DUMPS ARENA

CompTIA Security+

CompTIA SY0-501

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1132

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

dumpsarena.com

QUESTION NO: 1

A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis.

B. Restrict administrative privileges and patch all systems and applications.

C. Rebuild all workstations and install new antivirus software.

D. Implement application whitelisting and perform user application hardening.

ANSWER: A

QUESTION NO: 2

A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user’s machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

A. SSH

B. SFTP

C. HTTPS

D. SNMP

ANSWER: A

QUESTION NO: 3

A security analyst is updating a BIA document. The security analyst notices the support vendor's time to replace a server hard drive went from eight hours to two hours.

Given these new metrics, which of the following can be concluded? (Choose two.)

A. The MTTR is faster.

B. The MTTR is slower.

C. The RTO has increased.

D. The RTO has decreased.

E. The MTTF has increased.

F. The MTTF has decreased.

ANSWER: A D

QUESTION NO: 4 - (DRAG DROP)

DRAG DROP

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS).

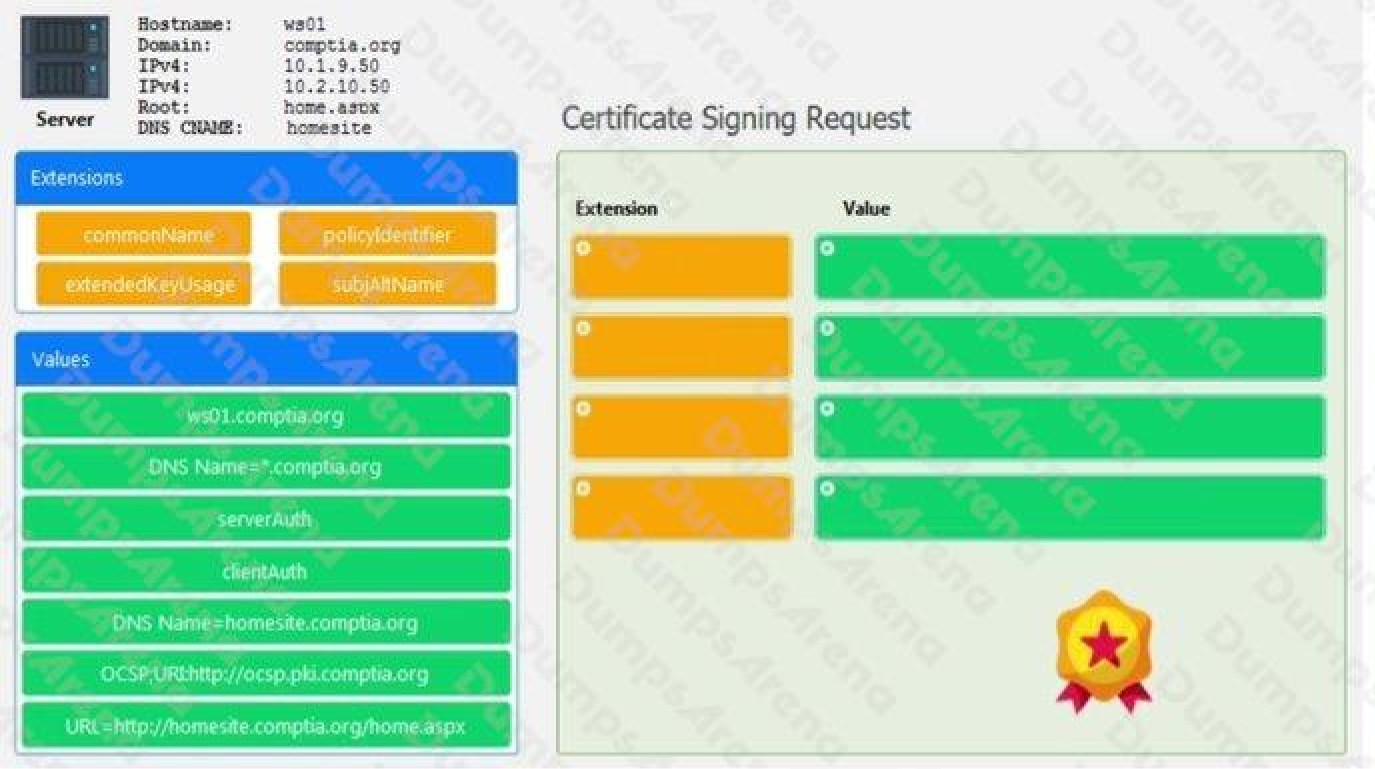
- Hostname: ws01
- Domain: comptia.org
- IPv4: 10.1.9.50
- IPv4: 10.2.10.50
- Root: home.aspx
- DNS CNAME: homesite

INSTRUCTIONS

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the left-hand column and values belong in the corresponding row in the right-hand column.

