

CERTPARK

QUESTION & ANSWER



CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



<https://www.certpark.com>

Exam : RC0-501

**Title : CompTIA Security+
Recertification Exam**

Version : DEMO

1. DRAG DROP

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.

The screenshot shows a security simulation interface. On the left, a list of controls is displayed under the heading 'Controls': Screen Lock, Strong Password, Device Encryption, Remote Wipe, GPS Tracking, Pop-up blocker, Cable Locks, Antivirus, Host Based Firewall, Proximity Reader, Sniffer, and Mantrap. In the center, there are two asset placeholders: 'Company Managed Smart Phone' (top) and 'Data Center Terminal Server' (bottom). Each placeholder has a grid of empty slots for dragging controls. On the right, a 'Question' box contains the text: '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 type?'. Below the question, it says '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.' There is a 'Done' button and a 'Reset All' button at the bottom.

Answer:

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




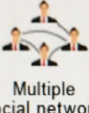






2.HOTSPOT

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.

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>	<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>
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>	 <p>Victims</p> <div> <p>Fraudulent site</p> <p>Legitimate site</p> </div>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>

Answer:

Question
 Show

Attacks

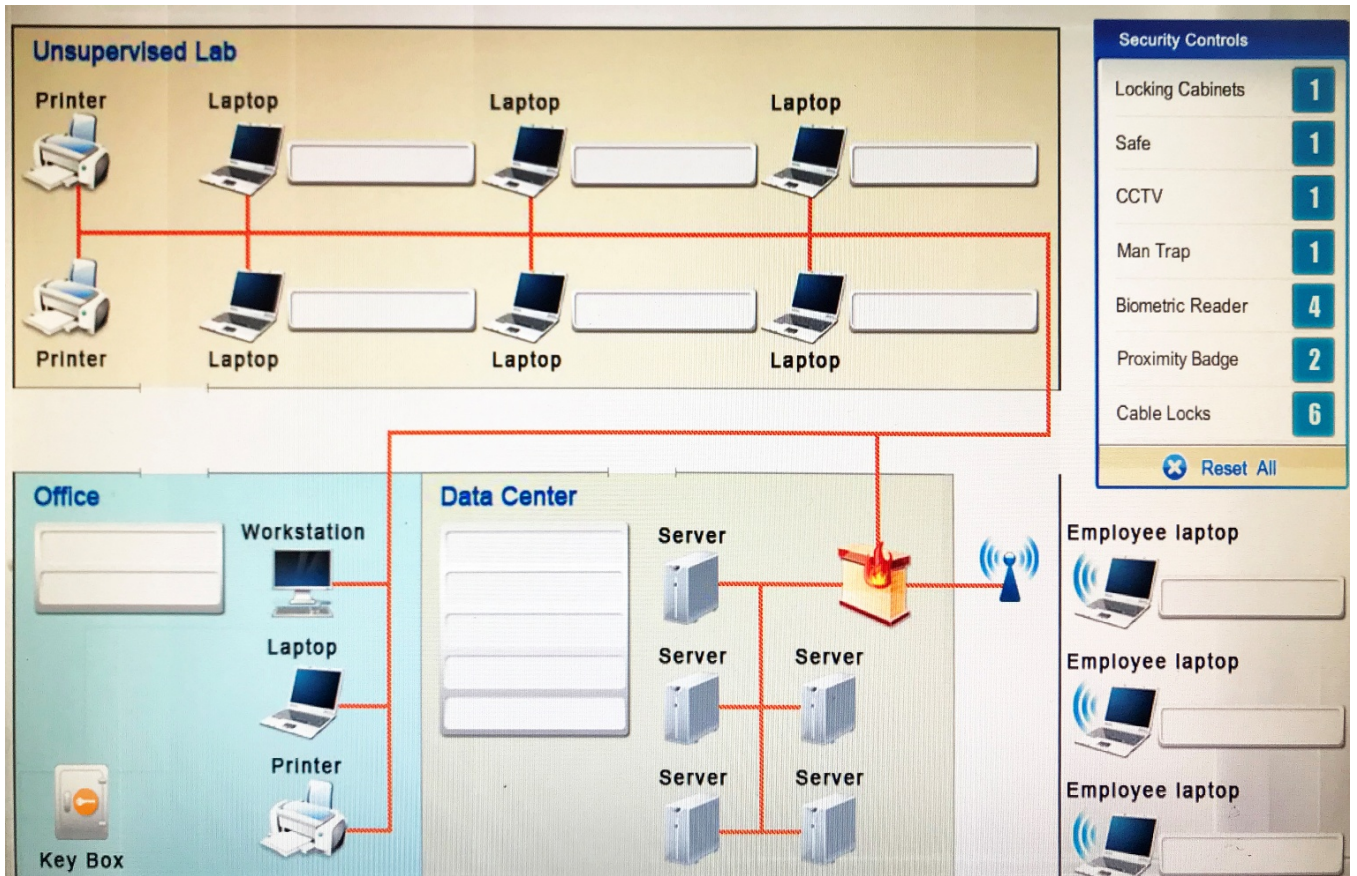
Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.

