



EC-Council

Exam Questions 312-38

EC-Council Network Security Administrator (ENSA)

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

John wants to implement a packet filtering firewall in his organization's network. What TCP/IP layer does a packet filtering firewall work on?

- A. Application layer
- B. Network Interface layer
- C. TCP layer
- D. IP layer

Answer: D

NEW QUESTION 2

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 3

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 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

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 6

Kelly is taking backups of the organization's data. 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

NEW QUESTION 7

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 separates the storage units from the servers and the user network.

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

Answer: A

NEW QUESTION 8

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. Faster restoration
- C. Slower than a full backup
- D. Faster than a full backup
- E. Less expensive than full backup

Answer: AD

NEW QUESTION 9

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 10

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 14

James is working as a Network Administrator in a reputed company situated in California. He is monitoring his network traffic with the help of Wireshark. He wants to check and analyze the traffic against a PING sweep attack. Which of the following Wireshark filters will he use?

- A. `icmp.type==0 and icmp.type==16`
- B. `icmp.type==8 or icmp.type==16`
- C. `icmp.type==8 and icmp.type==0`
- D. `icmp.type==8 or icmp.type==0`

Answer: D

NEW QUESTION 15

Identify the spread spectrum technique that multiplies the original data signal with a pseudo random noise spreading code.

- A. FHSS
- B. DSSS
- C. OFDM
- D. ISM

Answer: B

NEW QUESTION 17

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 20

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 22

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

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 29

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 33

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 37

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 39

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 42

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 44

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 47

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 authenticity of the mails.

Answer: D

NEW QUESTION 52

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 53

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 56

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 61

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 64

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 68

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 71

John, the network administrator and he wants to enable the NetFlow feature in Cisco routers to collect and monitor the IP network traffic passing through the router. Which command will John use to enable NetFlow on an interface?

- A. Router(Config-if) # IP route - cache flow
- B. Router# Netmon enable
- C. Router IP route
- D. Router# netflow enable

Answer: A

NEW QUESTION 72

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 75

.....

Relate Links

100% Pass Your 312-38 Exam with Exam Bible Prep Materials

<https://www.exambible.com/312-38-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>