

EXAMUNION

Certified IT Exam Material Authority



Accurate study guides, High passing rate!
We offer free update service for one year!

<http://www.examunion.com>

Exam : **RC0-501**

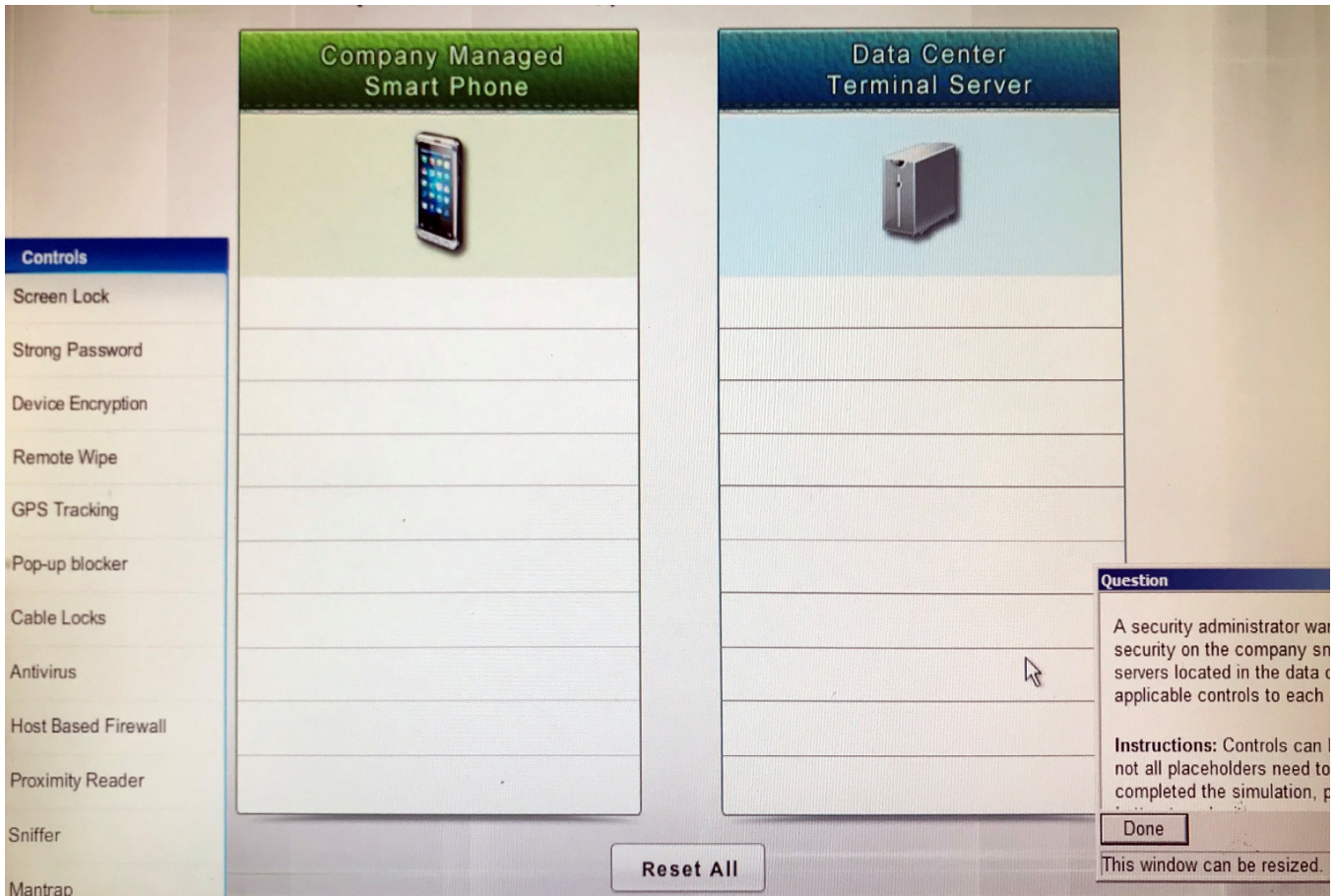
Title : **CompTIA Security+
Recertification Exam**

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.



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











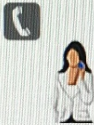





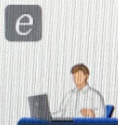
2.HOTSPOT

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>	<ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 <p>Attacker posts link to fake AV software</p>	    <p>Broad set of victims</p>	<ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 <p>Attacker collecting credit card details</p>	  <p>Phone-based victim</p>	<ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 <p>Attacker mass-mails product information to parties that have already opted out of receiving advertisements</p>	  <p>Broad set of recipients</p>	<ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>	  <p>Victims</p> <div style="display: flex; align-items: center; gap: 10px;"> <div style="border: 1px solid red; padding: 2px;">Fraudulent site</div> <div style="border: 1px solid green; padding: 2px;">Legitimate site</div> </div>	<ul style="list-style-type: none"> WHALING SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK

Answer:

Question
Show

Attacks

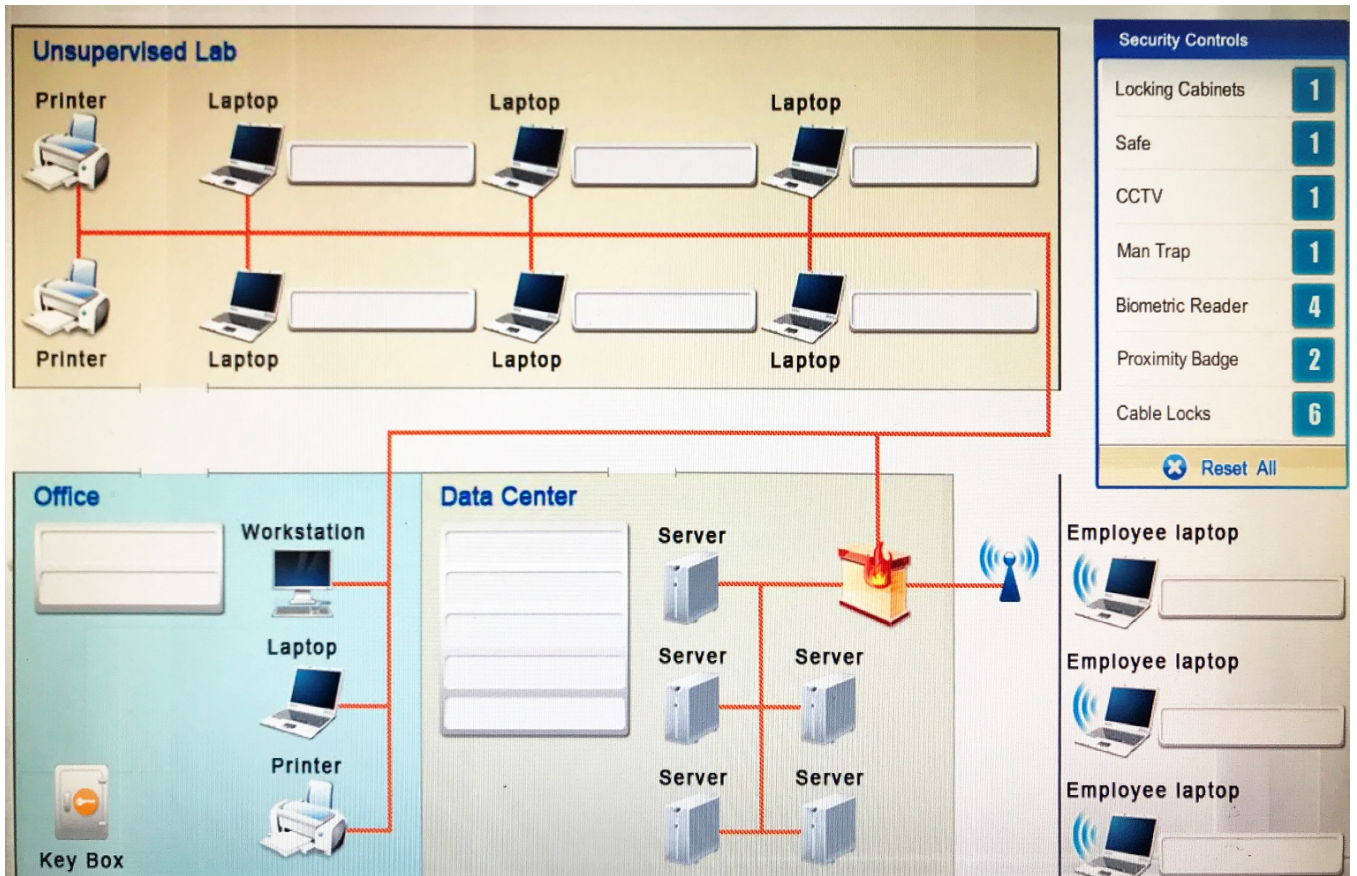
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

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

Question
Show

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.**

Unsupervised Lab

Printer Laptop Cable Locks Laptop Cable Locks Laptop Cable Locks

Printer Laptop Cable Locks Laptop Cable Locks Laptop Cable Locks

Office

Proximity Badge Workstation Laptop Printer

Key Box

Data Center

CCTV Proximity Badge Man Trap Locking Cabinets Biometric Reader

Server Server Server

Security Controls

Locking Cabinets	0
Safe	0
CCTV	0
Man Trap	0
Biometric Reader	0
Proximity Badge	0
Cable Locks	0

Reset All

Employee laptop

Biometric Reader

Employee laptop

Biometric Reader

Employee laptop

Biometric Reader

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