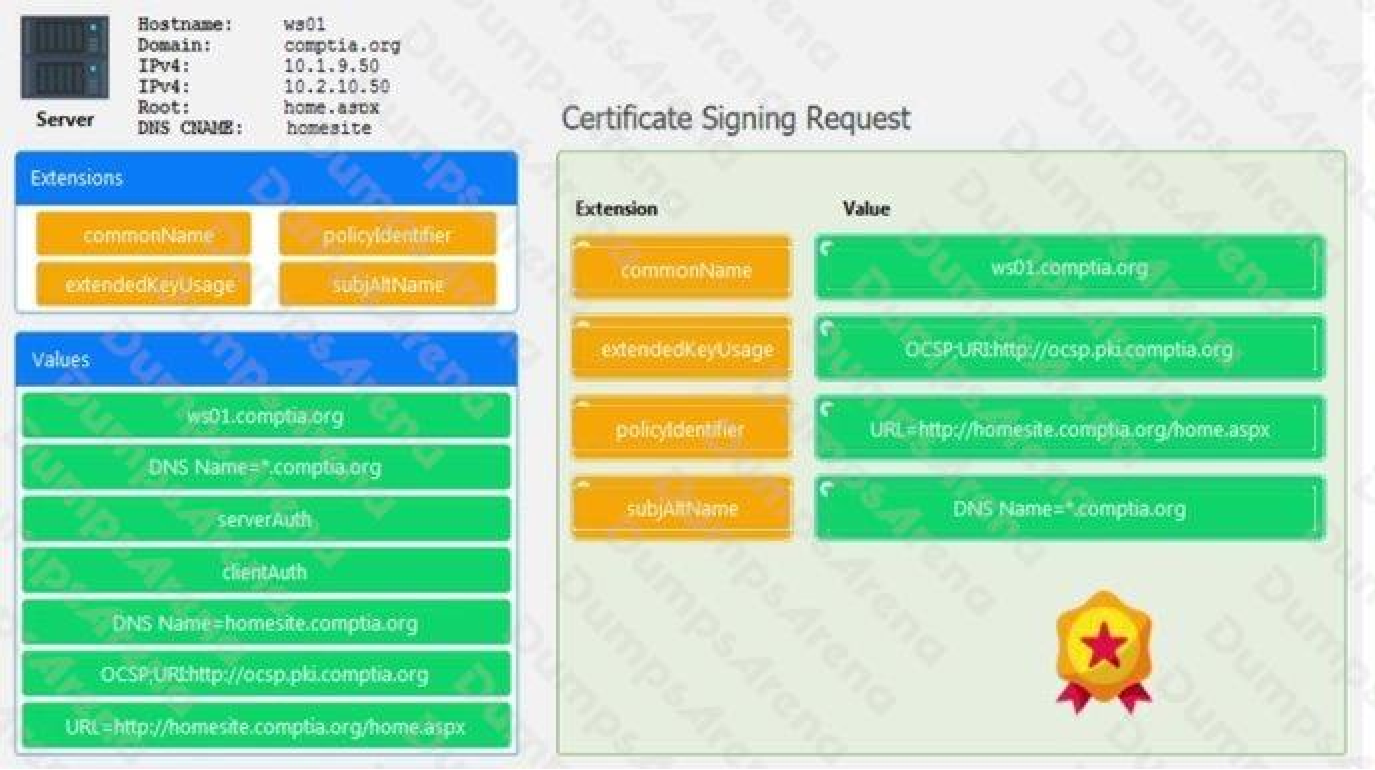
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



```
Hostname:    ws01
Domain:      comptia.org
IPv4:        10.1.9.50
IPv4:        10.2.10.50
Root:        home.aspx
DNS CNAME:   homesite
```

ANSWER:



```
Hostname:    ws01
Domain:      comptia.org
IPv4:        10.1.9.50
IPv4:        10.2.10.50
Root:        home.aspx
DNS CNAME:   homesite
```

