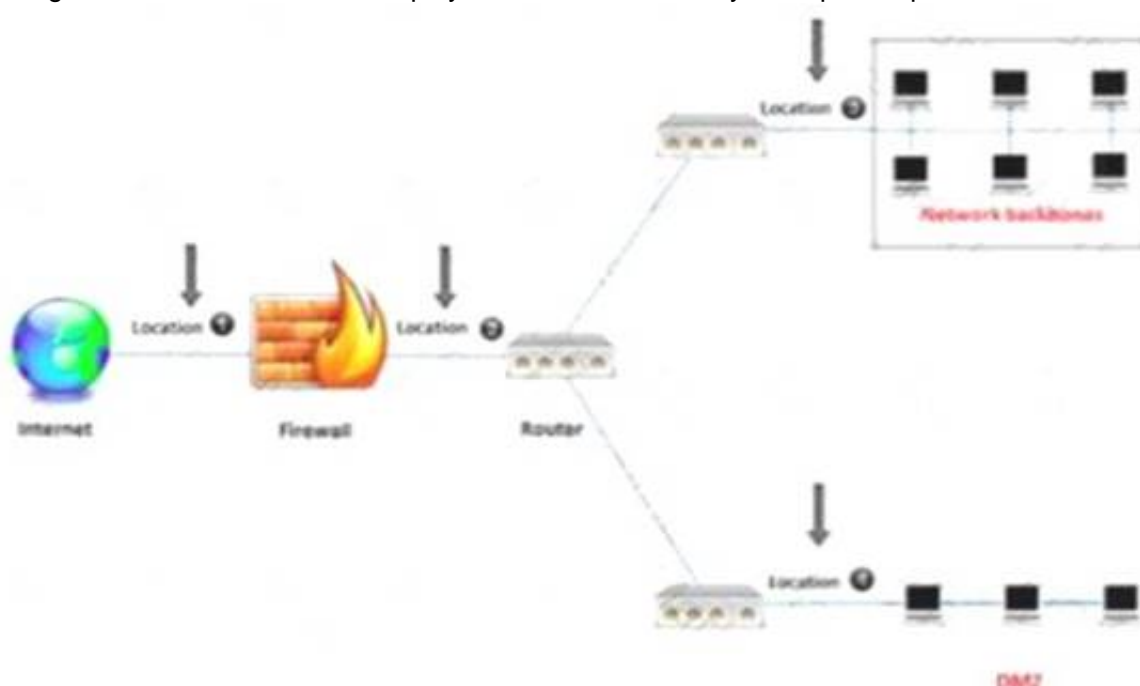
Jason has set a firewall policy that allows only a specific list of network services and deny everything else. This strategy is known as a _____.

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

Answer: B

NEW QUESTION 15

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 20

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 23

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 28

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 33

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 38

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 43

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 47

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

Eric is receiving complaints from employees that their systems are very slow and experiencing odd issues including restarting automatically and frequent system hangs. Upon investigating, he is convinced the systems are infected with a virus that forces systems to shut down automatically after period of time. What type of security incident are the employees a victim of?

- A. Scans and probes
- B. Malicious Code
- C. Denial of service
- D. Distributed denial of service

Answer: B

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 58

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 63

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 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

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 73

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 76

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 80

-----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 82

Consider a scenario consisting of a tree network. The root Node N is connected to two main nodes N1 and N2. N1 is connected to N11 and N12. N2 is connected to N21 and N22. What will happen if any one of the main nodes fail?

- A. Failure of the main node affects all other child nodes at the same level irrespective of the main node.
- B. Does not cause any disturbance to the child nodes or its transmission
- C. Failure of the main node will affect all related child nodes connected to the main node
- D. Affects the root node only

Answer: C

NEW QUESTION 87

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 90

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 95

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 99

Bryson is the IT manager and sole IT employee working for a federal agency in California. The agency was just given a grant and was able to hire on 30 more employees for a new extended project. Because of this, Bryson has hired on two more IT employees to train up and work. Both of his new hires are straight out of college and do not have any practical IT experience. Bryson has spent the last two weeks teaching the new employees the basics of computers, networking, troubleshooting techniques etc. To see how these two new hires are doing, he asks them at what layer of the OSI model do Network Interface Cards (NIC) work

on. What should the new employees answer?

