



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 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 4

Daniel is monitoring network traffic with the help of a network monitoring tool to detect any abnormalities. What type of network security approach is Daniel adopting?

- A. Preventative
- B. Reactive
- C. Retrospective
- D. Defense-in-depth

Answer: B

NEW QUESTION 5

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 6

Sam wants to implement a network-based IDS in the network. Sam finds out the one IDS solution which works is based on patterns matching. Which type of network-based IDS is Sam implementing?

- A. Behavior-based IDS
- B. Anomaly-based IDS
- C. Stateful protocol analysis
- D. Signature-based IDS

Answer: D

NEW QUESTION 7

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 8

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 9

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 10

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 10

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 14

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 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 20

James is working as a Network Administrator in a reputed company situated in California. He is monitoring his network traffic with the help of Wireshark. He wants to check and analyze the traffic against a PING sweep attack. Which of the following Wireshark filters will he use?

- A. `icmp.type==0 and icmp.type==16`

- B. icmp.type==8 or icmp.type==16
- C. icmp.type==8 and icmp.type==0
- D. icmp.type==8 or icmp.type==0

Answer: D

NEW QUESTION 23

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 25

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 26

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 30

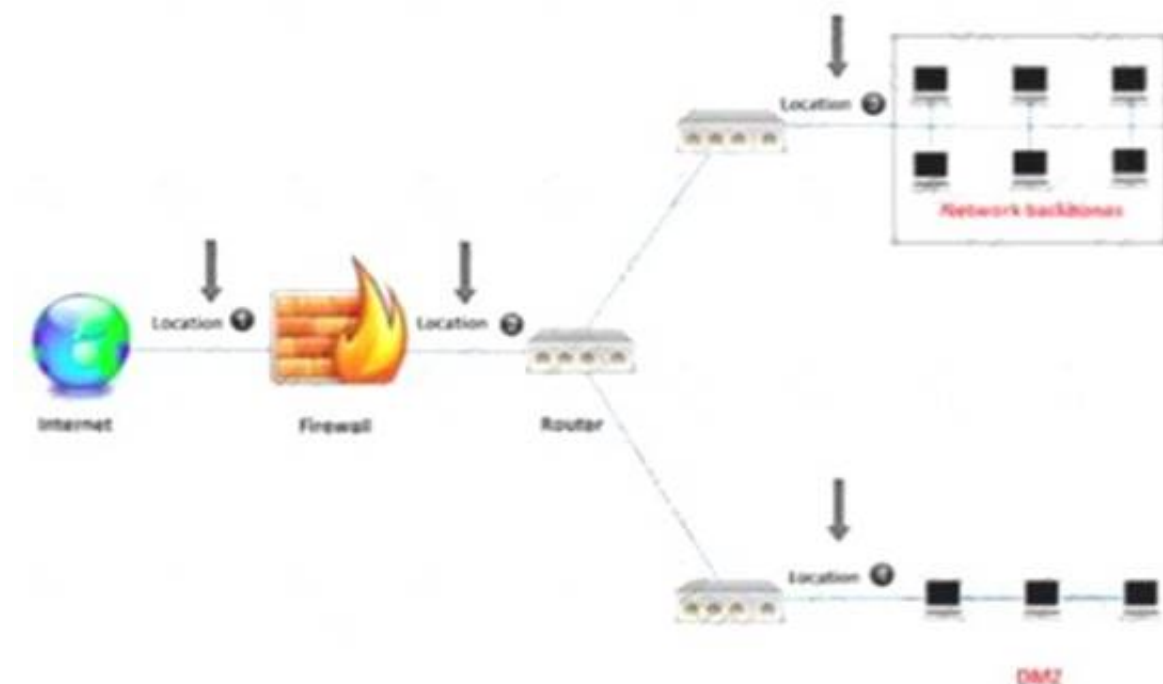
An US-based organization decided to implement a RAID storage technology for their data backup plan. John wants to setup a RAID level that require a minimum of six drives but will meet high fault tolerance and with a high speed for the data read and write operations. What RAID level is John considering to meet this requirement?

- A. RAID level 1
- B. RAID level 10
- C. RAID level 5
- D. RAID level 50

Answer: D

NEW QUESTION 35

An administrator wants to monitor and inspect large amounts of traffic and detect unauthorized attempts from inside the organization, with the help of an IDS. They are not able to recognize the exact location to deploy the IDS sensor. Can you help him spot the location where the IDS sensor should be placed?



- A. Location 2
- B. Location 3
- C. Location 4
- D. Location 1

Answer: A

NEW QUESTION 39

The IR team and the network administrator have successfully handled a malware incident on the network. The team is now preparing countermeasure guideline to avoid a future occurrence of the malware incident.

Which of the following countermeasure(s) should be added to deal with future malware incidents? (Select all that apply)

- A. Complying with the company's security policies
- B. Implementing strong authentication schemes
- C. Implementing a strong password policy
- D. Install antivirus software

Answer: D

NEW QUESTION 42

Larry is responsible for the company's network consisting of 300 workstations and 25 servers. After using a hosted email service for a year, the company wants to control the email internally. Larry likes this idea because it will give him more control over the email. Larry wants to purchase a server for email but does not want the server to be on the internal network due to the potential to cause security risks. He decides to place the server outside of the company's internal firewall. There is another firewall connected directly to the Internet that will protect traffic from accessing the email server. The server will be placed between the two firewalls. What logical area is Larry putting the new email server into?

- A. He is going to place the server in a Demilitarized Zone (DMZ)
- B. He will put the email server in an IPsec zone.
- C. Larry is going to put the email server in a hot-server zone.
- D. For security reasons, Larry is going to place the email server in the company's Logical Buffer Zone (LBZ).

