Product Questions: 346
Version: 12.1

Question: 1

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. Risk Assessment. Risk Monitoring & Review, Risk Treatment

Answer: A

Explanation:

The correct order in the risk management phase starts with Risk Identification, where potential business risks are determined. This is followed by Risk Assessment, which involves analyzing and prioritizing the identified risks. Next is Risk Treatment, where plans are made to mitigate the risks. Finally, Risk Monitoring & Review is conducted to oversee the risk management process and make necessary adjustments. This sequence ensures a structured and effective approach to managing risks within an organization. Reference: The sequence aligns with the widely recognized ISO 31000 risk management standard, which outlines these core steps in managing risks123.

Question: 2

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

Explanation:

Network Address Translation (NAT) is a network function that translates private IP addresses into a public IP address. This technique restricts the number of public IP addresses required by an organization, as multiple devices on a private network can share a single public IP address. NAT also enhances firewall filtering techniques by hiding the internal IP addresses from the external network, which adds a layer of security by making it more difficult for attackers to target specific devices within the organization's network. It is a common practice in network security to use NAT in conjunction with firewalls to manage the traffic entering and leaving the network, ensuring that only authorized access is permitted.
Reference: The information provided aligns with the Certified Network Defender (CND) program's focus on network defense fundamentals, including the application of network security controls like NAT12. Additionally, NAT's role in conserving IP addresses and providing security by hiding internal network addresses is well-documented and is part of the network security best practices345.

Question: 3

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: B

Explanation:

In Ubuntu, to terminate a specific process, you would use the kill command followed by the signal you want to send and the Process ID (PID) of the target process. The -9 signal is the SIGKILL signal, which forcefully terminates the process. The correct syntax is kill -9 [PID], where [PID] is replaced with the actual numerical ID of the process you wish to terminate.
Reference: This information is consistent with standard Linux documentation and practices as well as the Certified Network Defender (CND) course material, which covers system administration and security tasks including process management. The kill command is a fundamental tool for process management in Unix-like operating systems, which is covered in the CND curriculum.

Question: 4

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

Explanation:

In a tree network, each node is connected in a hierarchical manner, with the root node at the top. If a main node (such as N1 or N2) fails, all the child nodes connected to it (N11, N12 for N1 and N21, N22 for N2) will be affected because the tree structure relies on the connectivity of the parent node to its children. The failure of a main node will disrupt the transmission path from the root to the child nodes, leading to a loss of connectivity for those child nodes. This is consistent with the principles of network resilience and fault tolerance as outlined in the EC-Council's Certified Network Defender (CND) program, which emphasizes the importance of each node in maintaining the network's overall integrity.
Reference: The explanation is based on the standard network topologies and fault tolerance principles covered in the EC-Council's Certified Network Defender (CND) curriculum.

Question: 5

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

Explanation:

Stephanie is working on ensuring data integrity for her company's email communications. Data integrity refers to the assurance that data has not been altered or tampered with during transit. By setting up encryption, Stephanie is ensuring confidentiality, which protects the contents of the email from being read by unauthorized parties. However, to ensure that the emails have not been modified, she is implementing digital signatures. Digital signatures provide a means to verify the authenticity of the sender and to ensure that the message has not been changed, which directly relates to the concept of data integrity in cybersecurity.
Reference: The information aligns with the objectives and documents of the EC-Council's Certified Network Defender (CND) program, which emphasizes the importance of protecting data integrity through measures like digital signatures as part of a defense-in-depth security strategy1.

Question: 6

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

Explanation:

The best option for 24-hour monitoring of the physical perimeter and entrance doors is to install a CCTV system. CCTV cameras serve as both a deterrent to unauthorized entry and a means of surveillance to monitor activities. They can be positioned to cover the entrance doors and the street, providing a broad view of the area that needs to be secured. This aligns with the principles of intrusion detection and prevention, which include deterrence through visible security measures like cameras, and detection through continuous monitoring.
Reference: The information aligns with the core principles of intrusion detection systems, which include deterrence and detection, as outlined in the resources related to Physical Intrusion Detection Systems (PIDS) and Certified Network Defender (CND) training materials12.