Extension	Value
commonName	ws01.comptia.org
extendedKeyUsage	OCSP;URI:http://ocsp.pki.comptia.org
policyIdentifier	URL=http://homesite.comptia.org/home.aspx
subjAltName	DNS Name=*.comptia.org

Server
Certificate Signing Request
Extensions
commonName
policyIdentifier
extendedKeyUsage
subjAltName
Values
ws01.comptia.org
DNS Name=*.comptia.org
serverAuth
clientAuth
DNS Name=homesite.comptia.org
OCSP;URI:http://ocsp.pki.comptia.org
URL=http://homesite.comptia.org/home.aspx

Explanation:

QUESTION NO: 5

A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

A. Tunnel mode IPSec

B. Transport mode VPN IPSec

C. L2TP

D. SSL VPN

ANSWER: D

QUESTION NO: 6

Which of the following impacts are associated with vulnerabilities in embedded systems? (Choose two.)

A. Repeated exploitation due to unpatchable firmware

B. Denial of service due to an integrated legacy operating system.

C. Loss of inventory accountability due to device deployment

D. Key reuse and collision issues due to decentralized management.

E. Exhaustion of network resources resulting from poor NIC management.

ANSWER: A D

QUESTION NO: 7

While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack.

Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Choose two.)

A. Minimum complexity

B. Maximum age limit

C. Maximum length

D. Minimum length

E. Minimum age limit

F. Minimum re-use limit

ANSWER: A D

QUESTION NO: 8

Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Choose two.)

A. Rainbow table attacks greatly reduce compute cycles at attack time.

B. Rainbow tables must include precomputed hashes.

C. Rainbow table attacks do not require access to hashed passwords.

D. Rainbow table attacks must be performed on the network.

E. Rainbow table attacks bypass maximum failed login restrictions.

ANSWER: B E

QUESTION NO: 9

An organization needs to integrate with a third-party cloud application. The organization has 15000 users and does not want to allow the cloud provider to query its LDAP authentication server directly. Which of the following is the BEST way for the organization to integrate with the cloud application?

A. Upload a separate list of users and passwords with a batch import.

B. Distribute hardware tokens to the users for authentication to the cloud.

C. Implement SAML with the organization's server acting as the identity provider.

D. Configure a RADIUS federation between the organization and the cloud provider.

ANSWER: D

QUESTION NO: 10

Which of the following is a major difference between XSS attacks and remote code exploits?

A. XSS attacks use machine language, while remote exploits use interpreted language

B. XSS attacks target servers, while remote code exploits target clients

C. Remote code exploits aim to escalate attackers' privileges, while XSS attacks aim to gain access only

D. Remote code exploits allow writing code at the client side and executing it, while XSS attacks require no code to work

ANSWER: C

QUESTION NO: 11

A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Choose two.)

A. Ping

B. Ipconfig

C. Tracert

D. Netstat

E. Dig

F. Nslookup

ANSWER: B C

QUESTION NO: 12

A network administrator is brute forcing accounts through a web interface. Which of the following would provide the BEST defense from an account password being discovered?

A. Password history

B. Account lockout

C. Account expiration

D. Password complexity

ANSWER: B

QUESTION NO: 13

An organization has hired a new remote workforce. Many new employees are reporting that they are unable to access the shared network resources while traveling. They need to be able to travel to and from different locations on a weekly basis. Shared offices are retained at the headquarters location. The remote workforce will have identical file and system access requirements, and must also be able to log in to the headquarters location remotely. Which of the following BEST represent how the remote employees should have been set up initially? (Choose two.)

