

# 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

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

Daniel is giving training on designing and implementing a security policy in the organization. He is explaining the hierarchy of the security policy which demonstrates how policies are drafted, designed and implemented. What is the correct hierarchy for a security policy implementation?

- A. Laws, Policies, Regulations, Procedures and Standards
- B. Regulations, Policies, Laws, Standards and Procedures
- C. Laws, Regulations, Policies, Standards and Procedures
- D. Procedures, Policies, Laws, Standards and Regulations

**Answer: C**

#### 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

A company has the right to monitor the activities of their employees on different information systems according to the \_\_\_\_\_ policy.

- A. Information system
- B. User access control
- C. Internet usage
- D. Confidential data

**Answer: B**

#### NEW QUESTION 6

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 7

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 8

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 9

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 10

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 10

Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the data. Which RAID level is used here?

- A. RAID 3
- B. RAID 1
- C. RAID 5
- D. RAID 0

**Answer: B**

#### NEW QUESTION 12

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 14

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 17

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 20**

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 24**

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 27**

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 29**

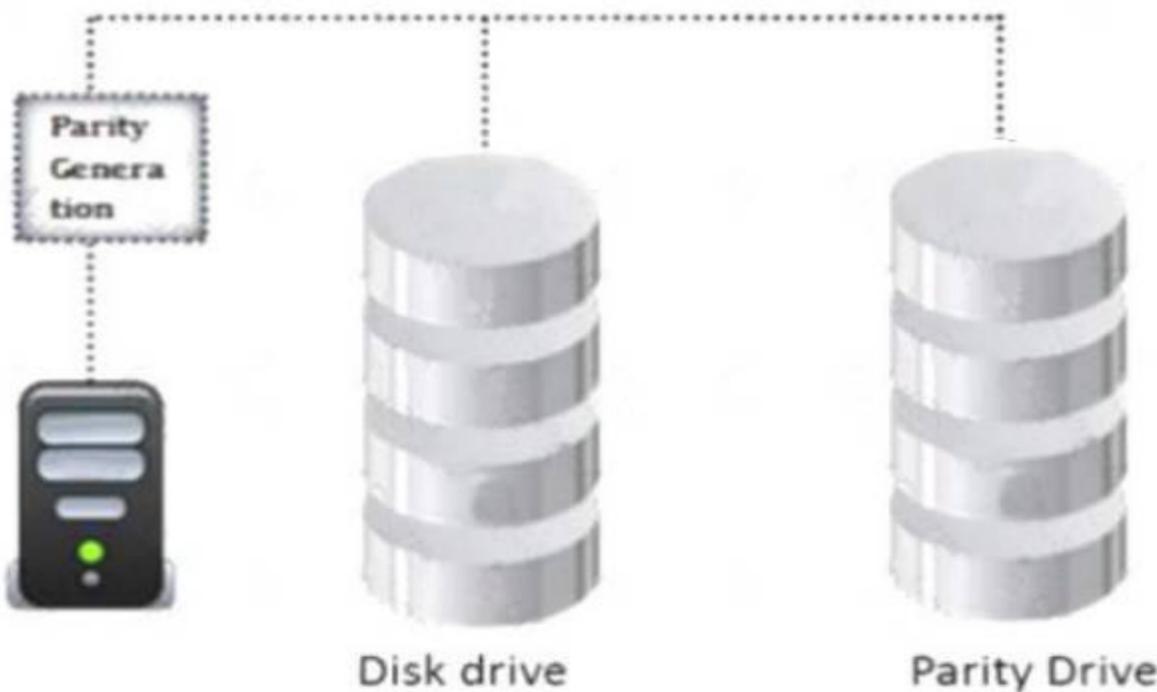
John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a \_\_\_\_\_ and it has to adhere to the \_\_\_\_\_

- A. Verification, Security Policies
- B. Mitigation, Security policies
- C. Vulnerability scanning, Risk Analysis
- D. Risk analysis, Risk matrix

Answer: A

**NEW QUESTION 30**

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



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

Answer: B

#### NEW QUESTION 34

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 36

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 41

Lyle is the IT director for a medium-sized food service supply company in Nebraska. Lyle's company employs over 300 workers, half of which use computers. He recently came back from a security training seminar on logical security. He now wants to ensure his company is as secure as possible. Lyle has many network nodes and workstation nodes across the network. He does not have much time for implementing a network-wide solution. He is primarily concerned about preventing any external attacks on the network by using a solution that can drop packets if they are found to be malicious. Lyle also wants this solution to be easy to implement and be network-wide. What type of solution would be best for Lyle?

- A. A NEPT implementation would be the best choice.
- B. To better serve the security needs of his company, Lyle should use a HIDS system.
- C. Lyle would be best suited if he chose a NIPS implementation
- D. He should choose a HIPS solution, as this is best suited to his needs.

Answer: C

#### NEW QUESTION 43

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 47

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 50

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 55

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 56**

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 58**

.....

## **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](#)**