Question: 7

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

Explanation:

The symptoms described by the employees, such as systems being very slow, restarting automatically, and experiencing frequent hangs, are indicative of a security incident involving malicious code. Malicious code refers to software or scripts designed to cause harm to a computer system, network, or server. In this case, the virus that forces systems to shut down automatically after a period of time is a type of malicious code. It disrupts the normal functioning of the system, leading to decreased performance and unexpected behavior.
Reference: The classification of this type of security incident aligns with the Certified Network

Defender (CND) curriculum, which includes understanding and identifying various types of security threats, including those caused by viruses and other forms of malicious code12. The CND program emphasizes the importance of recognizing the signs of malware infection, which can include system slowdowns, crashes, and other erratic behaviors that impact system availability and performance1.

Question: 8

----------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

Explanation:

The IEEE 802.16 is a series of wireless broadband standards, also known as WirelessMAN, that are designed for Metropolitan Area Networks (MANs). It specifies the air interface, including the medium access control layer (MAC) and physical layer (PHY), of combined fixed and mobile point-to-multipoint broadband wireless access systems. This standard supports rapid deployment of broadband wireless access systems and encourages competition by providing alternatives to wireline broadband access.
Reference: The information is verified by the IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems1, and further details can be found in the IEEE 802.16 Working Group's documents23.

Question: 9

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: B

Explanation:

Class B IP addresses range from 128.0.0.0 to 191.255.255.255. The first two bits of the first octet in a Class B address are always set to '10', and the default subnet mask is 255.255.0.0. Option B, 18.12.4.1, falls within this range, with the first octet being 18, which is between 128 and 191. Reference: The information is based on the standard IP address classification as per the IPv4 protocol1234.

Question: 10

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

Explanation:

To effectively correlate incidents across various security controls like firewalls and IDS systems, it is essential to ensure that the timestamps of logs and events are synchronized. This is where Network Time Protocol (NTP) comes into play. NTP ensures that all devices on the network are on the same time setting, which is crucial for event correlation. Without synchronized time settings, it would be challenging to establish a timeline of events and understand the sequence in which they occurred, making incident response and forensic analysis more difficult.
Reference: The importance of using NTP for incident correlation is well-documented in network security best practices and is also highlighted in the EC-Council's Certified Network Defender (CND) course materials. The CND course emphasizes the role of NTP in maintaining accurate time stamps across network devices for effective security incident management and analysis.

Question: 11

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: D

Explanation:

When deciding on the appropriate backup medium, the network administrator will consider Reliability as the primary factor. This is because the backup medium must be dependable for restoring data in case of data loss or system failure. The reliability of a backup medium ensures that data can be recovered accurately and completely when needed.
Reference: The importance of reliability in choosing a backup medium is supported by best practices in data backup and recovery, which emphasize the need for a dependable backup solution to ensure data integrity and availability1234.

Question: 12

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: B

Explanation:

Switch-based network monitoring requires additional monitoring software or hardware because switches operate at the data link layer of the OSI model and do not inherently provide monitoring capabilities. To monitor traffic through a switch, network administrators must use port mirroring or a network tap, which involves configuring the switch to send a copy of the network packets to a monitoring device. This allows the monitoring device to analyze the traffic passing through the switch without interfering with the network's normal operation. This technique is essential for deep packet inspection, intrusion detection systems, and for gaining visibility into the traffic between devices in a switched network.
Reference: The need for extra monitoring software or hardware in switch-based network monitoring is consistent with the Certified Network Defender (CND) curriculum, which emphasizes the importance of implementing robust network monitoring practices to detect and respond to security threats12. Additionally, the use of port mirroring and network taps as methods to monitor switch-based networks is a standard practice in network security, aligning with the CND's focus on technical network security measures34.