A. User-based access control

B. Shared accounts

C. Group-based access control

D. Mapped drives

E. Individual accounts

F. Location-based policies

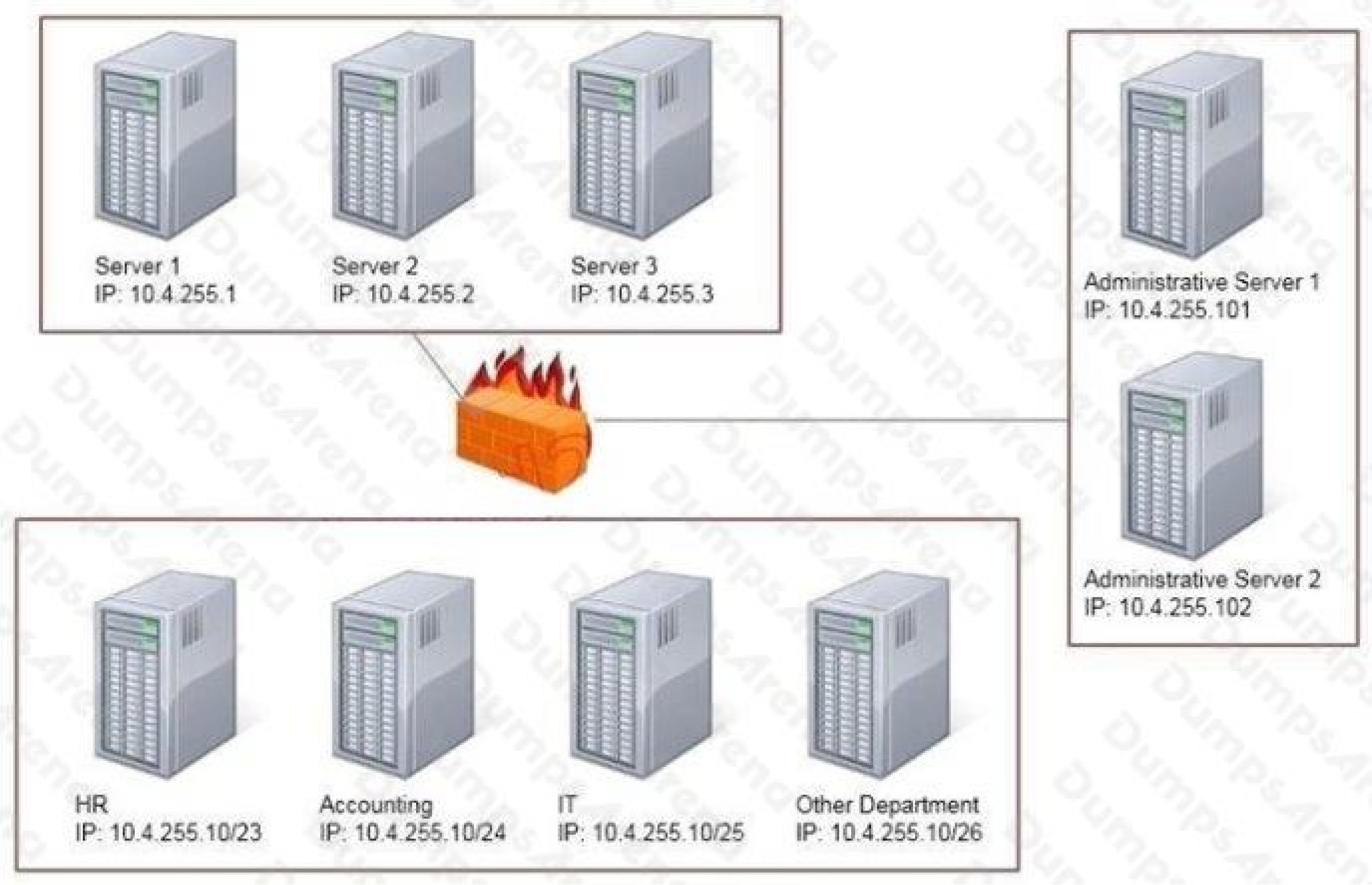
ANSWER: C E

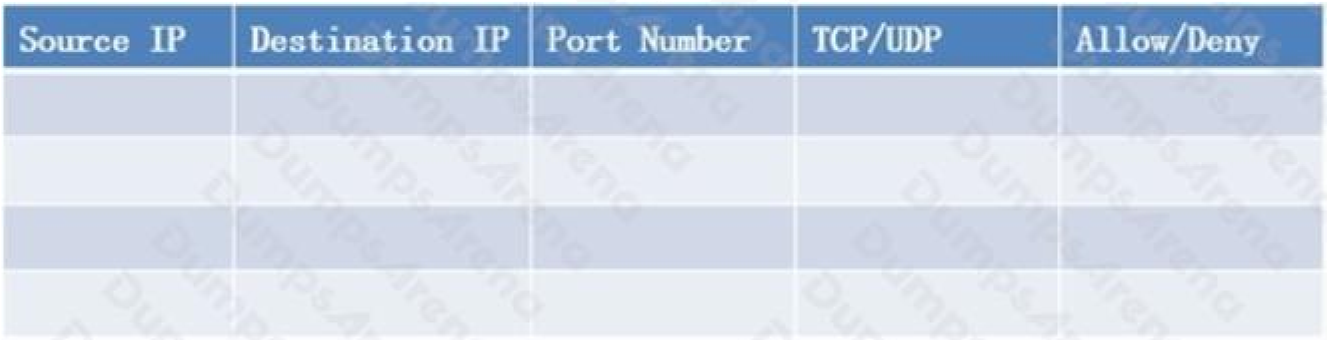
QUESTION NO: 14 - (SIMULATION)

