

Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

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



NEW QUESTION 1

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 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

According to the company's security policy, all access to any network resources must use Windows Active Directory Authentication. A Linux server was recently installed to run virtual servers and it is not using Windows Authentication. What needs to happen to force this server to use Windows Authentication?

- A. Edit the ADLIN file.
- B. Edit the shadow file.
- C. Remove the /var/bin/localauth.conf file.
- D. Edit the PAM file to enforce Windows Authentication

Answer: D

NEW QUESTION 4

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 5

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 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

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 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

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 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

Management wants to calculate the risk factor for their organization. Kevin, a network administrator in the organization knows how to calculate the risk factor.

Certain parameters are required before calculating risk factor. What are they? (Select all that apply) Risk factor =.....X.....X.....

- A. Vulnerability
- B. Impact
- C. Attack
- D. Threat

Answer: ABD

NEW QUESTION 14

Identify the spread spectrum technique that multiplies the original data signal with a pseudo random noise spreading code.

- A. FHSS
- B. DSSS
- C. OFDM
- D. ISM

Answer: B

NEW QUESTION 16

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 19

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 24

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 25

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 27

-----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 28

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 29

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 34

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 37

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 40

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 45

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 46

During a security awareness program, management was explaining the various reasons which create threats to network security. Which could be a possible threat to network security?

- A. Configuring automatic OS updates
- B. Having a web server in the internal network
- C. Implementing VPN
- D. Patch management

Answer: B

NEW QUESTION 51

-----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 56

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 60

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 61

A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other function(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 62

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 65

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 68

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 70

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 73

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 74

Which of the following network monitoring techniques requires extra monitoring software or hardware?

- A. Non-router based
- B. Switch based
- C. Hub based
- D. Router based

Answer: A

NEW QUESTION 76

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 77

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 78

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 79

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 83

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 88

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 93

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 95

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 99

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 102

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

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 110

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 112

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 115

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 117

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 121

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 126

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 127

.....

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