Answer: A

NEW QUESTION 45

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. What is the last step he should list?

- A. Assign eradication.
- B. Recovery
- C. Containment
- D. A follow-up.

Answer: D

NEW QUESTION 46

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 48

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 53

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 55

James is a network administrator working at a student loan company in Minnesota. This company processes over 20,000 student loans a year from colleges all over the state. Most communication between the company schools, and lenders is carried out through emails. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, James wants to utilize email encryption. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt emails. What should James use?

- A. James could use PGP as a free option for encrypting the company's emails.
- B. James should utilize the free OTP software package.
- C. James can use MD5 algorithm to encrypt all the emails
- D. James can enforce mandatory HTTPS in the email clients to encrypt emails

Answer: A

NEW QUESTION 59

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 61

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 64

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 67

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 72

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 75

-----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 79

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 84

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. Brute force
- B. Rainbow table
- C. Hybrid
- D. Dictionary

Answer: D

NEW QUESTION 86

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 89

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 92

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 97

Which IEEE standard does wireless network use?

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

Answer: A

NEW QUESTION 101

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 105

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. What is the last step he should list?

- A. Containment
- B. Assign eradication
- C. A follow-up
- D. Recovery

Answer: C

NEW QUESTION 109

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 111

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 through 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 114

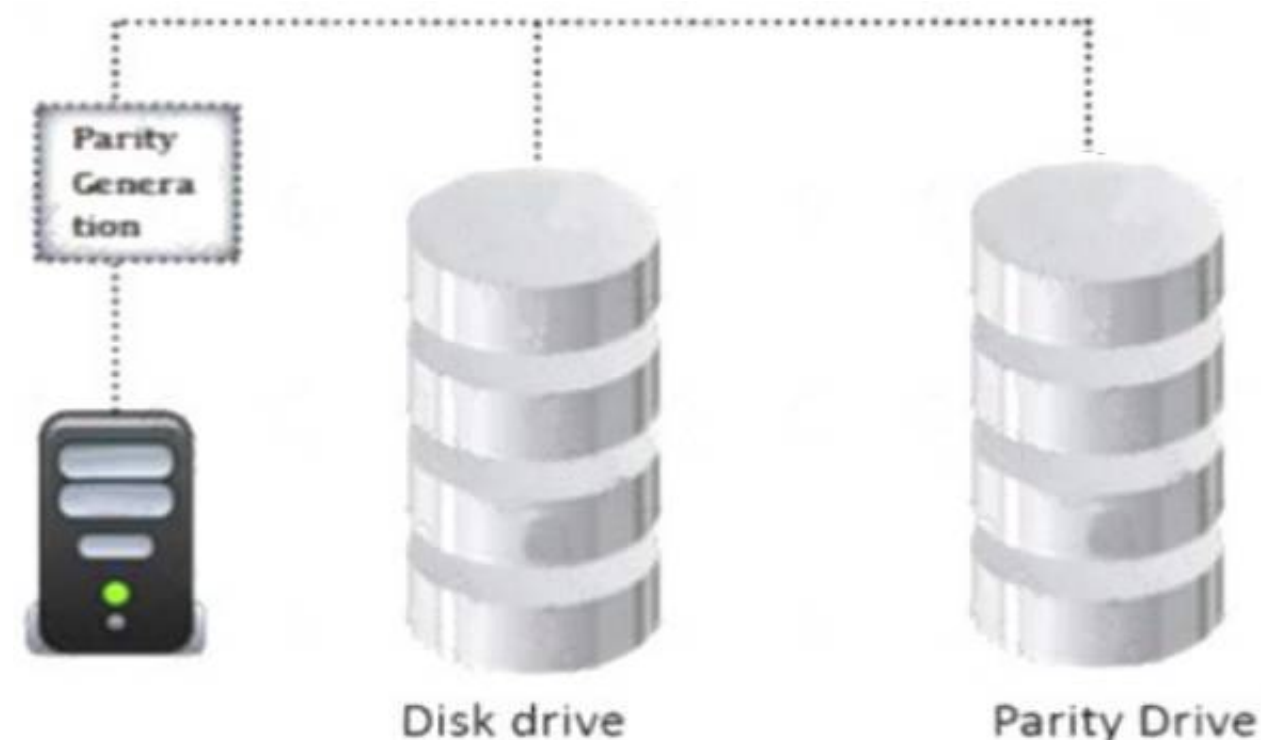
If a network is at risk from unskilled individuals, what type of threat is this?

- A. External Threats
- B. Structured Threats
- C. Unstructured Threats
- D. Internal Threats

Answer: C

NEW QUESTION 116

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



- A. Multiple
- B. 3

- C. 4
- D. 2

Answer: B

NEW QUESTION 119

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 120

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 123

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 125

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 127

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 129

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

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 135

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 136

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 137

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 141

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 144

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 147

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 enable Network Address Translation(NAT)

Answer: D

NEW QUESTION 148

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

- A. HIPAA
- B. PCI DSS
- C. ISEC
- D. SOX

Answer: A

NEW QUESTION 150

Frank installed Wireshark at all ingress points in the network. Looking at the logs he notices an odd packet source. The odd source has an address of 1080:0:FF:0:8:800:200C:4171 and is using port 21. What does this source address signify?

- A. This address means that the source is using an IPv6 address and is spoofed and signifies an IPv4 address of 127.0.0.1.
- B. This source address is IPv6 and translates as 13.1.68.3
- C. This source address signifies that the originator is using 802dot1x to try and penetrate into Frank's network
- D. This means that the source is using IPv4

Answer: D

NEW QUESTION 155

.....

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](#)