
# EC-Council

## Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

**NEW QUESTION 1**
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 2**
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 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**
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. Usability
B. Data Integrity
C. Availability
D. Confidentiality

**Answer:** B

**NEW QUESTION 5**
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 6**
If there is a fire incident caused by an electrical appliance short-circuit, which fire suppressant should be used to control it?

A. Water
B. Wet chemical
C. Dry chemical
D. Raw chemical

**Answer:** C

**NEW QUESTION 7**
George was conducting a recovery drill test as a part of his network operation. Recovery drill tests are conducted on the _____.

A. Archived data
B. Deleted data

C. Data in transit
D. Backup data

**Answer:** D

**NEW QUESTION 8**
John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network. Which of the following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt?

A. Tcp.flags==0x2b
B. Tcp.flags=0x00
C. Tcp.options.mss_val<1460
D. Tcp.options.wscale_val==20

**Answer:** ABC

**NEW QUESTION 9**
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 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 10**
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 11**
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 13**
Geon Solutions INC., had only 10 employees when it started. But as business grew, the organization had to increase the amount of staff. The network administrator is finding it difficult to accommodate an increasing number of employees in the existing network topology. So the organization is planning to implement a new topology where it will be easy to accommodate an increasing number of employees. Which network topology will help the administrator solve the problem of needing to add new employees and expand?

A. Bus
B. Star
C. Ring
D. Mesh

**Answer:** B

**NEW QUESTION 14**
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 18**
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 23**
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 25**
A company wants to implement a data backup method which allows them to encrypt the data ensuring its security as well as access at any time and from any location. What is the appropriate backup method that should be implemented?

A. Onsite backup
B. Hot site backup
C. Offsite backup
D. Cloud backup

**Answer:** D

**NEW QUESTION 29**
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 34**
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 38**
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 43**

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 44**
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 48**
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 49**
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 54**
Brendan wants to implement a hardware based RAID system in his network. He is thinking of choosing a suitable RAM type for the architectural setup in the system. The type he is interested in provides access times of up to 20 ns. Which type of RAM will he select for his RAID system?

A. NVRAM
B. SDRAM
C. NAND flash memory
D. SRAM

**Answer:** D

**NEW QUESTION 59**
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 61**
----------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 66**

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 67**
Consider a scenario consisting of a tree network. The root Node N is connected to two man nodes N1 and N2. N1 is connected to N11 and N12. N2 is connected to N21 and N22. What will happen if any one of the main nodes fail?

A. Failure of the main node affects all other child nodes at the same level irrespective of the main node.
B. Does not cause any disturbance to the child nodes or its tranmission
C. Failure of the main node will affect all related child nodes connected to the main node
D. Affects the root node only

**Answer:** C

**NEW QUESTION 69**
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 71**
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 76**
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 81**
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 84**
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 88**
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 89**
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 93**
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 95**
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 98**
Michael decides to view the----------to track employee actions on the organization's network.

A. Firewall policy
B. Firewall log
C. Firewall settings
D. Firewall rule set

**Answer:** B

**NEW QUESTION 101**
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 106**
Identify the minimum number of drives required to setup RAID level 5.

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

**Answer:** B

**NEW QUESTION 110**
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 115**
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 Identificatio
E. Risk Assessmen
F. Risk Monitoring & Review, Risk Treatment

**Answer:** A

**NEW QUESTION 120**
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 125**
Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A. Automated Field Correlation
B. Field-Based Approach
C. Rule-Based Approach
D. Graph-Based Approach

**Answer:** A

**NEW QUESTION 128**
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 131**
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 133**

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 134**
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 135**
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 138**
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 140**
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 142**
Steven's company has recently grown from 5 employees to over 50. Every workstation has a public IP address and navigated to the Internet with little to no protection. Steven wants to use a firewall. He also wants IP addresses to be private addresses, to prevent public Internet devices direct access to them. What should Steven implement on the firewall to ensure this happens?

A. Steven should use a Demilitarized Zone (DMZ)
B. Steven should use Open Shortest Path First (OSPF)
C. Steven should use IPsec
D. Steven should enabled Network Address Translation(NAT)

**Answer:** D

**NEW QUESTION 143**
Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered. What tool could Simon and his administrators implement to accomplish this?

A. Snort is the best tool for their situation
B. They can implement Wireshark

C. They could use Tripwire
D. They need to use Nessus

**Answer:** C

**NEW QUESTION 146**
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 150**
.....

# 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