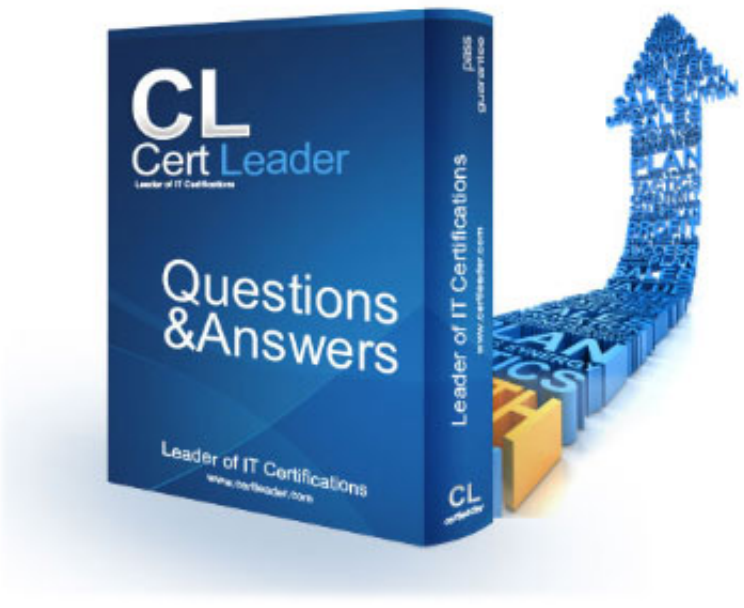
312-38 Dumps

EC-Council Network Security Administrator (ENSA)

https://www.certleader.com/312-38-dumps.html



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
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 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
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 6
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 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 15
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 18
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 19
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 22
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 26
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 27
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 28
----------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 30
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 35
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 38
Henry needs to design a backup strategy for the organization with no service level downtime. Which backup method will he select?

A. Normal backup
B. Warm backup
C. Hot backup
D. Cold backup

Answer: C

NEW QUESTION 42
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 47
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 50
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 53
----------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 55
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 57
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 59
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 61
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 64
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 67
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 72
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 75
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 79
Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session. She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?

A. The type of scan she is usinq is called a NULL scan.
B. Cindy is using a half-open scan to find live hosts on her network.
C. Cindy is attempting to find live hosts on her company's network by using a XMAS scan.
D. She is utilizing a RST scan to find live hosts that are listening on her network.

Answer: B

NEW QUESTION 82
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 85
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 88
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 89
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 90
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 93
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

NEW QUESTION 98

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 103
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 108
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: A

NEW QUESTION 109
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 113
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 115
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 118
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 120
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-38 Exam with Our Prep Materials Via below:

https://www.certleader.com/312-38-dumps.html