Attack Vector		Target	Identified Attack
 Attacker gains confidential company information	➔	 Targeted CEO and board members	<input type="text" value="SPEAR PHISHING"/>
 Attacker posts link to fake AV software	➔  ➔	 Broad set of victims	<input type="text" value="HOAX"/>
 Attacker collecting credit card details	➔	 Phone-based victim	<input type="text" value="VISHING"/>
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	➔	 Broad set of recipients	<input type="text" value="PHISHING"/>
 Attacker redirects name resolution entries from legitimate site to fraudulent site	➔	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">➔ Fraudulent site</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">➔ Legitimate site</div> </div> </div> Victims	<input type="text" value="PHARMING"/>

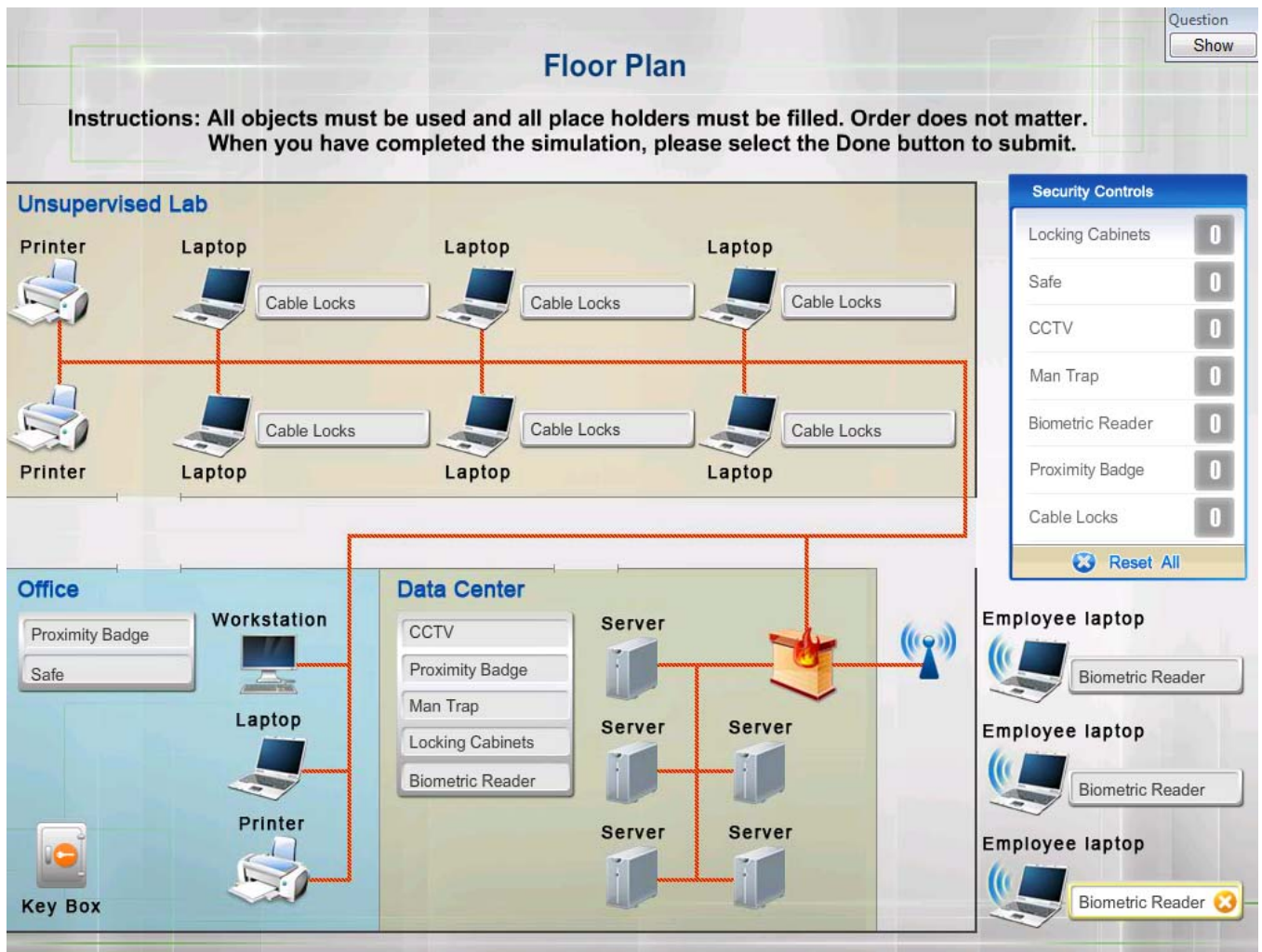
3.DRAG DROP

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.



Answer:



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

Answer: D

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. tracert
- B. netstat
- C. ping
- D. nslookup

Answer: B