KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

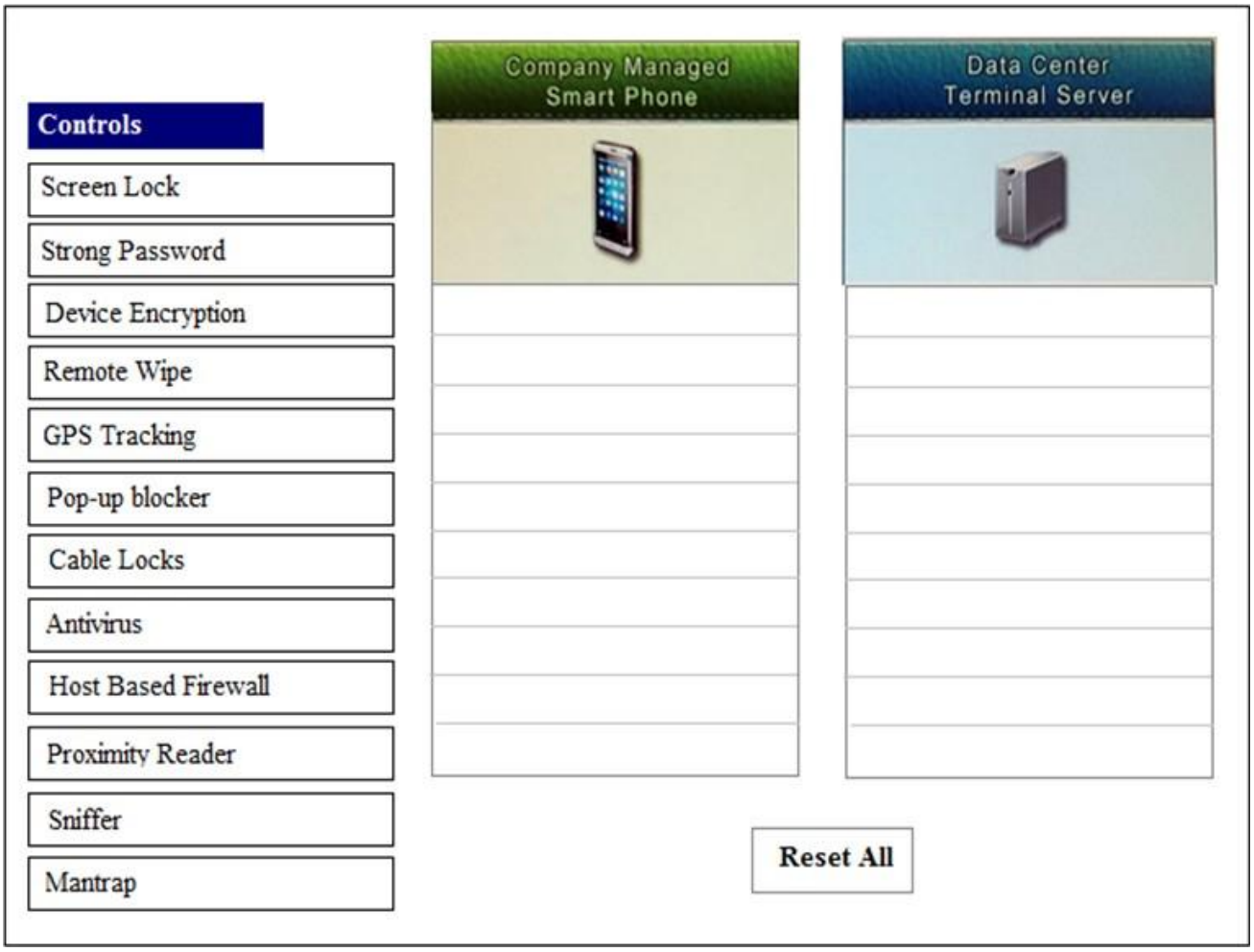
Exam : SY0-501

Title : CompTIA Security+

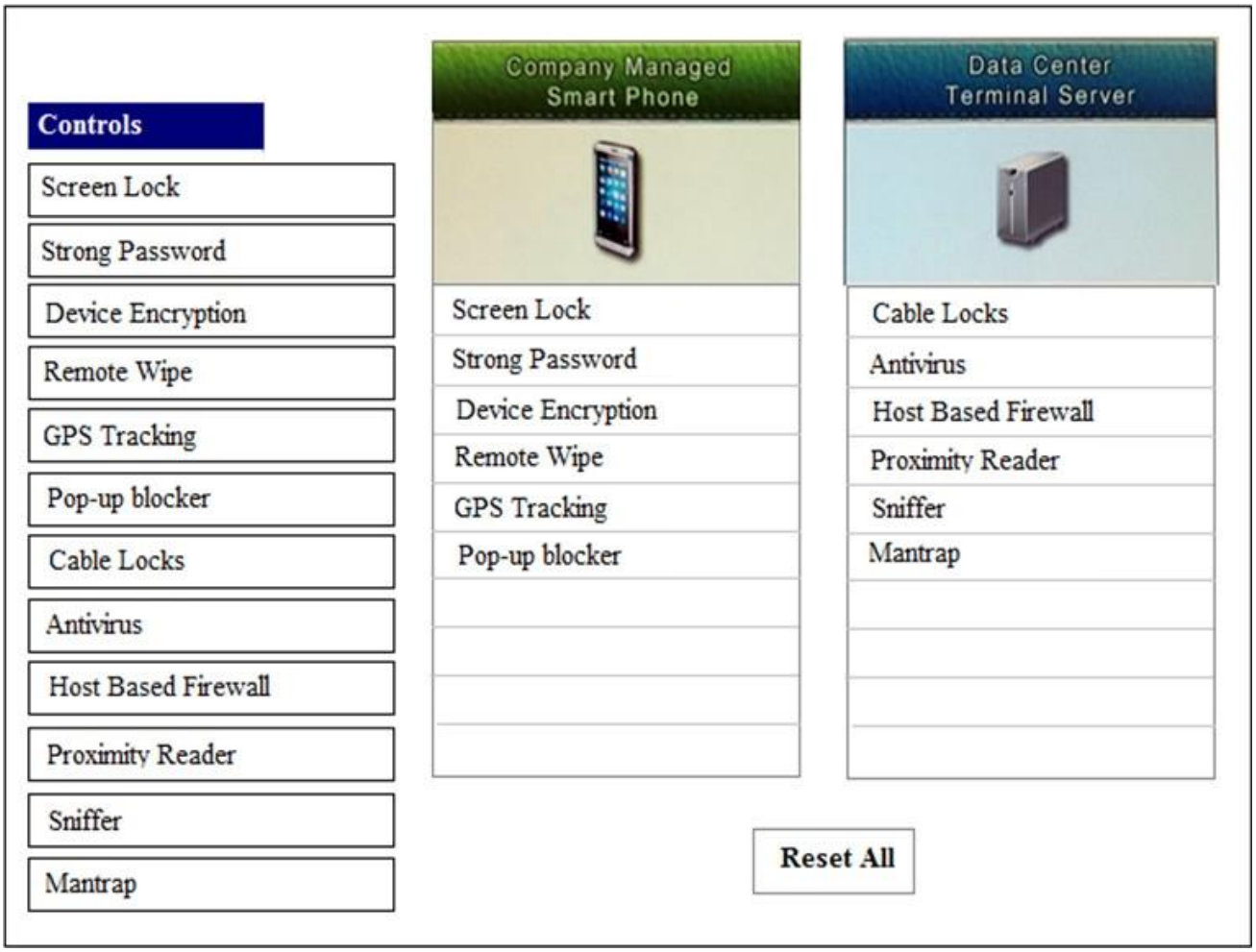
Version : DEMO

1.DRAG DROP
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center.

INSTRUCTIONS
Drag and drop the applicable controls to each asset type.
Controls can be used multiple times and not all placeholders need to be filled.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:



