Vendor: CompTIA

Exam Code:SY0-501

Exam Name: CompTIA Security+ Certification Exam

Version: Demo

QUESTION 1

Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive. Which of the following procedures did Joe follow?

A. Order of volatility

B. Chain of custody

C. Recovery procedure

D. Incident isolation

Correct Answer: A

QUESTION 2

Which of the following types of vulnerability scans typically returns more detailed and thorough insights into actual system vulnerabilities?

A. Non-credentialed

B. Intrusive

C. Credentialed

D. Non-intrusive

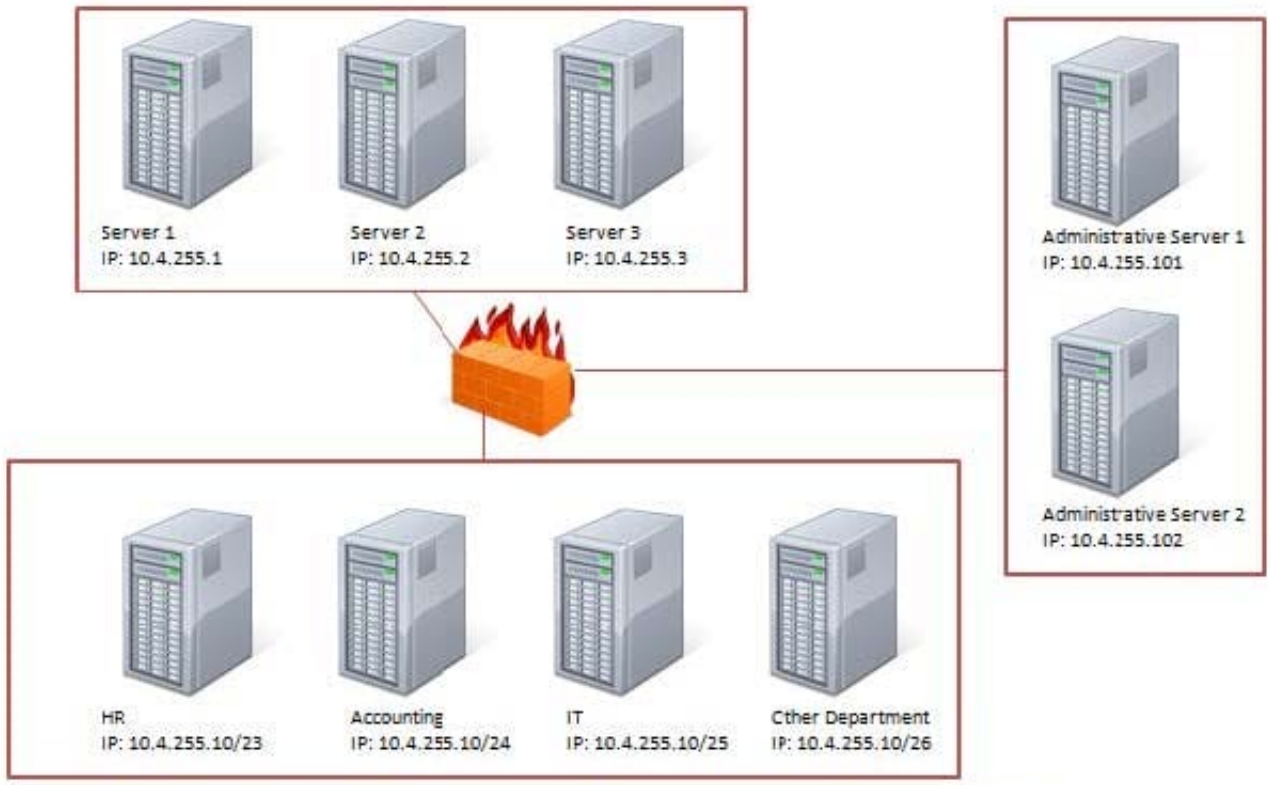
Correct Answer: C

QUESTION 3

Configure the Firewall

Task: Configure the firewall (fill out the table) to allow these four rules:

1. Only allow the Accounting computer to have HTTPS access to the Administrative server.
2. Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
3. Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Correct Answer:

Use the following answer for this simulation task: Source IP Destination IP

Port number

TCP/UDP

Allow/Deny

10.4.255.10/24

10.4.255.101

443

TCP

Allow

10.4.255.10/23

10.4.255.2

22

TCP

Allow

10.4.255.10/25

10.4.255.101

Any

Any

Allow

10.4.255.10/25

10.4.255.102

Any

Any

Allow

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule\\'s criteria:

Block the connection

Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent. Two hosts communicate packet results with each other. TCP also

ensures that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it\\'s considerably faster than TCP. The sessions don\\'t establish a synchronized session like the kind used in TCP,

and UDP doesn\\'t guarantee error-free communications. The primary purpose of UDP is to send small packets of information. The application is responsible for acknowledging the correct reception of the data.

Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections

QUESTION 4

Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

A. Spear phishing

B. Main-in-the-middle

C. URL hijacking

D. Transitive access

Correct Answer: B

QUESTION 5

Which of the following cloud models is used to share resources and information with business partners and like businesses without allowing everyone else access?

A. Public

B. Hybrid

C. Community

D. Private

Correct Answer: C

QUESTION 6

As a security measure, an organization has disabled all external media from accessing the network Since some users may have data that needs to be transferred to the network, which of the would BEST assist a security administrator with transferring the data while keeping the internal network secure?

A. Upload the media in the DMZ

B. Upload the data in a separate VLAN

C. Contact the data custodian

D. Use a standalone scanning system

Correct Answer: A

QUESTION 7

A credentialed vulnerability scan is often preferred over a non-credentialed scan because credentialed scans:

A. generates more false positives.

B. rely solely on passive measures.

C. are always non-intrusive.

D. provide more accurate data.

Correct Answer: D

QUESTION 8

While monitoring the SIEM, a security analyst observes traffic from an external IP to an IP address of the business network on port 443. Which of the following protocols would MOST likely cause this traffic?

A. HTTP

B. SSH

C. SSL

D. DNS

Correct Answer: B

QUESTION 9

Joe, a contractor, is hired by a firm to perform a penetration test against the firm\\'s infrastructure. When conducting the scan, he receives only the network diagram and the network list to scan against the network. Which of the following scan types is Joe performing?

A. Authenticated

B. White box

C. Automated

D. Gray box

Correct Answer: D

QUESTION 10

Which of the following could an attacker use to overwrite instruction pointers in order to execute malicious code?

A. Memory leak

B. SQL injection

C. Resource exhaustion

D. Buffer overflow

Correct Answer: D

QUESTION 11

A computer forensics analyst collected a flash drive that contained a single file with 500 pages of text. Which of the following algorithms should the analyst use to validate the integrity of the file?

A. 3DES

B. AES

C. MD5

D. RSA

Correct Answer: C

QUESTION 12

An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription. Which of the following types of services is this company now using?

A. SaaS

B. CASB

C. IaaS

D. PaaS

Correct Answer: B

Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.