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
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
The bank where you work has 600 windows computers and 400 Red Hat computers which primarily serve as bank teller consoles. You have created a plan and deployed all the patches to the Windows computers and you are now working on updating the Red Hat computers. What command should you run on the network to update the Red Hat computers, download the security package, force the package installation, and update all currently installed packages?

A. You should run the up2date -d -f -u command
B. You should run the up2data -u command
C. You should run the WSUS -d -f -u command.
D. You should type the sysupdate -d command

Answer: A

NEW QUESTION 6
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 7
Tom works as a network administrator in a multinational organization having branches across North America and Europe. Tom wants to implement a storage technology that can provide centralized data storage and provide free data backup on the server. He should be able to perform data backup and recovery more efficiently with the selected technology. Which of the following storage technologies best suits Tom's requirements?

A. DAS
B. PAS
C. RAID
D. NAS

Answer: D

NEW QUESTION 8
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 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
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. Father restoration
C. Slower than a full backup
D. Faster than a full backup
E. Less expensive than full backup

Answer: AD

NEW QUESTION 10
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 14
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 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 19
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 22
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 26
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 31
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 32
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 36
------------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 38
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 39

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 43

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 44

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 48

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 52

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 54

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 57

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 60

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 65
Which IEEE standard does wireless network use?

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

Answer: A

NEW QUESTION 68
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 73
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 77
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
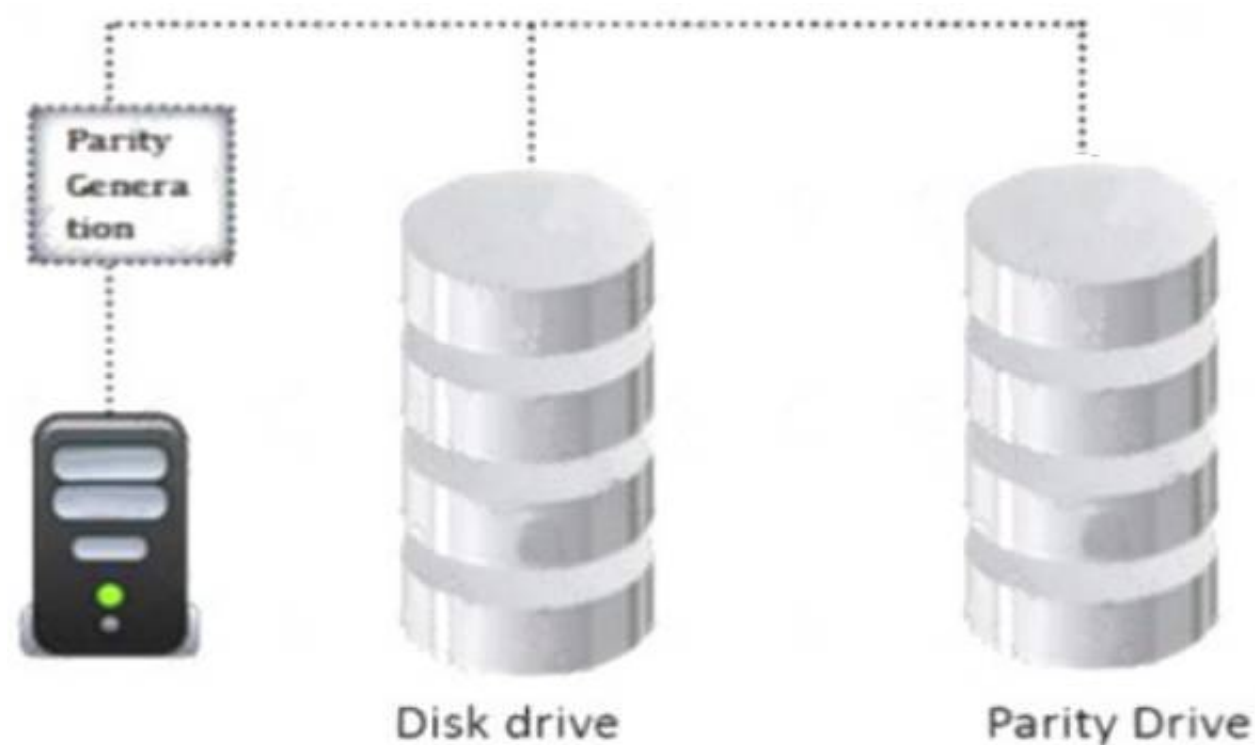
Answer: ACD

NEW QUESTION 78
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 81
Identify the minimum number of drives required to setup RAID level 5.

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

Answer: B

NEW QUESTION 85
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 88
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 93
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 98
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 99

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 101
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 104
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 106
......

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

100% Actual & Verified — Instant Download, Please Click
Order The 312-38 Practice Test Here