

# EC-Council

## Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)



#### NEW QUESTION 1

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 2

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 3

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 4

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 separates the storage units from the servers and the user network.

- A. SAN
- B. SCSA
- C. NAS
- D. SAS

**Answer: A**

#### 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

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. Faster restoration
- C. Slower than a full backup
- D. Faster than a full backup
- E. Less expensive than full backup

**Answer: AD**

#### NEW QUESTION 7

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 8**

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 9**

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 10**

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**

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 11**

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 15**

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 17**

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 21

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 25

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 30

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 33

-----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 36

Dan and Alex are business partners working together. Their Business-Partner Policy states that they should encrypt their emails before sending to each other. How will they ensure the authenticity of their emails?

- A. Dan will use his public key to encrypt his mails while Alex will use Dan's digital signature to verify the authenticity of the mails.
- B. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.
- C. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.
- D. Dan will use his digital signature to sign his mails while Alex will use Dan's public key to verify the authenticity of the mails.

**Answer:** D

#### NEW QUESTION 41

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 44

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 48**

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 53**

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 56**

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 60**

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 65**

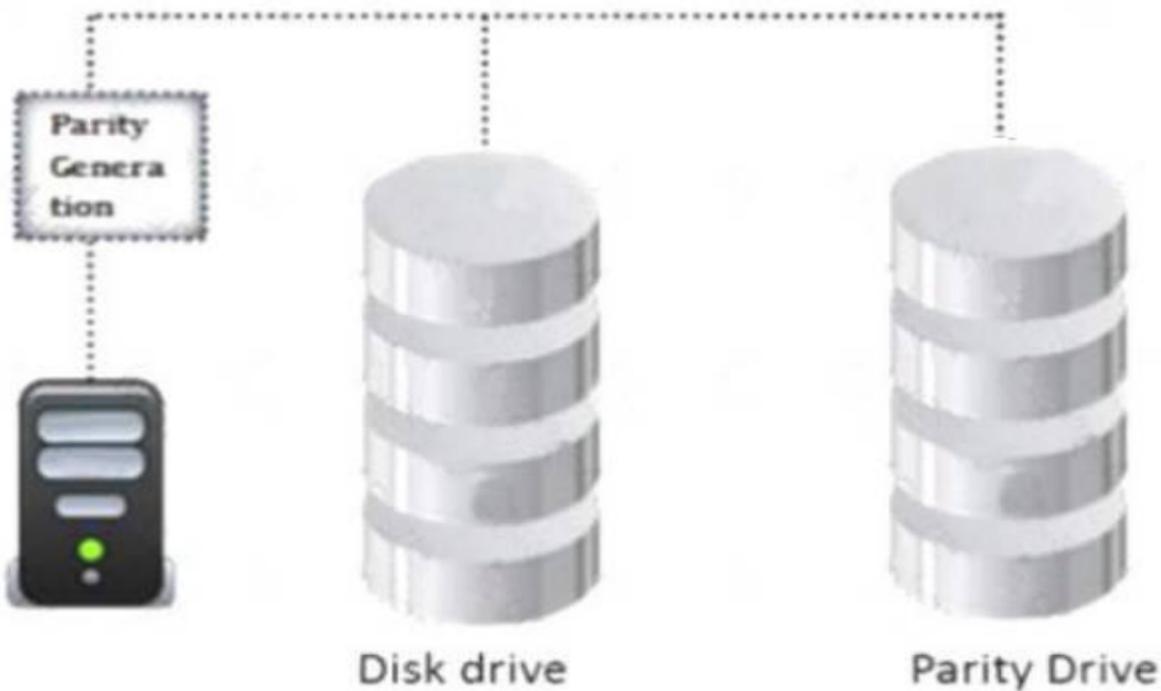
Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she 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 66**

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



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

Answer: B

**NEW QUESTION 71**

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 74**

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 79**

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 84**

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 85**

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 88**

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 89**

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 93**

An organization needs to adhere to the \_\_\_\_\_ rules for safeguarding and protecting the electronically stored health information of employees.

- A. HI PA A
- B. PCI DSS
- C. ISEC
- D. SOX

**Answer: A**

**NEW QUESTION 98**

.....

## **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](#)**