SIMULATION

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

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





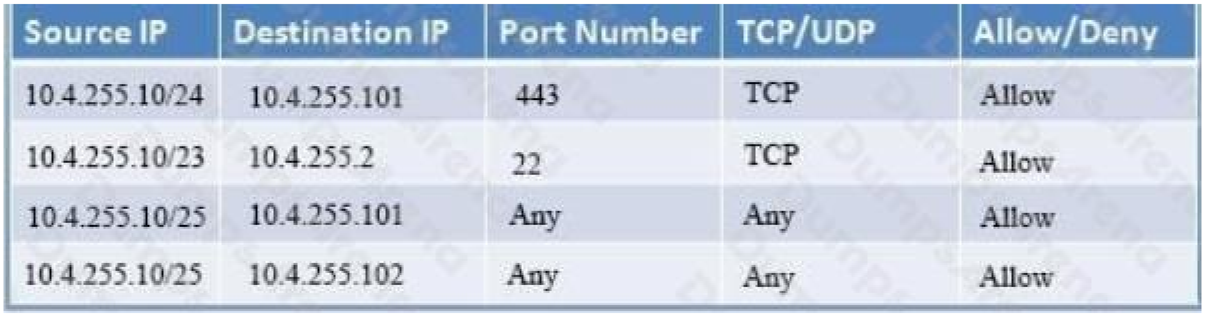
Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

ANSWER: See the solution below.

Explanation:

Use the following answer for this simulation task.

Below table has all the answers required for this question.



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? HTTPS and is a TCP port.

Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between:

10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)

10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

QUESTION NO: 15

Which of the following command line tools would be BEST to identify the services running in a server?

A. Traceroute

B. Nslookup

C. Ipconfig

D. Netstat

ANSWER: D

QUESTION NO: 16

A company has migrated to two-factor authentication for accessing the corporate network, VPN, and SSO. Several legacy applications cannot support multifactor authentication and must continue to use usernames and passwords. Which of the following should be implemented to ensure the legacy applications are as secure as possible while ensuring functionality? (Choose two.)

A. Privileged accounts

B. Password reuse restrictions

C. Password complexity requirements

D. Password recovery

E. Account disablement

ANSWER: C E

QUESTION NO: 17

A security administrator has configured a RADIUS and a TACACS+ server on the company's network. Network devices will be required to connect to the TACACS+ server for authentication and send accounting information to the RADIUS server. Given the following information:

RADIUS IP: 192.168.20.45

TACACS+ IP: 10.23.65.7

Which of the following should be configured on the network clients? (Choose two.)

A. Accounting port: TCP 389

B. Accounting port: UDP 1812

C. Accounting port: UDP 1813

D. Authentication port: TCP 49

E. Authentication port: TCP 88

F. Authentication port: UDP 636

ANSWER: C D

QUESTION NO: 19

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. perform attribution to specific APTs and nation-state actors.

B. anonymize any PII that is observed within the IoC data.

C. add metadata to track the utilization of threat intelligence reports.

D. assist companies with impact assessments based on the observed data.

ANSWER: B

QUESTION NO: 20 - (DRAG DROP)

