

KillTest

高品質 より良いサービス



練習問題

<https://www.killtest.jp>

1年間無料アップデート

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, there is a list of controls 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
- Mantrap

On the right, there are two asset types with placeholder boxes for controls:

- Company Managed Smart Phone** (represented by a smartphone icon)
- Data Center Terminal Server** (represented by a server rack icon)

At the bottom center, there is a 'Reset All' button. On the bottom right, there is a 'Question' box with the following text:

Question

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?

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.

Below the instructions is a 'Done' button and a note: 'This window can be resized.'

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

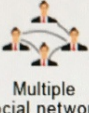
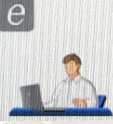
2.HOTSPOT

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
 Attacker gains confidential company information	 Targeted CEO and board members	- SPIM - VISHING - PHISHING - WHALING - HOAX - PHARMING - SPEAR PHISHING - SPOOFING - SPAM - XMAS ATTACK
 Attacker posts link to fake AV software	 Multiple social networks	- SPIM - VISHING - PHISHING - WHALING - HOAX - PHARMING - SPEAR PHISHING - SPOOFING - SPAM - XMAS ATTACK
 Attacker collecting credit card details	 Phone-based victim	- 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	- SPIM - VISHING - PHISHING - WHALING - HOAX - PHARMING - SPEAR PHISHING - SPOOFING - SPAM - XMAS ATTACK
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims Fraudulent site Legitimate site	- SPIM - VISHING - PHISHING - WHALING - HOAX - PHARMING - SPEAR PHISHING - SPOOFING - SPAM - XMAS ATTACK

Answer:

Question
 Show

Attacks

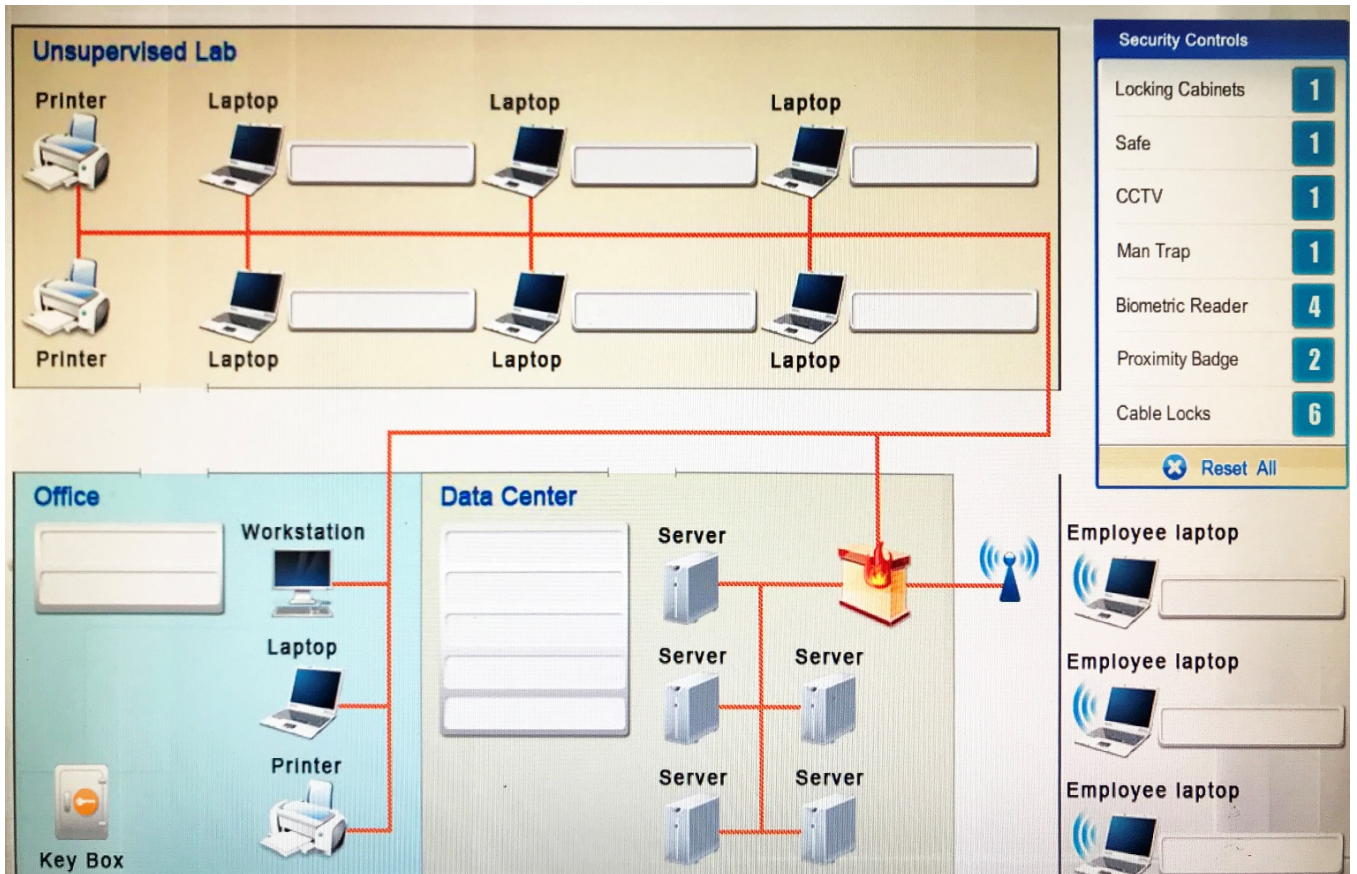
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector		Target	Identified Attack
 Attacker gains confidential company information	➔	 Targeted CEO and board members	SPEAR PHISHING
 Attacker posts link to fake AV software	➔	 Multiple social networks	HOAX
 Attacker collecting credit card details	➔	 Phone-based victim	VISHING
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	➔	 Broad set of recipients	PHISHING
 Attacker redirects name resolution entries from legitimate site to fraudulent site	➔	 ➔ Fraudulent site ➔ Legitimate site Victims	PHARMING

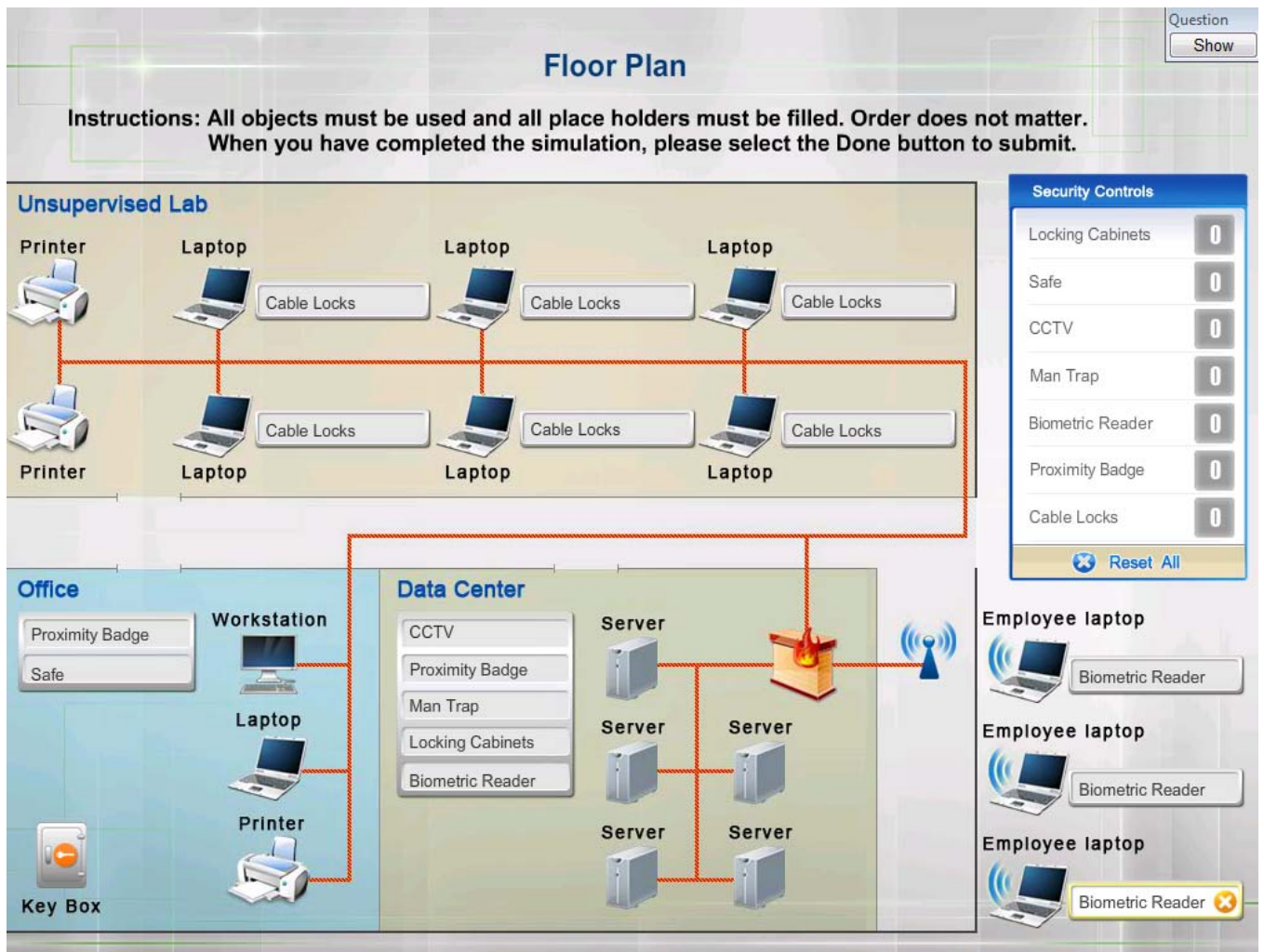
3.DRAG DROP

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

Answer: B