Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

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

NEW QUESTION 1
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 2
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 3
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

NEW QUESTION 4
You are responsible for network functions and logical security throughout the corporation. Your company has over 250 servers running Windows Server 2012, 5000 workstations running Windows 10, and 200 mobile users working from laptops on Windows 8. Last week 10 of your company's laptops were stolen from a salesman, while at a conference in Barcelona. These laptops contained proprietary company information.
While doing a damage assessment, a news story leaks about a blog post containing information about the stolen laptops and the sensitive information. What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?

A. You should have used 3DES.
B. You should have implemented the Distributed File System (DFS).
C. If you would have implemented Pretty Good Privacy (PGP).
D. You could have implemented the Encrypted File System (EFS)

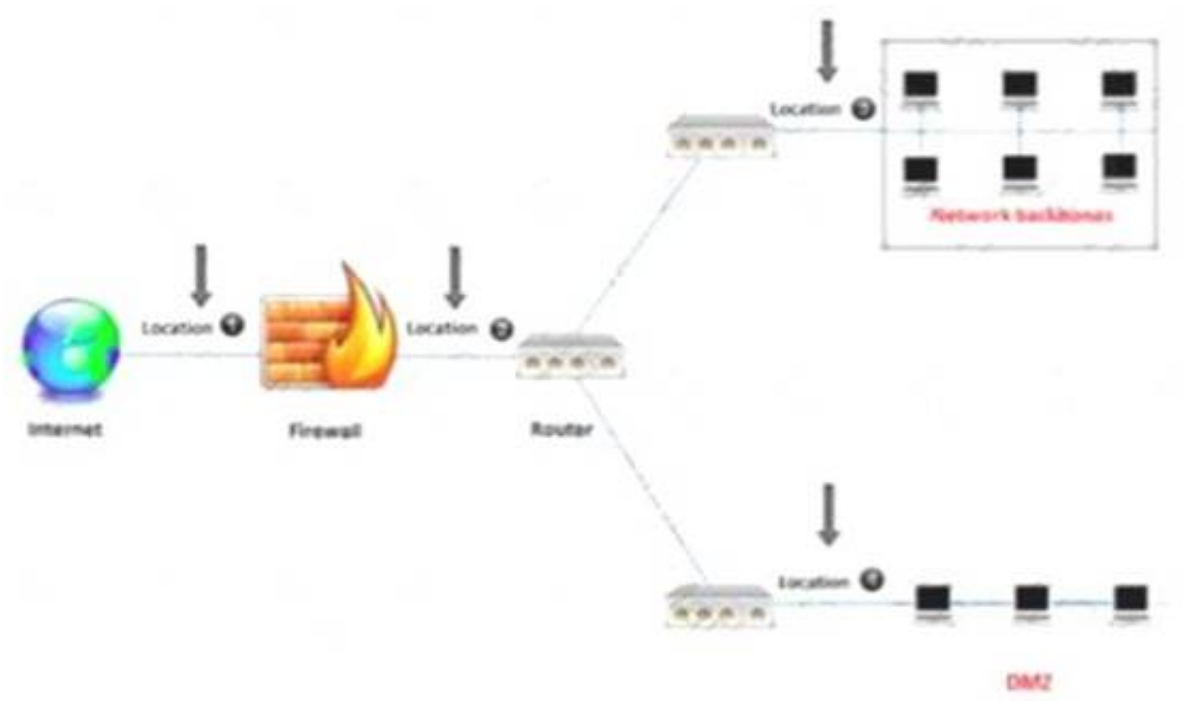
Answer: D

NEW QUESTION 5
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 6
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 7
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 8
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 9
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 10
Larry is responsible for the company's network consisting of 300 workstations and 25 servers. After using a hosted email service for a year, the company wants to control the email internally. Larry likes this idea because it will give him more control over the email. Larry wants to purchase a server for email but does not want the server to be on the internal network due to the potential to cause security risks. He decides to place the server outside of the company's internal firewall. There is another firewall connected directly to the Internet that will protect traffic from accessing the email server. The server will be placed between the two firewalls.
What logical area is Larry putting the new email server into?

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

Answer: A

NEW QUESTION 10
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 13
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 16
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 21
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 26
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 28
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 32
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 36
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 40
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 45
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 46
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

NEW QUESTION 51
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 56
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 57
Which IEEE standard does wireless network use?

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

Answer: A

NEW QUESTION 59
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 64
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 69
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 70
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 74
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 77
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 81
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 86
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 89
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 91
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 95
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 96
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 97
.....

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