Question: 13

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

Explanation:

Steven should implement Network Address Translation (NAT) on the firewall to ensure that the IP

addresses of the workstations are private and not directly accessible from the public Internet. NAT translates the private IP addresses of the workstations to a public IP address before they are sent out to the Internet, and vice versa for incoming traffic. This not only hides the internal IP addresses but also allows multiple devices to share a single public IP address, which is essential as the company grows.
Reference: The concept of NAT and its role in protecting internal network resources while allowing Internet access is a fundamental topic covered in the Certified Network Defender (CND) course. It is also a standard practice in network security, aligning with the objectives of ensuring the confidentiality and integrity of network infrastructure.

Question: 14

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: C

Explanation:

In the context of digital certificates, the Registration Authority (RA) is responsible for verifying the identity of entities requesting a certificate before the Certificate Authority (CA) issues it. The RA acts as a verifier for the CA, ensuring that the entity requesting the certificate is who they claim to be. This process is crucial for maintaining trust within a digital environment, as it prevents the issuance of certificates to fraudulent or unauthorized entities.
Reference: The role of the Registration Authority in the verification process is outlined in the EC-Council's Certified Network Defender (CND) curriculum, which covers the essential concepts of network security, including the management and issuance of digital certificates.

Question: 15

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 dat
a.

Which RAID level is used here?
A. RAID 3
B. RAID 1
C. RAID 5
D. RAID 0

Answer: B

Explanation:

The RAID level used here is RAID 1, which is also known as disk mirroring. In this setup, all the data written to one disk is automatically copied to another disk, creating an exact duplicate of the data. This ensures that if one disk fails, the data is still available on the other disk, providing redundancy and protecting against data loss. RAID 1 is a common choice for systems where data availability and integrity are critical.
Reference: This explanation is consistent with the principles outlined in the EC-Council's Certified Network Defender (CND) course materials, which describe RAID 1 as a configuration that duplicates data across multiple disks to ensure redundancy and data availability1.

Question: 16

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: C

Explanation:

As a first responder to a suspected DoS incident, the initial reaction should be to make an initial assessment. This involves quickly evaluating the situation to understand the scope and impact of the incident. An initial assessment helps in determining whether the unusual traffic is indeed a DoS attack or a false positive. It also aids in deciding the next steps, such as whether to escalate the incident, what resources are required, and how to communicate the issue to relevant stakeholders.
Reference: The approach aligns with best practices for incident response, which emphasize the importance of an initial assessment to understand the nature and extent of a security incident before proceeding with further actions123.

Question: 17

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

Explanation:

Unstructured threats typically originate from individuals who lack advanced skills or a sophisticated understanding of network systems. These threats often involve simple methods to disrupt network operations, such as basic malware attacks or exploiting known vulnerabilities that have not been patched. In the context of the Certified Network Defender (CND) program, unstructured threats are recognized as those that can be caused by unskilled individuals who may inadvertently introduce risks to the network through misconfigurations or inadequate security practices.
Reference: The Certified Network Defender (CND) curriculum addresses various types of threats, including unstructured threats, and emphasizes the importance of securing networks against all levels of skill and sophistication among potential attackers12. It also covers the need for continuous monitoring and the implementation of security best practices to mitigate the risks posed by both unstructured and structured threats34.

Question: 18

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

Explanation:

To enforce Windows Active Directory Authentication on a Linux server, the Pluggable Authentication Modules (PAM) configuration files must be edited. PAM provides a way to develop programs that are independent of authentication scheme. These files, located in /etc/pam.d/, dictate how a Linux system handles authentication for various services. To integrate Windows Active Directory with a Linux server, specific PAM modules like pam_krb5 or pam_winbind can be used. These modules allow the Linux system to communicate with the Active Directory server for authentication purposes. The process typically involves installing necessary packages, joining the Linux server to the AD domain, and configuring the PAM files to use AD for authentication.
Reference: The procedure for integrating Linux servers with Windows Active Directory is documented in various Linux administration guides and resources12. Specific steps can also be found in tutorials and official documentation from Linux distributions that support Active Directory integration345.

Question: 19

Kelly is taking backups of the organization's dat
a. 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

Explanation:

An incremental backup is a type of data backup that copies only the files that have been created or modified since the last backup operation of any type. This method is efficient because it only backs up data that has changed, which can save on storage space and reduce the time needed to complete the backup. In Kelly's case, since he is backing up only the new or changed files since the last backup, he is using an incremental backup approach.
Reference: The explanation aligns with the standard backup methodologies where an incremental backup captures only the changes made since the last backup, which can be either a full or another incremental backup1234.

