



## **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

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

The bank where you work has 600 windows computers and 400 Red Hat computers which primarily serve as bank teller consoles. You have created a plan and deployed all the patches to the Windows computers and you are now working on updating the Red Hat computers. What command should you run on the network to update the Red Hat computers, download the security package, force the package installation, and update all currently installed packages?

- A. You should run the `up2date -d -f -u` command
- B. You should run the `up2data -u` command
- C. You should run the `WSUS -d -f -u` command.
- D. You should type the `sysupdate -d` command

**Answer:** A

#### NEW QUESTION 3

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 4

Daniel is giving training on designing and implementing a security policy in the organization. He is explaining the hierarchy of the security policy which demonstrates how policies are drafted, designed and implemented.

What is the correct hierarchy for a security policy implementation?

- A. Laws, Policies, Regulations, Procedures and Standards
- B. Regulations, Policies, Laws, Standards and Procedures
- C. Laws, Regulations, Policies, Standards and Procedures
- D. Procedures, Policies, Laws, Standards and Regulations

**Answer:** C

#### NEW QUESTION 5

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 6

Assume that you are working as a network administrator in the head office of a bank. One day a bank employee informed you that she is unable to log in to her system. At the same time, you get a call from another network administrator informing you that there is a problem connecting to the main server. How will you prioritize these two incidents?

- A. Based on approval from management
- B. Based on a first come first served basis
- C. Based on a potential technical effect of the incident
- D. Based on the type of response needed for the incident

**Answer:** C

#### NEW QUESTION 7

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 8

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 9

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 10

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 10

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 15

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 19

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 22

John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network. Which of the following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt?

- A. Tcp.flags==0x2b
- B. Tcp.flags=0x00
- C. Tcp.options.mss\_val<1460
- D. Tcp.options.wscale\_val==20

**Answer:** ABC

#### NEW QUESTION 24

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 28

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 32

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 36

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 39

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 43

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 46

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 50

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 51

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 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

Brendan wants to implement a hardware based RAID system in his network. He is thinking of choosing a suitable RAM type for the architectural setup in the system. The type he is interested in provides access times of up to 20 ns. Which type of RAM will he select for his RAID system?

- A. NVRAM
- B. SDRAM
- C. NAND flash memory
- D. SRAM

**Answer:** D

#### NEW QUESTION 65

-----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 70

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 71

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 76

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 78

John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information. Which type of firewall service is John thinking of implementing?

- A. Application level gateway
- B. Circuit level gateway
- C. Stateful Multilayer Inspection
- D. Packet Filtering

**Answer:** B

#### NEW QUESTION 83

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 86

John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information. Which type of firewall service is John thinking of implementing?

- A. Application level gateway
- B. Stateful Multilayer Inspection
- C. Circuit level gateway
- D. Packet Filtering

**Answer:** C

#### NEW QUESTION 90

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 93



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 96

.....



## 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/>