Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

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

NEW QUESTION 1
Identify the correct statements regarding a DMZ zone:

A. It is a file integrity monitoring mechanism
B. It is a Neutral zone between a trusted network and an untrusted network
C. It serves as a proxy
D. It includes sensitive internal servers such as database servers

Answer: B

NEW QUESTION 2
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 3
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 4
Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user's email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures. What is Stephanie working on?

A. Usability
B. Data Integrity
C. Availability
D. Confidentiality

Answer: B

NEW QUESTION 5
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
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 7
Kyle, a front office executive, suspects that a Trojan has infected his computer. What should be his first course of action to deal with the incident?

A. Contain the damage
B. Disconnect the five infected devices from the network
C. Inform the IRT about the incident and wait for their response
D. Inform everybody in the organization about the attack

Answer: C

NEW QUESTION 8
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 9
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 10
What is the name of the authority that verifies the certificate authority in digital certificates?

A. Directory management system
B. Certificate authority
C. Registration authority
D. Certificate Management system

Answer: D

NEW QUESTION 10
Management wants to calculate the risk factor for their organization. Kevin, a network administrator in the organization knows how to calculate the risk factor. Certain parameters are required before calculating risk factor. What are they? (Select all that apply) Risk factor =.....X.....X.....

A. Vulnerability
B. Impact
C. Attack
D. Threat

Answer: ABD

NEW QUESTION 14
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
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 21
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 24
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 26
Harry has sued the company claiming they made his personal information public on a social networking site in the United States. The company denies the allegations and consulted a/an _____ for legal advice to defend
them against this allegation.

A. PR Specialist
B. Attorney
C. Incident Handler
D. Evidence Manager

Answer: B

NEW QUESTION 29
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 30
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 35
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 39
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 40

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 42
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 46
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 48
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 53
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 58
Paul is a network security technician working on a contract for a laptop manufacturing company in Chicago. He has focused primarily on securing network devices, firewalls, and traffic traversing in and out of the network. He just finished setting up a server a gateway between the internal private network and the outside public network. This server will act as a proxy, limited amount of services, and will filter packets. What is this type of server called?

A. Bastion host
B. Edge transport server
C. SOCKS hsot
D. Session layer firewall

Answer: A

NEW QUESTION 62
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 64
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 68
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 70
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 74
----------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 82
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 83
A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other f unction(s) of the device? (Select all that apply)

A. Provides access memory, achieving high efficiency
B. Assigns user addresses
C. Enables input/output (I/O) operations
D. Manages security keys

Answer: BCD

NEW QUESTION 86
John has implemented _____ in the network to restrict the limit of public IP addresses in his organization and to enhance the firewall filtering technique.

A. DMZ
B. Proxies
C. VPN
D. NAT

Answer: D

NEW QUESTION 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. High severity level
B. Extreme severity level
C. Mid severity level
D. Low severity level

Answer: D

NEW QUESTION 90
Which of the information below can be gained through network sniffing? (Select all that apply)

A. Telnet Passwords
B. Syslog traffic
C. DNS traffic
D. Programming errors

Answer: ABC

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 95
Which IEEE standard does wireless network use?

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

Answer: A

NEW QUESTION 96
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 100
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 104
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 107
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 112
John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a _____ and it has to adhere to the _____

A. Verification, Security Policies
B. Mitigation, Security policies
C. Vulnerability scanning, Risk Analysis
D. Risk analysis, Risk matrix

Answer: A

NEW QUESTION 113
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 117
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 118
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 119
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 122
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
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. CRC-32
B. CRC-MAC
C. CBC-MAC
D. CBC-32

Answer: C

NEW QUESTION 129
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 131
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 133
Kyle is an IT technician managing 25 workstations and 4 servers. The servers run applications and mostly store confidential data. Kyle must backup the server's data daily to ensure nothing is lost. The power in the company's office is not always reliable, Kyle needs to make sure the servers do not go down or are without power for too long. Kyle decides to purchase an Uninterruptible Power Supply (UPS) that has a pair of inverters and converters to charge the battery and provides power when needed. What type of UPS has Kyle purchased?

A. Kyle purchased a Ferro resonant Standby UPS.
B. Kyle purchased a Line-Interactive UPS
C. He has bought a Standby UPS
D. He purchased a True Online UPS.

Answer: C

NEW QUESTION 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 138
Ivan needs to pick an encryption method that is scalable even though it might be slower. He has settled on a method that works where one key is public and the other is private. What encryption method did Ivan settle on?

A. Ivan settled on the private encryption method.
B. Ivan settled on the symmetric encryption method.
C. Ivan settled on the asymmetric encryption method
D. Ivan settled on the hashing encryption method

Answer: C

NEW QUESTION 140
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 142
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 147
.....

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