Question: 20

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: C

Explanation:

TCP OS fingerprinting attempts can be identified by analyzing various TCP/IP stack behaviors, one of which is the TCP Maximum Segment Size (MSS). The MSS value indicates the size of the largest segment of TCP data that a device is willing to receive. Different operating systems have different default MSS values, and a value less than 1460 can suggest an OS fingerprinting attempt, as it may indicate that the sender is trying to avoid fragmentation or is probing to discover the OS based on MSS response.
Reference: The use of Wireshark to monitor and analyze network traffic, including identifying TCP OS fingerprinting attempts, is covered in the EC-Council's Certified Network Defender (CND) course. The course materials would include detailed explanations on how to use Wireshark filters to detect such activities, and the reference to MSS values is consistent with standard network analysis practices for identifying OS fingerprinting attempts.

Question: 21

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

Explanation:

The right of a company to monitor the activities of their employees on its information systems is typically defined under the "User Access Control" policy. This policy sets out the rules and conditions under which employee activities can be monitored, ensuring that monitoring is conducted legally and ethically while protecting the privacy rights of employees. It often includes provisions for the monitoring of email, internet use, and other digital interactions to safeguard company assets and ensure compliance with corporate policies.
Reference: The establishment and enforcement of user access control policies are fundamental principles in cybersecurity management and are discussed in Network Defender training materials.

Question: 22

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

Explanation:

IPsec VPN tunnels function at the network layer of the OSI model. This layer is responsible for the logical transmission of data across a network and includes routing through different network paths. IPsec enhances the security at this layer by providing features such as data integrity, encryption, and authentication. These features are crucial for establishing a secure and encrypted connection across the internet, which is essential for VPN tunnels that connect different network segments, such as branch locations to a main office.
Reference: The role of IPsec at the network layer is well-established in network security literature and is consistent with the Certified Network Defender (CND) program's teachings on secure network architecture12. The network layer's involvement in routing and data transmission makes it the appropriate layer for IPsec's operation, aligning with the CND's emphasis on understanding and implementing network security protocols34.

Question: 23

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

Explanation:

The last step Malone should list in his incident handling plan is 'A follow-up'. This step is crucial as it involves analyzing the incident to understand how it occurred and what can be done to prevent similar incidents in the future. It often includes a review of the effectiveness of the response, identification of lessons learned, updating policies and procedures accordingly, and conducting training sessions if necessary. This step ensures that the organization improves its security posture and is better prepared for future incidents.
Reference: The follow-up step is aligned with the incident response life cycle which includes preparation, identification, containment, eradication, recovery, and then follow-up as the final phase. This is consistent with the best practices in incident response and is covered in the Certified Network Defender (CND) curriculum as well as in the NIST guidelines on incident response1.

Question: 24

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

Explanation:

The Pipe Model in VPN QoS is designed to guarantee bandwidth between one customer edge (CE) device to another. This model ensures a fixed amount of bandwidth is reserved for the traffic between these two points, providing a consistent and predictable service level. It is particularly useful in scenarios where a steady and reliable flow of data is critical. The Pipe Model contrasts with the Hose Model, which offers flexible bandwidth allocation based on the total amount of traffic entering and leaving the network, without guaranteeing individual flows between specific CEs.
Reference: This information aligns with the QoS strategies for VPNs that are part of the EC-Council's Certified Network Defender (CND) curriculum, which includes understanding various QoS models and their implications on network traffic1.

Question: 25

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 spoofinq
D. ARP Poisioning

Answer: D

Explanation:

James is analyzing an ARP Poisoning attack. This type of attack occurs when an attacker sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker has inserted their MAC address into the ARP cache of other devices, they can intercept, modify, or stop data in transit, effectively performing a man-in-the-middle or denial of service attack.
Reference: The analysis of ARP packets to identify potential ARP Poisoning is a critical skill for network defenders, as outlined in the EC-Council's Certified Network Defender (CND) course. The course emphasizes understanding and identifying various network threats, including ARP-related attacks, which are fundamental to maintaining network security123.

