Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

https://www.2passeasy.com/dumps/312-38/

NEW QUESTION 1
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 2
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 3
Chris is a senior network administrator. Chris wants to measure the Key Risk Indicator (KRI) to assess the organization. Why is Chris calculating the KRI for his organization? It helps Chris to:

A. Identifies adverse events
B. Facilitates backward
C. Facilitates post Incident management
D. Notifies when risk has reached threshold levels

Answer: AD

NEW QUESTION 4
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 5
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 6
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

NEW QUESTION 7
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 8
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 9
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. Father restoration
C. Slower than a full backup
D. Faster than a full backup
E. Less expensive than full backup

Answer: AD

NEW QUESTION 10
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 10
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 12
Sam, a network administrator is using Wireshark to monitor the network traffic of the organization. He wants to detect TCP packets with no flag set to check for a specific attack attempt. Which filter will he use to view the traffic?

A. Tcp.flags==0x000
B. Tcp.flags==0000x
C. Tcp.flags==000x0
D. Tcp.flags==x0000

Answer: A

NEW 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: D

NEW QUESTION 15
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 19
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 21
Ross manages 30 employees and only 25 computers in the organization. The network the company uses is a peer-to-peer. Ross configures access control measures allowing the employees to set their own control measures for their files and folders. Which access control did Ross implement?

A. Discretionary access control
B. Mandatory access control
C. Non-discretionary access control
D. Role-based access control

Answer: A

NEW QUESTION 25
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.

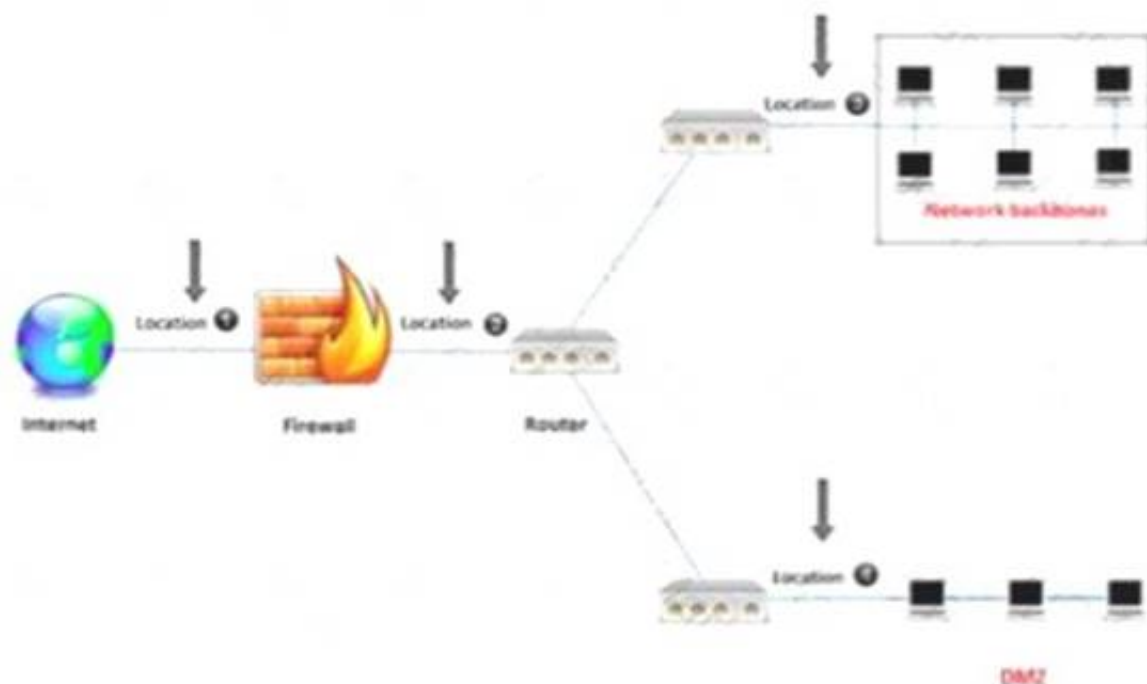**Answer:** B

NEW QUESTION 26
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 28
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 33
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

NEW QUESTION 36
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 39
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 42
------------is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs)

A. 802.15
B. 802.16
C. 802.15.4
D. 802.12

Answer: B

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 47
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 52
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
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 60
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 62
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 64
Rick has implemented several firewalls and IDS systems across his enterprise network. What should he do to effectively correlate all incidents that pass through these security controls?

A. Use firewalls in Network Address Transition (NAT) mode
B. Implement IPsec
C. Implement Simple Network Management Protocol (SNMP)
D. Use Network Time Protocol (NTP)

Answer: D

NEW QUESTION 66
David is working in a mid-sized IT company. Management asks him to suggest a framework that can be used effectively to align the IT goals to the business goals of the company. David suggests the _____ framework, as it provides a set of controls over IT and consolidates them to form a framework.

A. RMIS
B. ITIL
C. ISO 27007
D. COBIT

Answer: D

NEW QUESTION 67

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 69
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. Bruteforce
B. Rainbow table
C. Hybrid
D. Dictionary

Answer: D

NEW QUESTION 71
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 authencity of the mails.

Answer: D

NEW QUESTION 76
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 80
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 83
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 88
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 91
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 95
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 99
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 100
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
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 108
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 111
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
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 117
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 122
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 124
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 127
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 128
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 130
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 134
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 138
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 140
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 143
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 148
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 153
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-38 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-38 Product From:

https://www.2passeasy.com/dumps/312-38/

Money Back Guarantee

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