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 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 4
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 5
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 6
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 7
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 seperates the storage units from the servers and the user network.

A. SAN

B. SCSA
C. NAS
D. SAS

Answer: A

NEW QUESTION 8
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 9
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 10
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 10
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 15
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 18
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 19
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. lcmp.type==0 and icmp.type==16
B. lcmp.type==8 or icmp.type==16
C. lcmp.type==8 and icmp.type==0

D. lcmp.type==8 or icmp.type==0

Answer: D

NEW QUESTION 22
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 26
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 29
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 33
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 35
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 36
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 39

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 42
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 46
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 49
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 53
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 54
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 59
----------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 64

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 69
An attacker uses different types of password cracking techniques to crack the password and gain unauthorized access to a system. An attacker uses a file containing a list of commonly used passwords. They then upload this file into the cracking application that runs against the user accounts. Which of the following password cracking techniques is the attacker trying?

A. Bruteforce
B. Rainbow table
C. Hybrid
D. Dictionary

Answer: D

NEW QUESTION 73
Consider a scenario consisting of a tree network. The root Node N is connected to two man 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 tranmission
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 76
A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other f unction(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 79
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 84
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 87
Which IEEE standard does wireless network use?

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

Answer: A

NEW QUESTION 89
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 92
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 93
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 though 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 94
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 95
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 97
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 101
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 105
Identify the password cracking attempt involving precomputed hash values stored as plaintext and using these to crack the password.

A. Bruteforce
B. Rainbow table
C. Dictionary
D. Hybrid

Answer: B

NEW QUESTION 110
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 115
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 116
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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 FirstTry

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