Question: 26

Alex is administrating the firewall in the organization's network. What command will he use to check the ports applications open?

A. Netstat -an
B. Netstat -o
C. Netstat -a
D. Netstat -ao

Answer: A

Explanation:

The netstat -an command is used to display all active connections and the TCP and UDP ports on which the computer is listening, without resolving the hostnames. This command provides a list that includes both listening ports and established connections, making it a suitable choice for an administrator like Alex to check the ports that applications have opened on a firewall.
Reference: This explanation is based on standard networking practices and the functionality of the netstat command as described in networking and security documentation123.

Question: 27

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

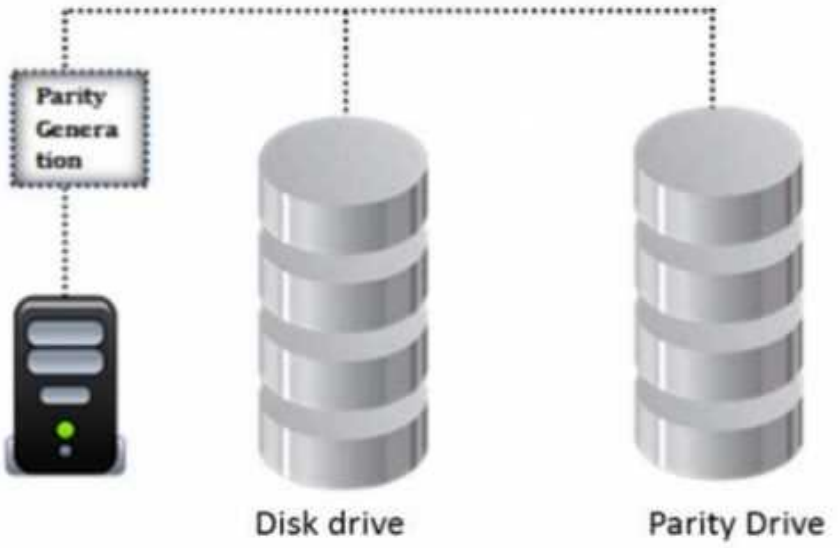
Answer: C

Explanation:

In the context of risk assessment, an incident that has a very high probability of occurring and the potential to impact almost 80% of a business is considered an extreme risk. This categorization is based on the severity of the impact and the likelihood of the event. The risk matrix, a tool used in risk assessment, helps in the classification of risks by considering both the impact and the probability of potential incidents. An event that affects such a significant portion of the business would typically necessitate immediate attention and the implementation of mitigation strategies to prevent substantial loss or damage.
Reference: The Certified Network Defender (CND) curriculum includes principles of risk assessment and the use of risk matrices to categorize and prioritize risks. It outlines that risks with high impact and high probability should be classified as extreme, requiring urgent action12.

Question: 28

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



A. Multiple
B. 3

C. 4
D. 2

Answer: B

Explanation:

RAID level 5 is a robust storage solution that provides fault tolerance and improved read performance. It requires a minimum of three drives to function. This setup allows for data and parity information to be striped across all drives in the array. If one drive fails, the system can use the parity information to reconstruct the lost data, ensuring no data loss occurs. This level of RAID is beneficial for systems where data availability and security are critical, without sacrificing too much storage capacity for parity.
Reference: The minimum number of drives required for RAID level 5 is confirmed by various authoritative sources on RAID technology and storage solutions1234.

Question: 29

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 seperates the storage units from the

servers and the user network.

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

Answer: A

Explanation:

Storage Area Network (SAN), which is a dedicated high-speed network that connects servers to storage devices, allowing for the sharing of storage resources. A SAN is designed to handle large amounts of data and provides a way to centralize storage management, making it an efficient solution for enterprises that require reliable and scalable storage infrastructure. It separates the storage units from the servers and the user network, which aligns with the scenario described for Timothy's organization.
Reference: The concept of a SAN as a dedicated network for sharing storage resources is well-documented and aligns with industry standards and practices1234.