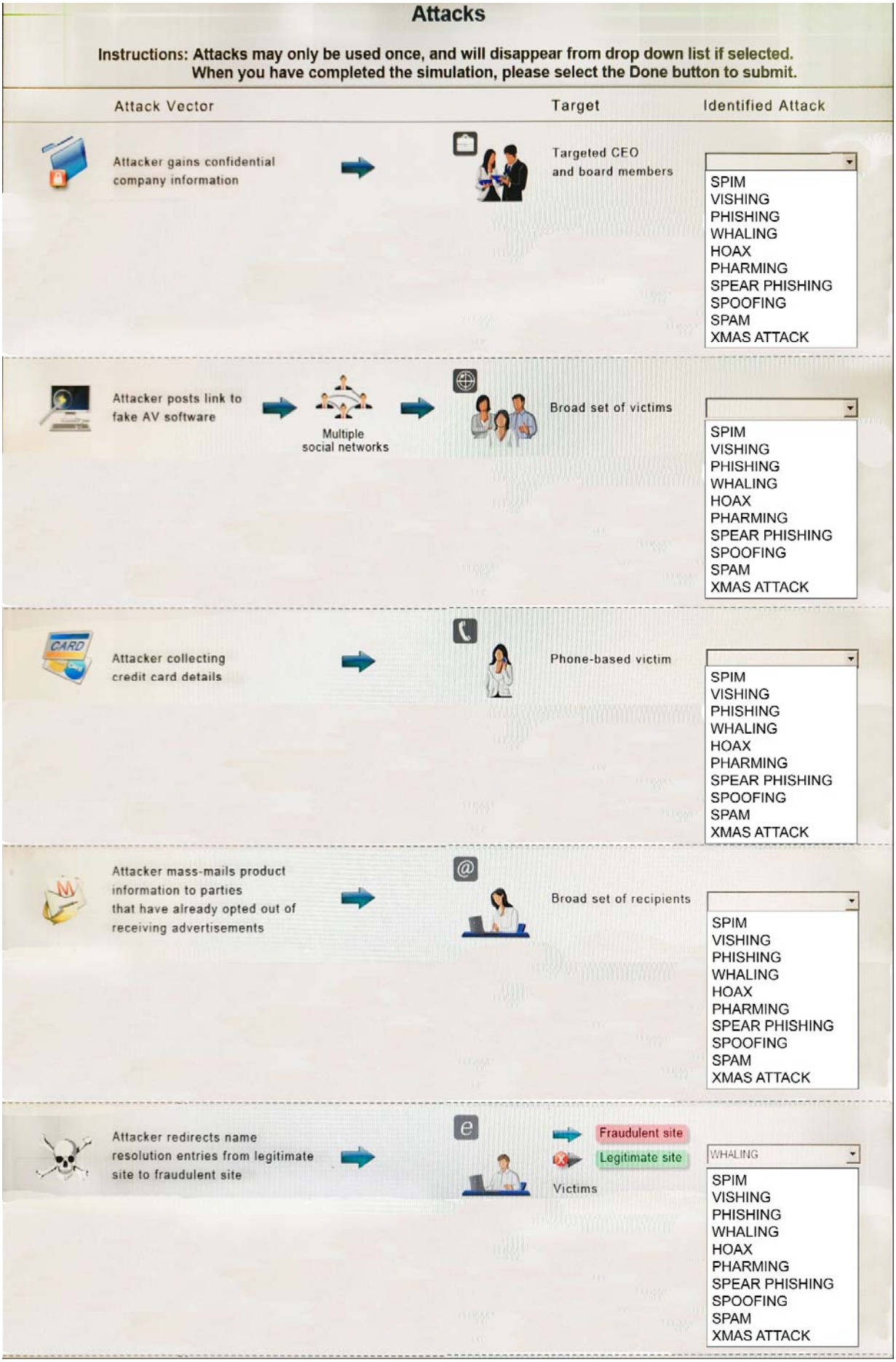
2.HOTSPOT

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
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
WHALING
SPIM
VISHING
PHISHING
WHALING
HOAX
PHARMING
SPEAR PHISHING
SPOOFING
SPAM
XMAS ATTACK

Answer:

Attacks

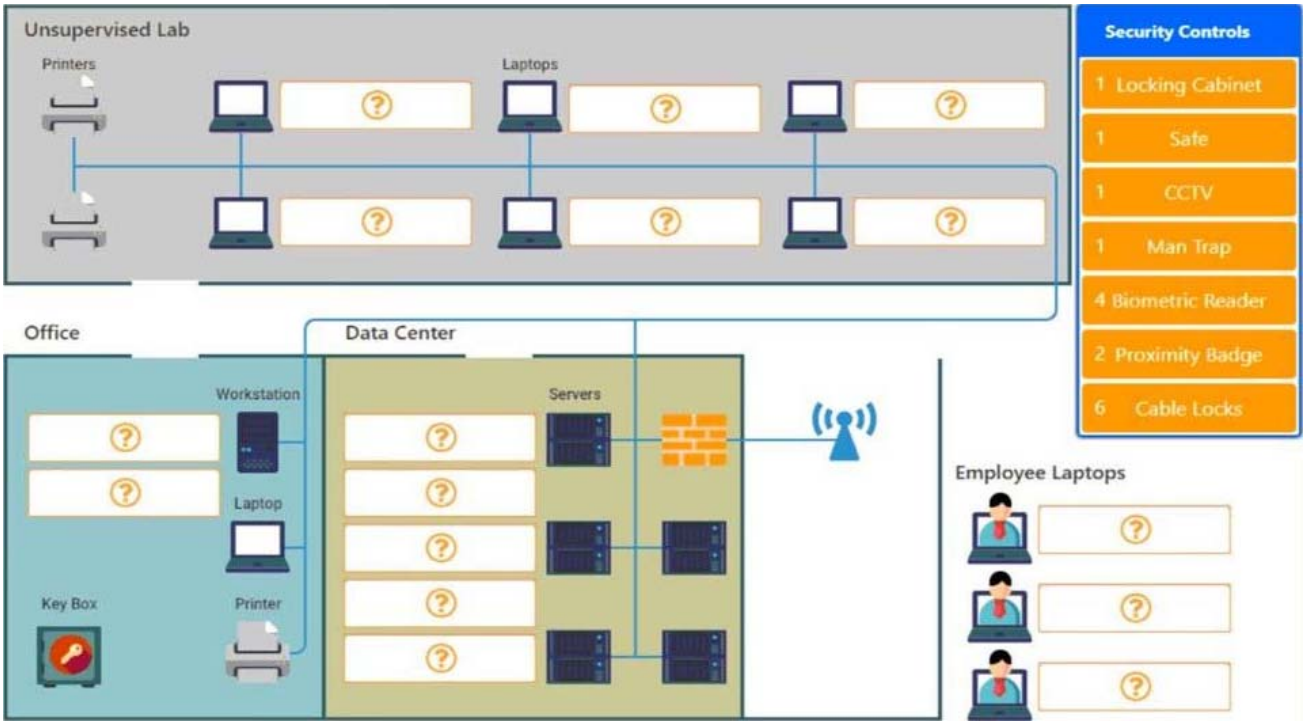
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
Attacker gains confidential company information	Targeted CEO and board members	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	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	Fraudulent site / Legitimate site → Victims	WHALING → SPIM, VISHING, PHISHING, WHALING, HOAX, **PHARMING**, SPEAR PHISHING, SPOOFING, SPAM, XMAS ATTACK