DRAG DROP

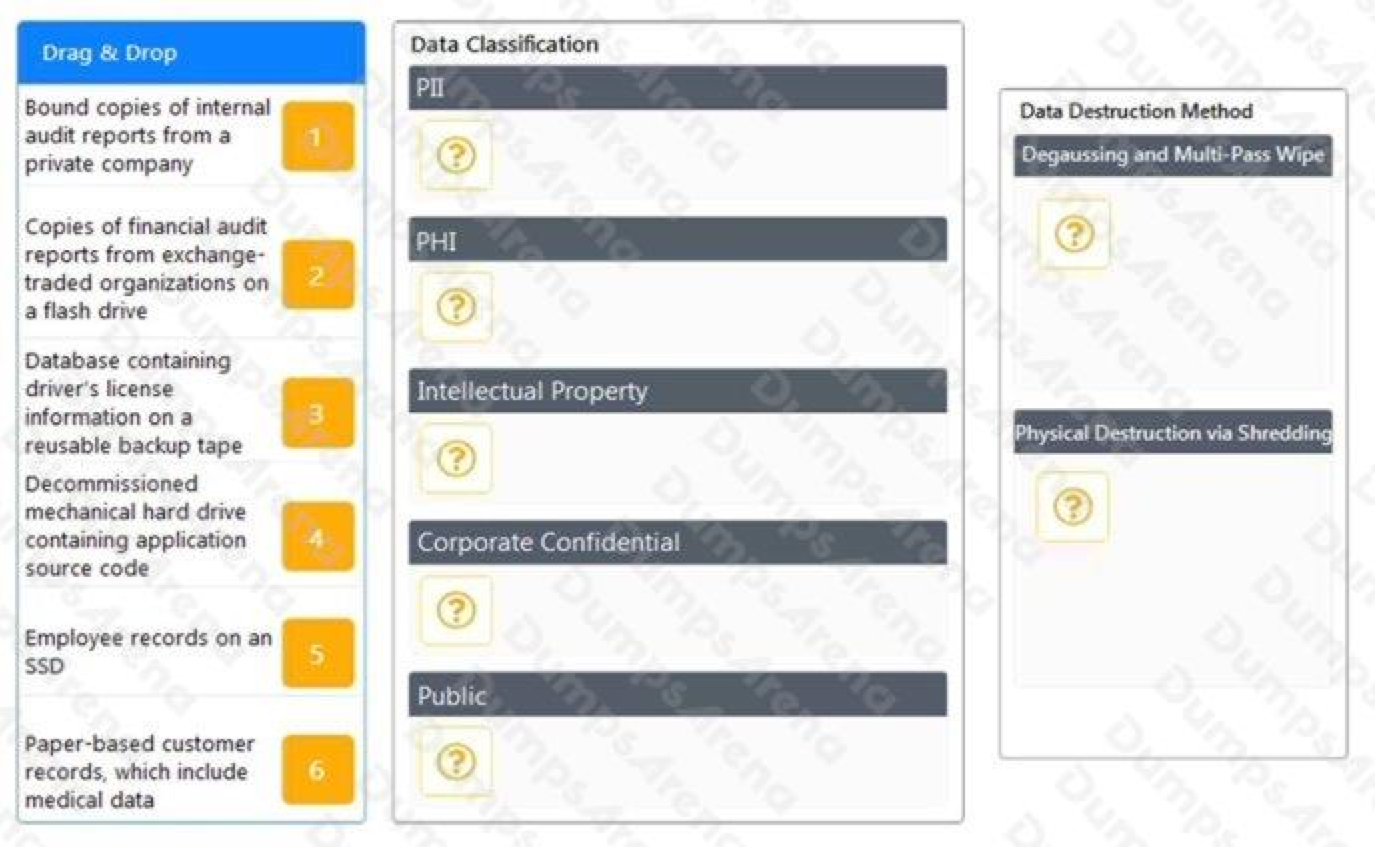
A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.

INSTRUCTIONS

From the options below, drag each item to its appropriate classification as well as the MOST appropriate form of disposal.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