- A. NICs work on the Session layer of the OSI model.
- B. The new employees should say that NICs perform on the Network layer.
- C. They should tell Bryson that NICs perform on the Physical layer
- D. They should answer with the Presentation layer.

Answer: C

NEW QUESTION 100

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 101

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 103

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 107

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 111

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 114

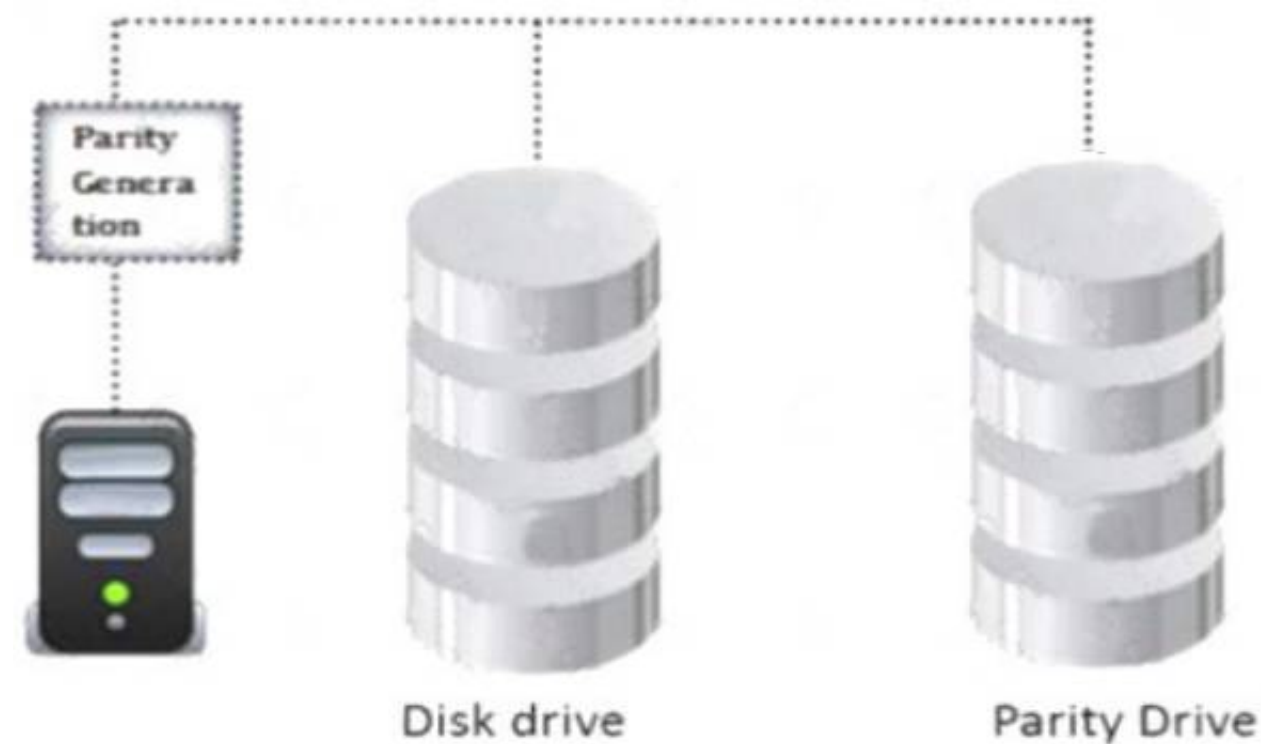
Sean has built a site-to-site VPN architecture between the head office and the branch office of his company. When users in the branch office and head office try to communicate with each other, the traffic is encapsulated. As the traffic passes through the gateway, it is encapsulated again. The header 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 115

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



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

Answer: B

NEW QUESTION 120

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 125

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 130

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 133

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 138

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 142

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 146

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 149

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 154

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 158

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 163

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 166

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 171

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 173

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 175

.....

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](#)