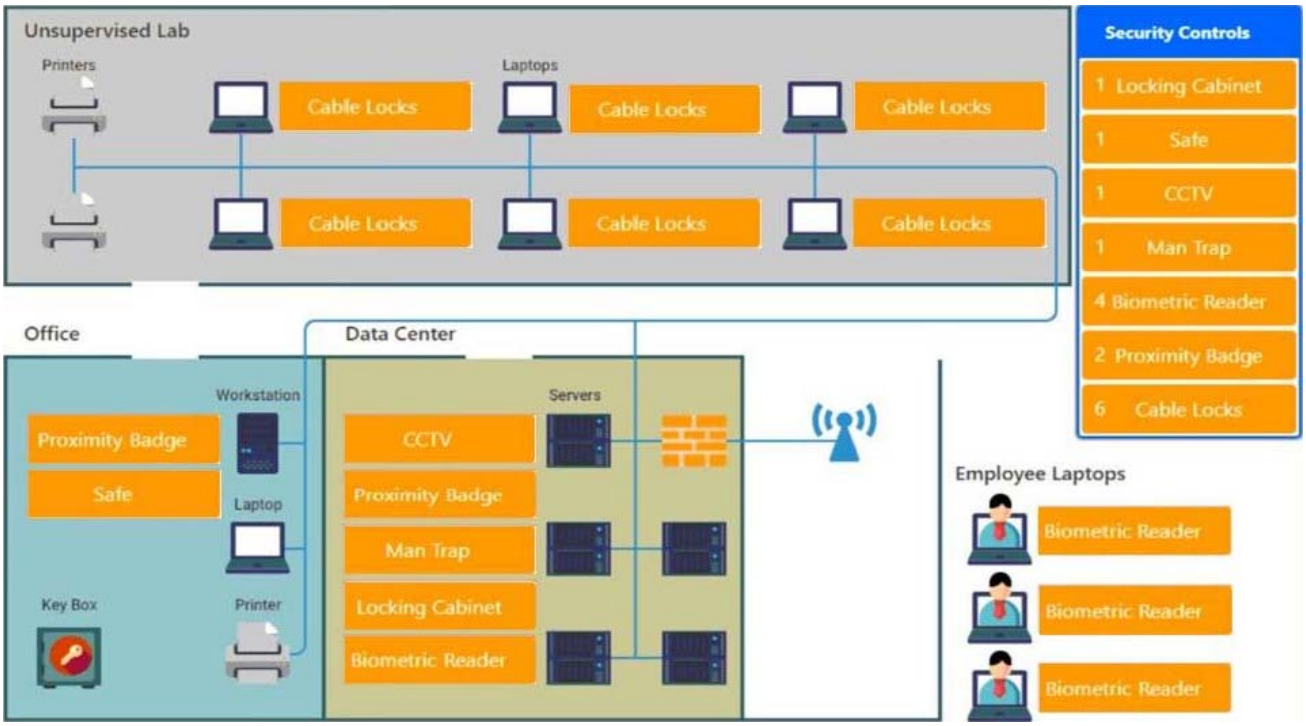
Explanation:
1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages 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: Email spam, also referred to as junk email, is unsolicited messages sent in bulk by email (spamming).
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.

INSTRUCTIONS
Drag and drop the appropriate security controls on the floor plan.
All objects must be used and all place holders must be filled. Order does not matter.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



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.

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