Question: 30

A local bank wants to protect their card holder dat
a. 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

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. It consists of steps that mirror security best practices, including protecting stored cardholder data, maintaining a vulnerability management program, and implementing strong access control measures. For a local bank that wants to protect cardholder data, compliance with PCI DSS is essential to ensure the security of this sensitive information.
Reference: The PCI DSS Quick Reference Guide and other official documents from the PCI Security Standards Council provide comprehensive information on the requirements and best practices for securing cardholder data. These documents are used as references in the EC-Council's Certified Network Defender (CND) course to educate network defenders on the importance of PCI DSS compliance12.

Question: 31

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

Explanation:

Sam is implementing a Signature-based Intrusion Detection System (IDS). This type of IDS uses predefined patterns of traffic, known as signatures, to identify and flag potential security threats. These signatures are based on known attack patterns and anomalies that have been identified from past incidents. When network traffic matches a signature within the IDS, an alert is generated, indicating a possible security event or breach. Signature-based IDS is effective in detecting known threats but may not be as effective in identifying new, previously unknown attacks.
Reference: The information aligns with the Certified Network Defender (CND) objectives and documents, which describe the role and function of signature-based IDS within network security. The CND training materials emphasize the importance of understanding various IDS types, including signature-based systems, which are critical for detecting known threats and maintaining network security1.

Question: 32

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

Explanation:

A circuit level gateway is a type of firewall that operates at the session layer of the OSI model, which is Layer 5. This kind of firewall is designed to provide security by validating and managing sessions without inspecting the actual contents of each packet. It is particularly adept at hiding the private network information because it only allows traffic through that is part of an established session, effectively masking the details of the network's internal structure from the outside. This makes it an ideal choice for John's requirements.
Reference: The information about circuit level gateways operating at the session layer and their ability to hide private network information is supported by multiple sources within the field, including educational resources and security-focused articles123. Additionally, the ECCouncil's Certified Network Defender (CND) program covers the necessary knowledge regarding network security and defense strategies, which includes understanding the functions and applications of different types of firewalls45.

Question: 33

You are an IT security consultant working on a contract for a large manufacturing company to audit their entire network. After performing all the tests and building your report, you present a number of recommendations

to the company and what they should implement to become more secure. One recommendation is to install a network-based device that notifies IT employees whenever malicious or questionable traffic is found. From

your talks with the company, you know that they do not want a device that actually drops traffic completely, they only want notification. What type of device are you suggesting?

A. The best solution to cover the needs of this company would be a HIDS device.
B. A NIDS device would work best for the company
C. You are suggesting a NIPS device
D. A HIPS device would best suite this company

Answer: B

Explanation:

The device suggested is a Network Intrusion Detection System (NIDS). A NIDS monitors network traffic for suspicious activity and alerts the system or network administrator. Unlike a Network

Intrusion Prevention System (NIPS), which actively blocks traffic deemed malicious, a NIDS does not interfere with the flow of traffic, thus fulfilling the company's requirement for a device that only notifies rather than drops traffic.
Reference: The information aligns with the Certified Network Defender (CND) course's focus on network security, which includes understanding and implementing devices that protect, detect, respond, and predict network security incidents. The CND course emphasizes the importance of network traffic monitoring and analysis, which is a key function of a NIDS12.

Question: 34

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: A,

Explanation:

The risk factor for an organization is typically calculated by considering the potential impact of a threat exploiting a vulnerability. The formula often used is Risk = Threat X Vulnerability X Impact. This means that for a risk to exist, there must be a threat that could exploit a vulnerability and cause an impact on the organization. An attack is not a parameter in the risk calculation but rather the act that occurs when a threat exploits a vulnerability.
Reference: The information is based on the principles of risk assessment and management as outlined in the EC-Council's Certified Network Defender (CND) course materials, which emphasize the importance of understanding threats, vulnerabilities, and their potential impact to calculate risk effectively12.

Question: 35

Lyle is the IT director for a medium-sized food service supply company in Nebrask
a. 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