

CompTIA.Premium.SY0-501.by.VCEplus.82q

Number: SY0-501 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Exam Code: SY0-501

Exam Name: CompTIA Security+

Certification Provider: CompTIA

Corresponding Certification: CompTIA Security+

Website: www.vceplus.com

Free Exam: <https://vceplus.com/comptia-security-sy0-501/>

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in SY0-501 exam products and you get latest questions. We strive to deliver the best SY0-501 exam product for top grades in your first attempt.

VCE to PDF Converter : <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

Google+ : <https://plus.google.com/+Vcepluscom>

LinkedIn : <https://www.linkedin.com/company/vceplus>

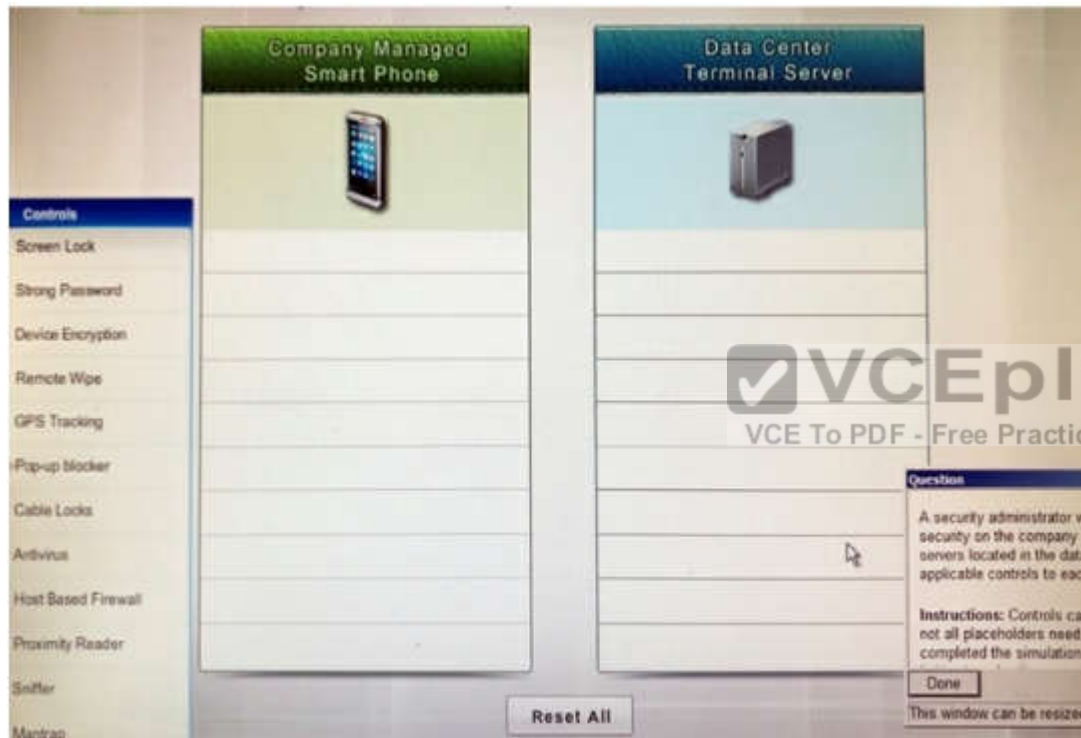
Exam A

QUESTION 1

SIMULATION

A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?

Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.



Your Response:
type here

A. Please see explanation below.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Company Manages Smart Phone

Screen Lock

Strong Password

Device Encryption

Remote Wipe

GPS Tracking

Pop-up blocker

Data Center Terminal Server

Cable Locks

Antivirus

Host Based Firewall Proximity Reader Sniffer Mantrap

QUESTION 2

HOTSPOT










Select the appropriate attack from each drop down list to label the corresponding illustrated attack.

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Hot Area:

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.










Attack Vector	Target	Identified Attack
 <p>Attacker gains confidential company information</p>	 <p>Targeted CEO and board members</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker posts link to fake AV software</p>	 <p>Multiple social networks</p>  <p>Broad set of victims</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker collecting credit card details</p>	 <p>Phone-based victim</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker mass-mails product information to parties that have already opted out of receiving advertisements</p>	 <p>Broad set of recipients</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>

Correct Answer:



Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
 Attacker gains confidential company information	 Targeted CEO and board members	<div> <input type="text"/> </div> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker posts link to fake AV software	 Multiple social networks  Broad set of victims	<div> <input type="text"/> </div> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker collecting credit card details	 Phone-based victim	<div> <input type="text"/> </div> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	<div> <input type="text"/> </div> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK

Section: (none)

Explanation

Explanation/Reference:

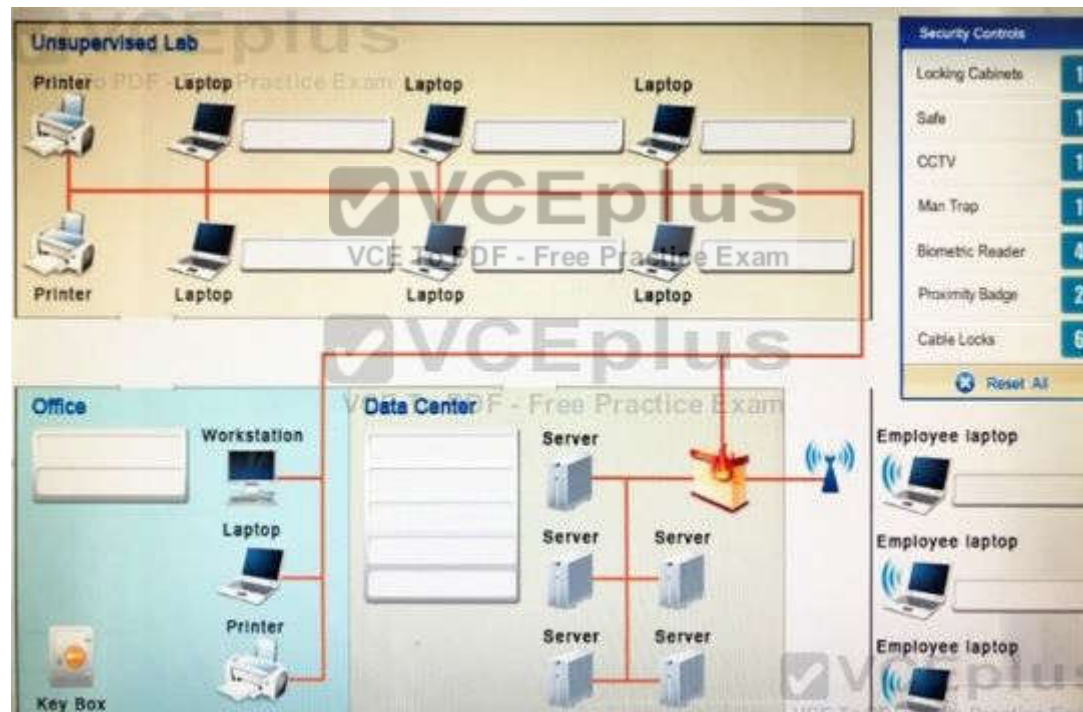
QUESTION 3

DRAG DROP

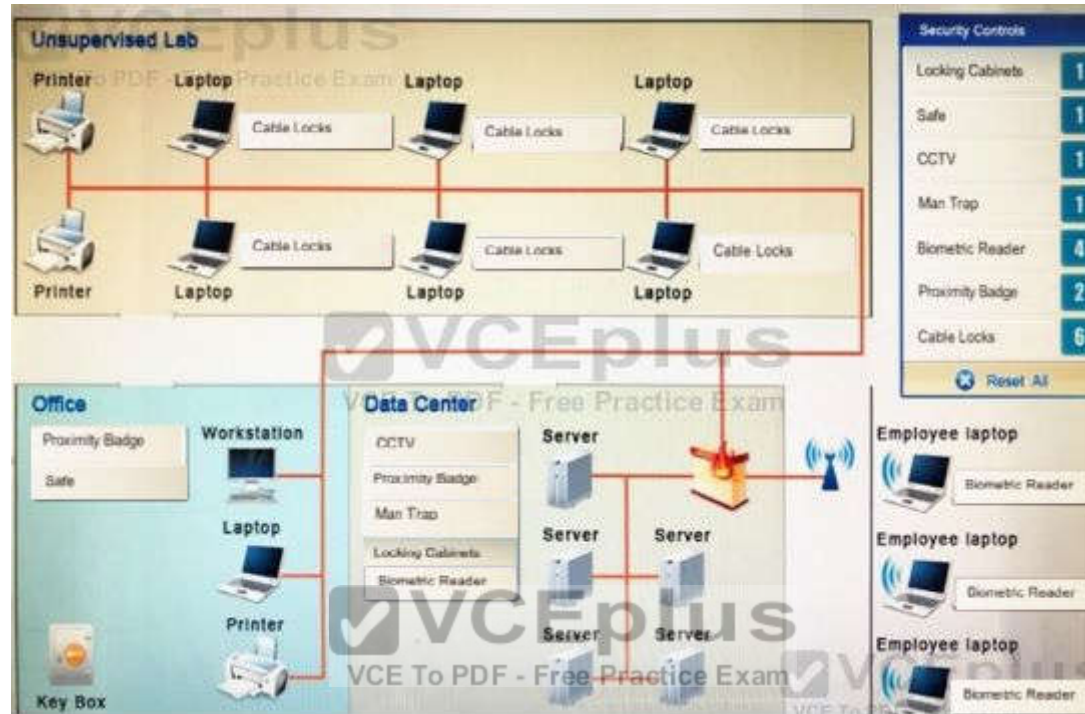
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.

Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.

Select and Place:



Correct Answer:



Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

Which of the following would a security specialist be able to determine upon examination of a server's certificate?

- A. CA public key
- B. Server private key
- C. CSR
- D. OID

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:****QUESTION 5**

A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?

- A. tracer
- B. netstat
- C. ping
- D. nslookup

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****QUESTION 6**

Multiple organizations operating in the same vertical wants to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

- A. Shibboleth
- B. RADIUS federation
- C. SAML
- D. OAuth
- E. OpenID connect

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****QUESTION 7**

Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

- A. Sustainability
- B. Homogeneity
- C. Resiliency
- D. Configurability

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost- effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

- A. Elasticity
- B. Scalability
- C. High availability
- D. Redundancy



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Which of the following attacks specifically impact data availability?

- A. DDoS
- B. Trojan
- C. MITM
- D. Rootkit

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Which of the following attacks specifically impact data availability?

- A. DDoS
- B. Trojan
- C. MITM
- D. Rootkit

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 11

A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select two.)

- A. Generate an X.509-compliant certificate that is signed by a trusted CA.
- B. Install and configure an SSH tunnel on the LDAP server.
- C. Ensure port 389 is open between the clients and the servers using the communication.
- D. Ensure port 636 is open between the clients and the servers using the communication.
- E. Remove the LDAP directory service role from the server.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?

- A. Competitor
- B. Hacktivist
- C. Insider
- D. Organized crime.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?

- A. URL hijacking
- B. Reconnaissance
- C. White box testing
- D. Escalation of privilege

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

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

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

- A. Error handling to protect against program exploitation
- B. Exception handling to protect against XSRF attacks.
- C. Input validation to protect against SQL injection.
- D. Padding to protect against string buffer overflows.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 16

A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.

The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

- A. Require the SFTP protocol to connect to the file server.
- B. Use implicit TLS on the FTP server.
- C. Use explicit FTPS for connections.
- D. Use SSH tunneling to encrypt the FTP traffic.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

- A. The recipient can verify integrity of the software patch.
- B. The recipient can verify the authenticity of the site used to download the patch.
- C. The recipient can request future updates to the software using the published MD5 value.
- D. The recipient can successfully activate the new software patch.

Correct Answer: A


Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

Refer to the following code:

 **VCEplus**
VCE To PDF - Free Practice Exam

```
public class rainbow {  
    public static void main (String [] args) {  
        object blue = null;  
        blue.hashCode (); }  
}
```

Which of the following vulnerabilities would occur if this is executed?

- A. Page exception
- B. Pointer deference
- C. Null Pointer Exception
- D. Missing null check

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened. The network and security teams perform the following actions:

- Shut down all network shares.
- Run an email search identifying all employees who received the malicious message.
- Reimage all devices belonging to users who opened the attachment.

Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?

- A. Eradication
- B. Containment
- C. Recovery
- D. Lessons learned

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 20**

An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

- A. RTO
- B. RPO
- C. MTBF
- D. MTTR

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

Which of the following types of keys is found in a key escrow?

- A. Public
- B. Private
- C. Shared
- D. Session

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

A security analyst is reviewing the following output from an IPS:

```
[**] [1:2467:7] EXPLOIT IGMP IGAP message overflow attempt [**]  
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]  
07/30-19:45:02.238185 250.19.18.71 -> 250.19.18.22  
IGMP TTL:255 TOS: 0x0 ID: 9742 IpLen:20 DgmLen: 502 MF  
Frag offset: 0x1FFF Frag Size: 0x01E2  
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0867]
```

Given this output, which of the following can be concluded? (Select two.)

- A. The source IP of the attack is coming from 250.19.18.22.
- B. The source IP of the attack is coming from 250.19.18.71.
- C. The attacker sent a malformed IGAP packet, triggering the alert.
- D. The attacker sent a malformed TCP packet, triggering the alert.
- E. The TTL value is outside of the expected range, triggering the alert

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23