Drag & Drop

1 Bound copies of internal audit reports from a private company

2 Copies of financial audit reports from exchange-traded organizations on a flash drive

3 Database containing driver's license information on a reusable backup tape

4 Decommissioned mechanical hard drive containing application source code

5 Employee records on an SSD

6 Paper-based customer records, which include medical data

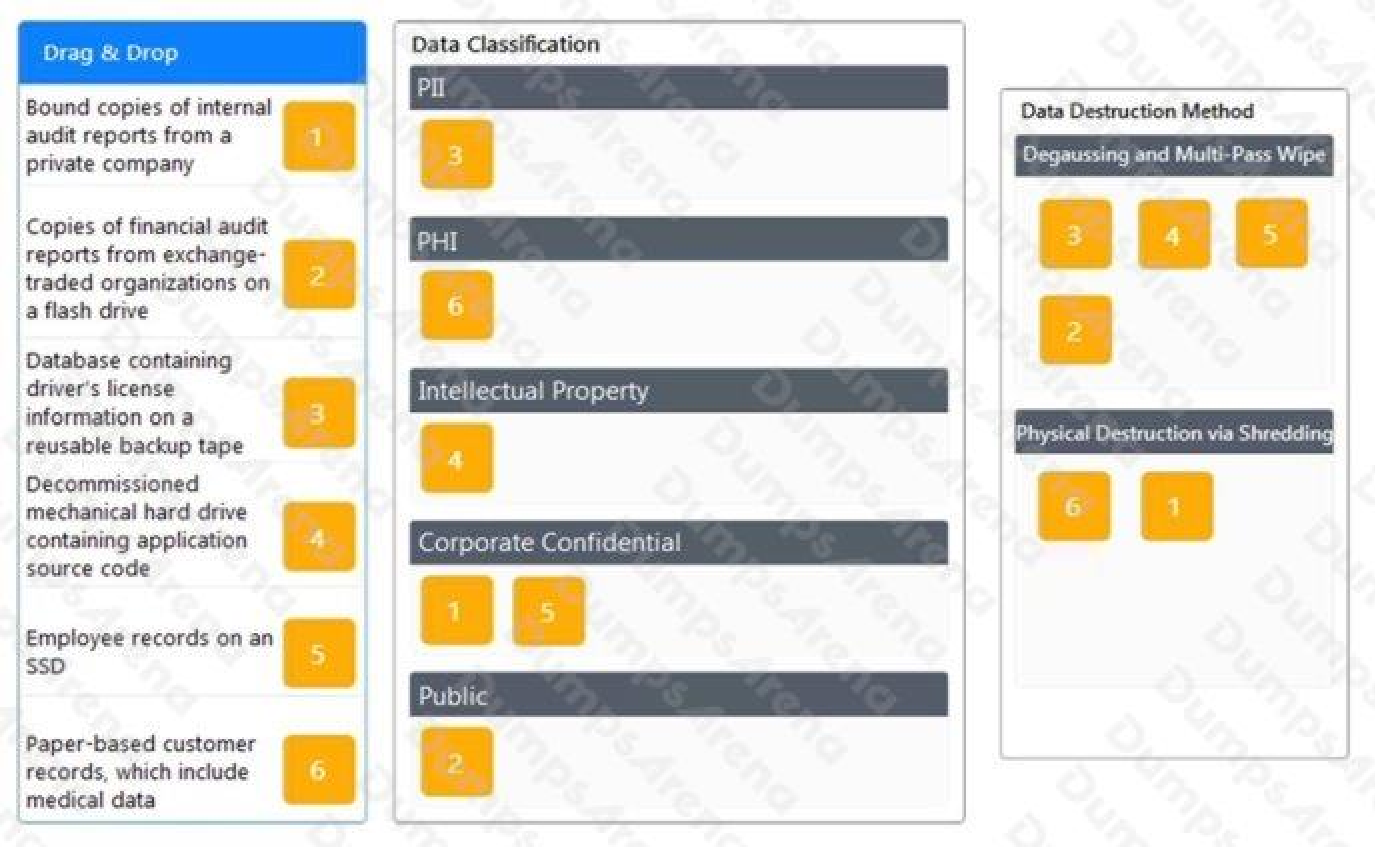
Data Classification

- PII
- PHI
- Intellectual Property
- Corporate Confidential
- Public

Data Destruction Method

- Degaussing and Multi-Pass Wipe
- Physical Destruction via Shredding

ANSWER:



Drag & Drop

- Bound copies of internal audit reports from a private company 1
- Copies of financial audit reports from exchange-traded organizations on a flash drive 2
- Database containing driver's license information on a reusable backup tape 3
- Decommissioned mechanical hard drive containing application source code 4
- Employee records on an SSD 5
- Paper-based customer records, which include medical data 6

Data Classification

- PII: 3
- PHI: 6
- Intellectual Property: 4
- Corporate Confidential: 1, 5
- Public: 2

Data Destruction Method

- Degaussing and Multi-Pass Wipe: 3, 4, 5, 2
- Physical Destruction via Shredding: 6, 1

Explanation: