KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **SY0-501**

Title : CompTIA Security+

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 type.

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

Controls
Screen Locks
Strong Password
Device Encryption
Remote Wipe
GPS Tracking
Pop-up Blocker
Cable Locks
Antivirus
Host Based Firewall
Proximity Reader
Sniffer
Mentor app

Company Manager Smart Phone


Data Center Terminal Server


Answer:

Controls
Screen Locks
Strong Password
Device Encryption
Remote Wipe
GPS Tracking
Pop-up Blocker
Cable Locks
Antivirus
Host Based Firewall
Proximity Reader
Sniffer
Mentor app

Company Manager Smart Phone

Screen Locks
Strong Password
Device Encryption
Remote Wipe
GPS Tracking
Pop-up Blocker

Data Center Terminal Server

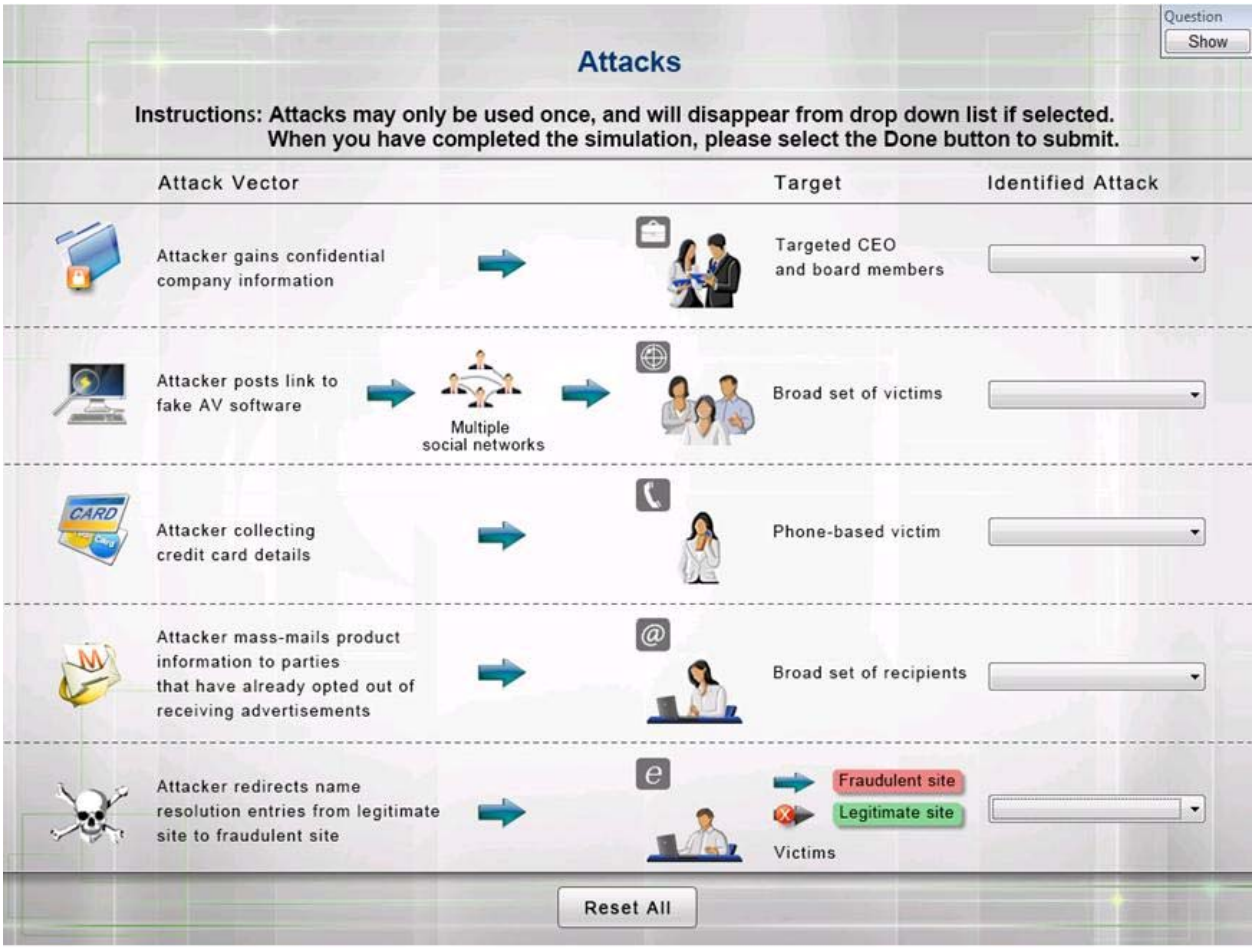
Cable Locks
Antivirus
Host Based Firewall
Proximity Reader
Sniffer
Mentor app

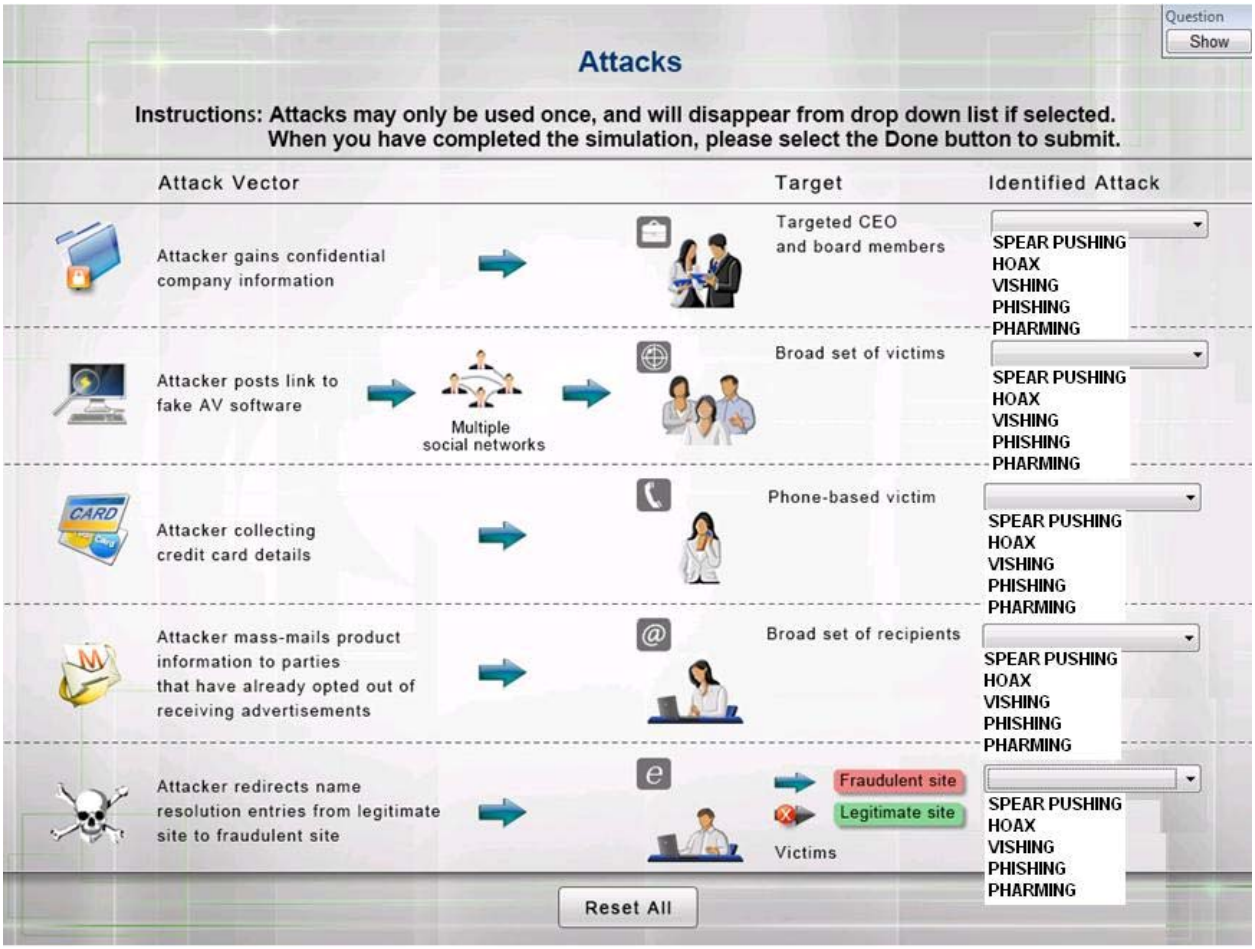
Explanation:

Cable locks are used as a hardware lock mechanism – thus best used on a Data Center Terminal Server.

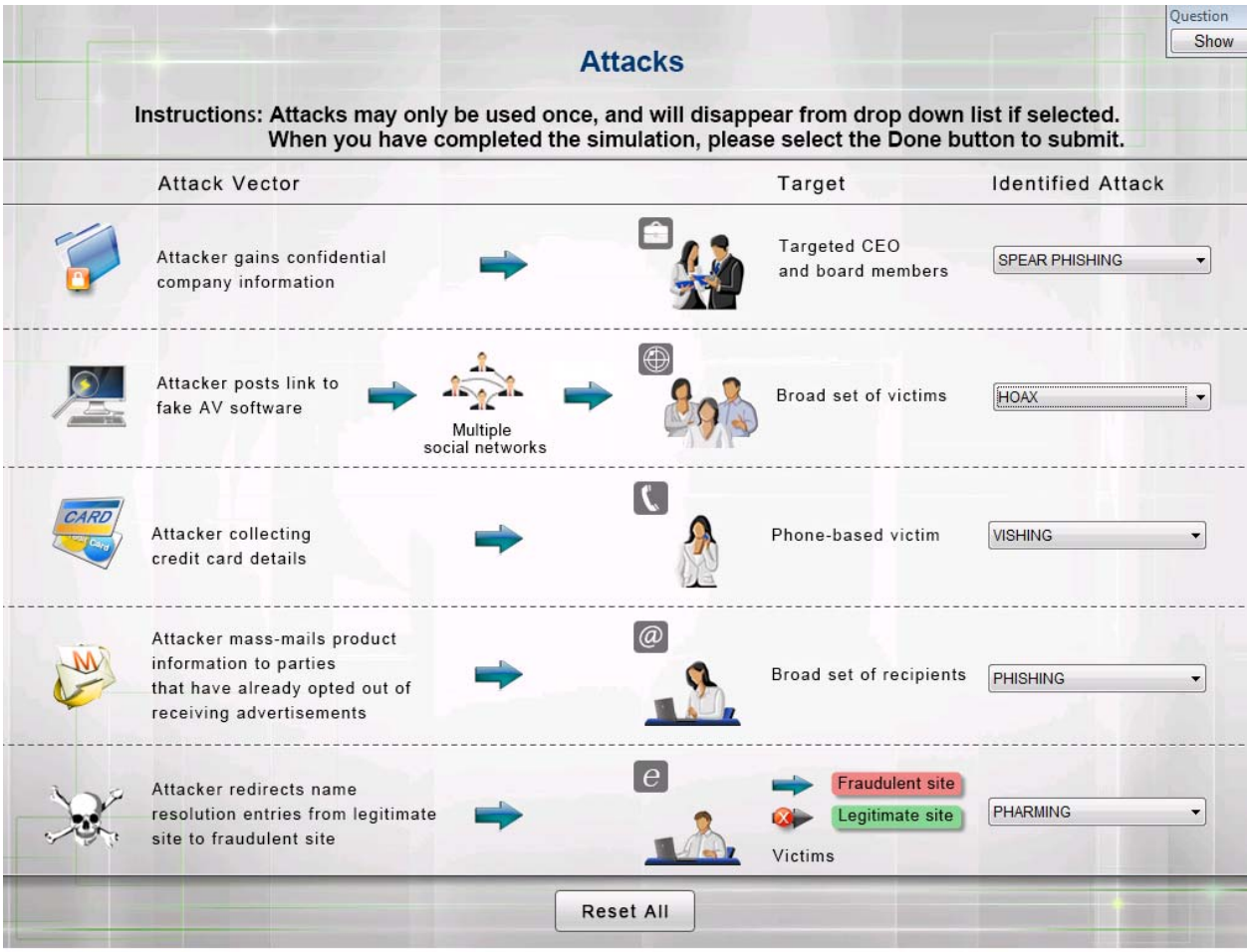
Network monitors are also known as sniffers – thus best used on a Data Center Terminal Server.
Install antivirus software. Antivirus software should be installed and definitions kept current on all hosts. Antivirus software should run on the server as well as on every workstation. In addition to active monitoring of incoming fi les, scans should be conducted regularly to catch any infections that have slipped through- thus best used on a Data Center Terminal Server.
Proximity readers are used as part of physical barriers which makes it more appropriate to use on a center's entrance to protect the terminal server.
Mentor app is an Apple application used for personal development and is best used on a mobile device such as a smart phone.
Remote wipe is an application that can be used on devices that are stolen to keep data safe. It is basically a command to a phone that will remotely clear the data on that phone. This process is known as a remote wipe, and it is intended to be used if the phone is stolen or going to another user.
Should a device be stolen, GPS (Global Positioning System) tracking can be used to identify its location and allow authorities to find it - thus best used on a smart phone.
Screen Lock is where the display should be configured to time out after a short period of inactivity and the screen locked with a password. To be able to access the system again, the user must provide the password. After a certain number of attempts, the user should not be allowed to attempt any additional logons; this is called lockout – thus best used on a smart phone.
Strong Password since passwords are always important, but even more so when you consider that the device could be stolen and in the possession of someone who has unlimited access and time to try various values – thus best use strong passwords on a smartphone as it can be stolen more easily than a terminal server in a data center.
Device Encryption- Data should be encrypted on the device so that if it does fall into the wrong hands, it cannot be accessed in a usable form without the correct passwords. It is recommended to you use Trusted Platform Module (TPM) for all mobile devices where possible.
Use pop-up blockers. Not only are pop-ups irritating, but they are also a security threat. Pop-ups (including pop-unders) represent unwanted programs running on the system, and they can jeopardize the system's well-being. This will be more effective on a mobile device rather than a terminal server.
Use host-based firewalls. A firewall is the first line of defense against attackers and malware. Almost every current operating system includes a firewall, and most are turned on by Default- thus best used on a Data Center Terminal Server.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 221, 222, 369, 418
http://www.mentor-app.com/

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.


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
Attacker posts link to fake AV software
Multiple social networks
Broad set of victims
Attacker collecting credit card details
Phone-based victim
Attacker mass-mails product information to parties that have already opted out of receiving advertisements
Broad set of recipients
Attacker redirects name resolution entries from legitimate site to fraudulent site
Fraudulent site
Legitimate site
Victims
Reset All


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
Attacker posts link to fake AV software
Multiple social networks
Broad set of victims
Attacker collecting credit card details
Phone-based victim
Attacker mass-mails product information to parties that have already opted out of receiving advertisements
Broad set of recipients
Attacker redirects name resolution entries from legitimate site to fraudulent site
Fraudulent site
Legitimate site
Victims
SPEAR PUSHING
HOAX
VISHING
PHISHING
PHARMING
Reset All

Answer:



Explanation:

1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti-virus) software is genuine.

3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

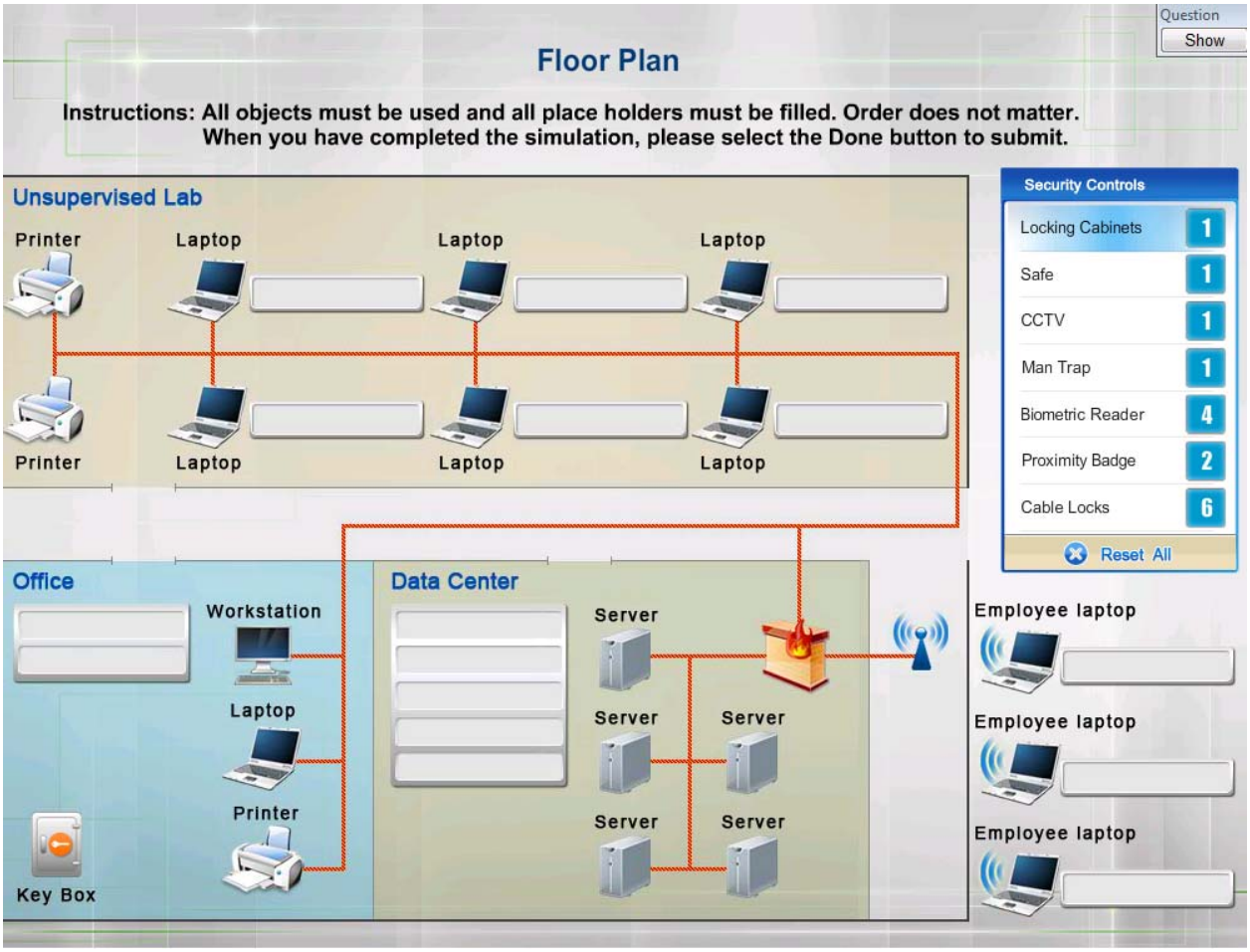
4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

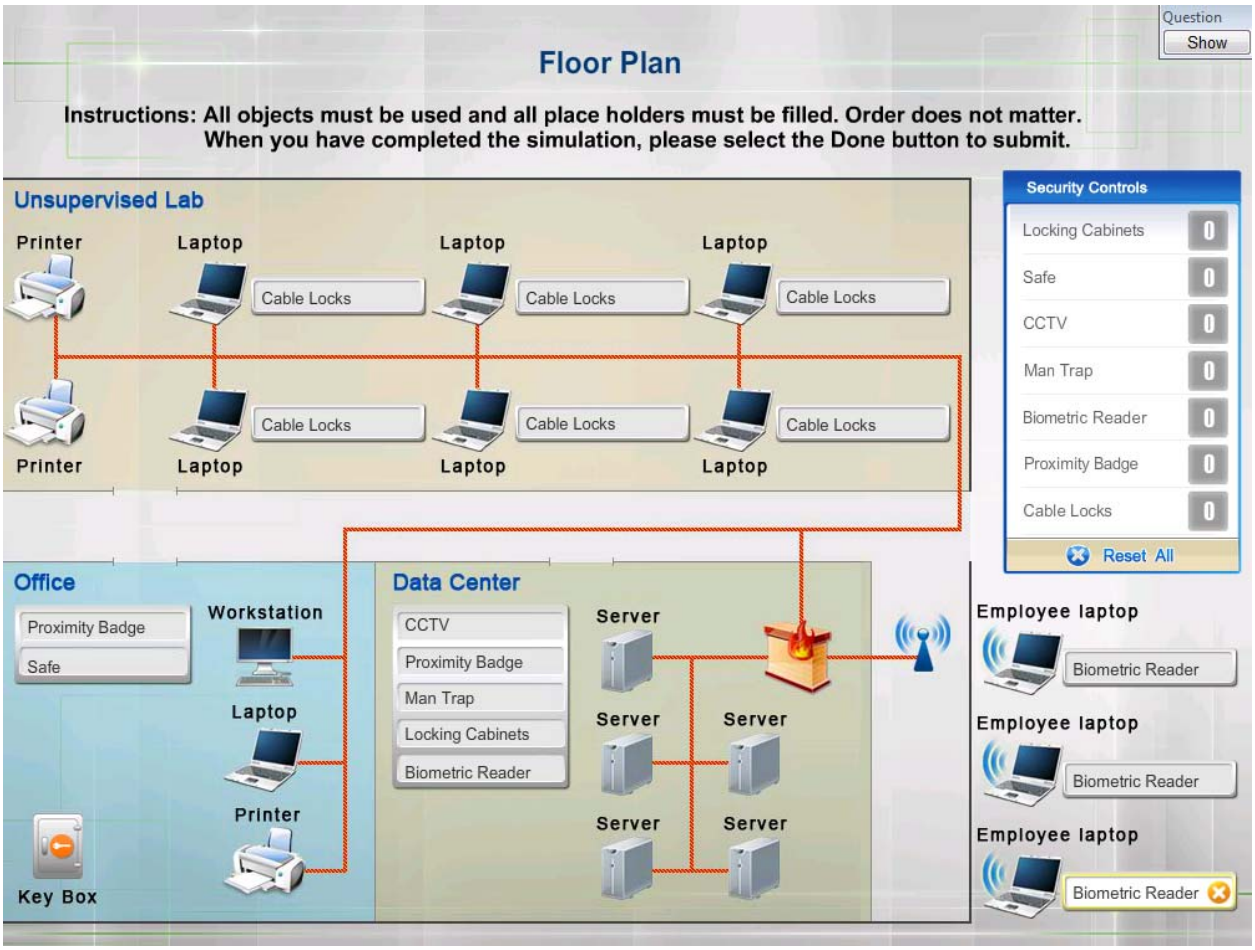
5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and

mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.
References:
http://searchsecurity.techtarget.com/definition/spear-phishing
http://www.webopedia.com/TERM/V/vishing.html
http://www.webopedia.com/TERM/P/phishing.html
http://www.webopedia.com/TERM/P/pharming.html

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:



Explanation:
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away
Proximity badge + reader
Safe is a hardware/physical security measure
Mantrap can be used to control access to sensitive areas.
CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access.
Locking cabinets can be used to protect backup media, documentation and other physical artefacts.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 369

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: B

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 207.46.130.6666. 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: A