

# EC-Council

## Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)



#### 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

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 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

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 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

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 7

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 8

James wants to implement certain control measures to prevent denial-of-service attacks against the organization. Which of the following control measures can help James?

- A. Strong passwords
- B. Reduce the sessions time-out duration for the connection attempts
- C. A honeypot in DMZ
- D. Provide network-based anti-virus

**Answer:** B

#### NEW QUESTION 9

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

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 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 13

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 18

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 20

-----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 24**

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 26**

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 27**

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 32**

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 36**

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 37**

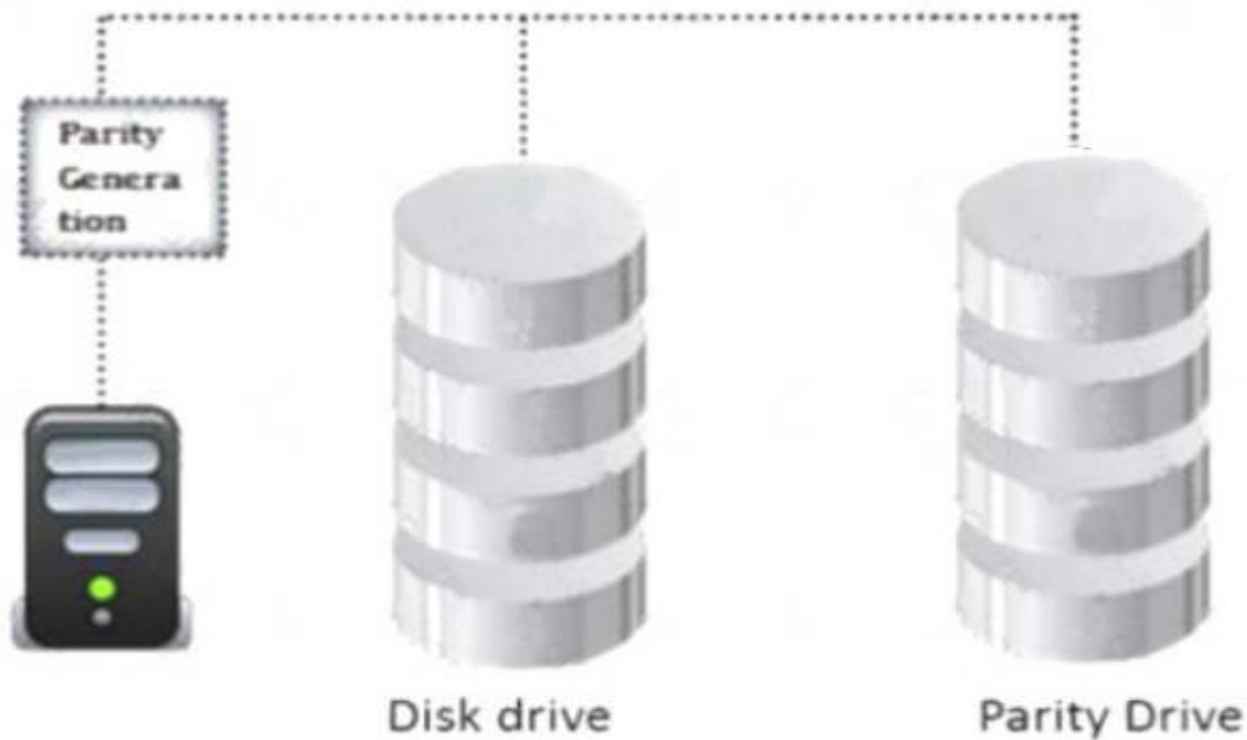
Which of the following network monitoring techniques requires extra monitoring software or hardware?

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

**Answer:** A

**NEW QUESTION 38**

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



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

**Answer: B**

**NEW QUESTION 42**

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 44**

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 48**

Management decides to implement a risk management system to reduce and maintain the organization's risk at an acceptable level. Which of the following is the correct order in the risk management phase?

- A. Risk Identification, Risk Assessment, Risk Treatment, Risk Monitoring & Review
- B. Risk Treatment, Risk Monitoring & Review, Risk Identification, Risk Assessment
- C. Risk Assessment, Risk Treatment, Risk Monitoring & Review, Risk Identification
- D. Risk Identification
- E. Risk Assessment
- F. Risk Monitoring & Review, Risk Treatment

**Answer: A**

**NEW QUESTION 51**

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 52**

Justine has been tasked by her supervisor to ensure that the company's physical security is on the same level as their logical security measures. She installs video cameras at all entrances and exits and installs badge access points for all doors. The last item she wants to install is a method to prevent unauthorized people piggybacking employees. What should she install to prevent piggybacking?

- A. She should install a mantrap
- B. Justine needs to install a biometrics station at each entrance
- C. Justine will need to install a revolving security door
- D. She should install a Thompson Trapdoor.

**Answer:** A

#### NEW QUESTION 54

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 56

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 57

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 61

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 62

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 63

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 65

.....

## 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](#)**