

CompTIA Security+

CompTIA SY0-501 Dumps Available Here at:

<https://www.certification-questions.com/comptia-exam/sy0-501-dumps.html>

Enrolling now you will get access to 540 questions in a unique set of SY0-501 dumps

Question 1

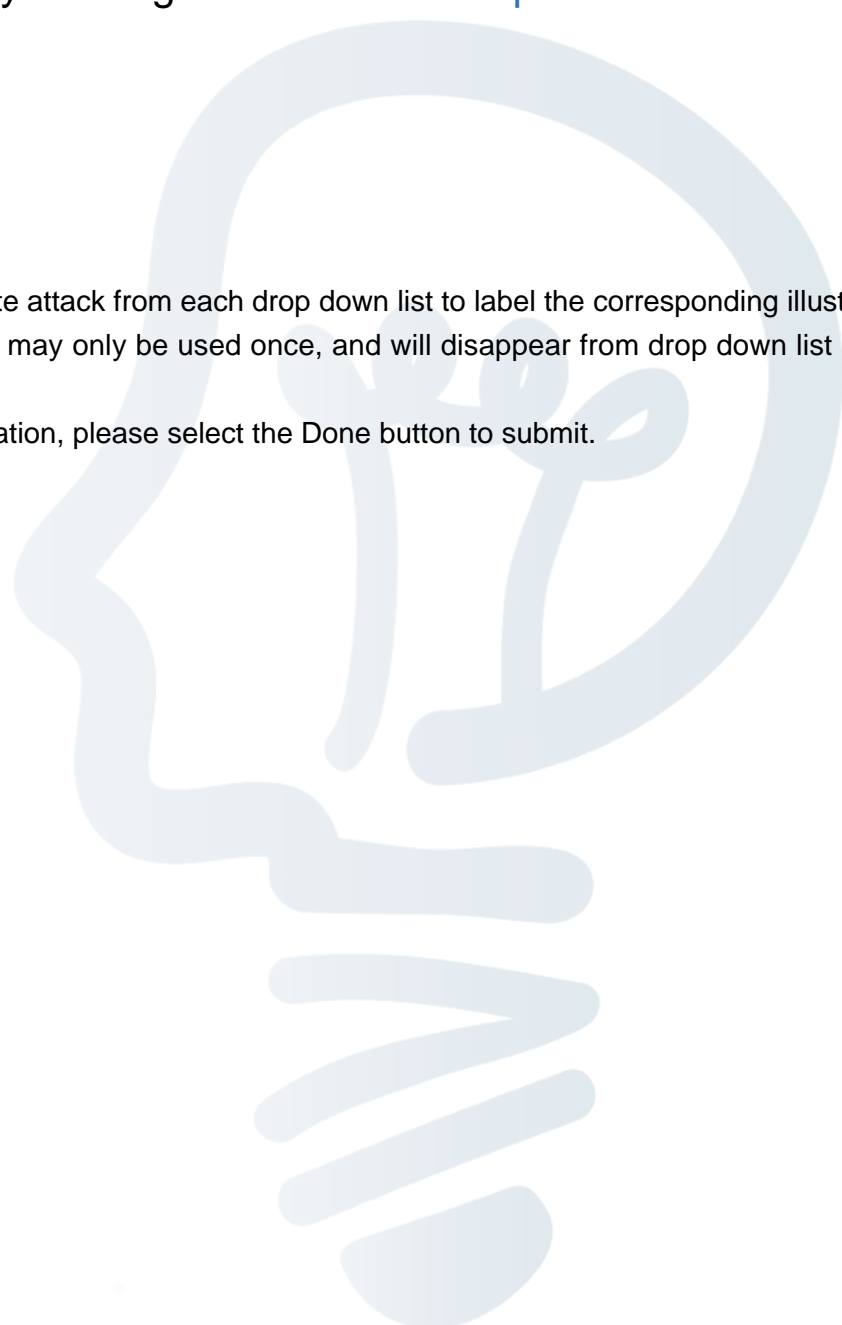
HOTSPOT

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.

Hot Area:



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 style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>SPIM</p> <p>VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p>PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </div>
 <p>Attacker posts link to fake AV software</p>		 <p>Broad set of victims</p>	<div style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>SPIM</p> <p>VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p>PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </div>
 <p>Attacker collecting credit card details</p>		 <p>Phone-based victim</p>	<div style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>SPIM</p> <p>VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p>PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </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 style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>SPIM</p> <p>VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p>PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </div>
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>		 <p>Victims</p>	<div style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>WHALING</p> <p>SPIM</p> <p>VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p>PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </div>












Options:

A.



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 style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>SPIM</p> <p>VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p>PHARMING</p> <p style="background-color: #e0ffe0;">SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </div>
 <p>Attacker posts link to fake AV software</p>	➔	 <p>Multiple social networks</p>	➔
		 <p>Broad set of victims</p>	<div style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>SPIM</p> <p>VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p style="background-color: #e0ffe0;">HOAX</p> <p>PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </div>
 <p>Attacker collecting credit card details</p>	➔	 <p>Phone-based victim</p>	<div style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>SPIM</p> <p style="background-color: #e0ffe0;">VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p>PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </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 style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p>SPIM</p> <p>VISHING</p> <p style="background-color: #e0ffe0;">PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p>PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </div>
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>	➔	 <p>Victims</p>	<div style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; padding-bottom: 2px;">▼</div> <p style="background-color: #e0ffe0;">WHALING</p> <p>SPIM</p> <p>VISHING</p> <p>PHISHING</p> <p>WHALING</p> <p>HOAX</p> <p style="background-color: #e0ffe0;">PHARMING</p> <p>SPEAR PHISHING</p> <p>SPOOFING</p> <p>SPAM</p> <p>XMAS ATTACK</p> </div>

Answer: A

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>

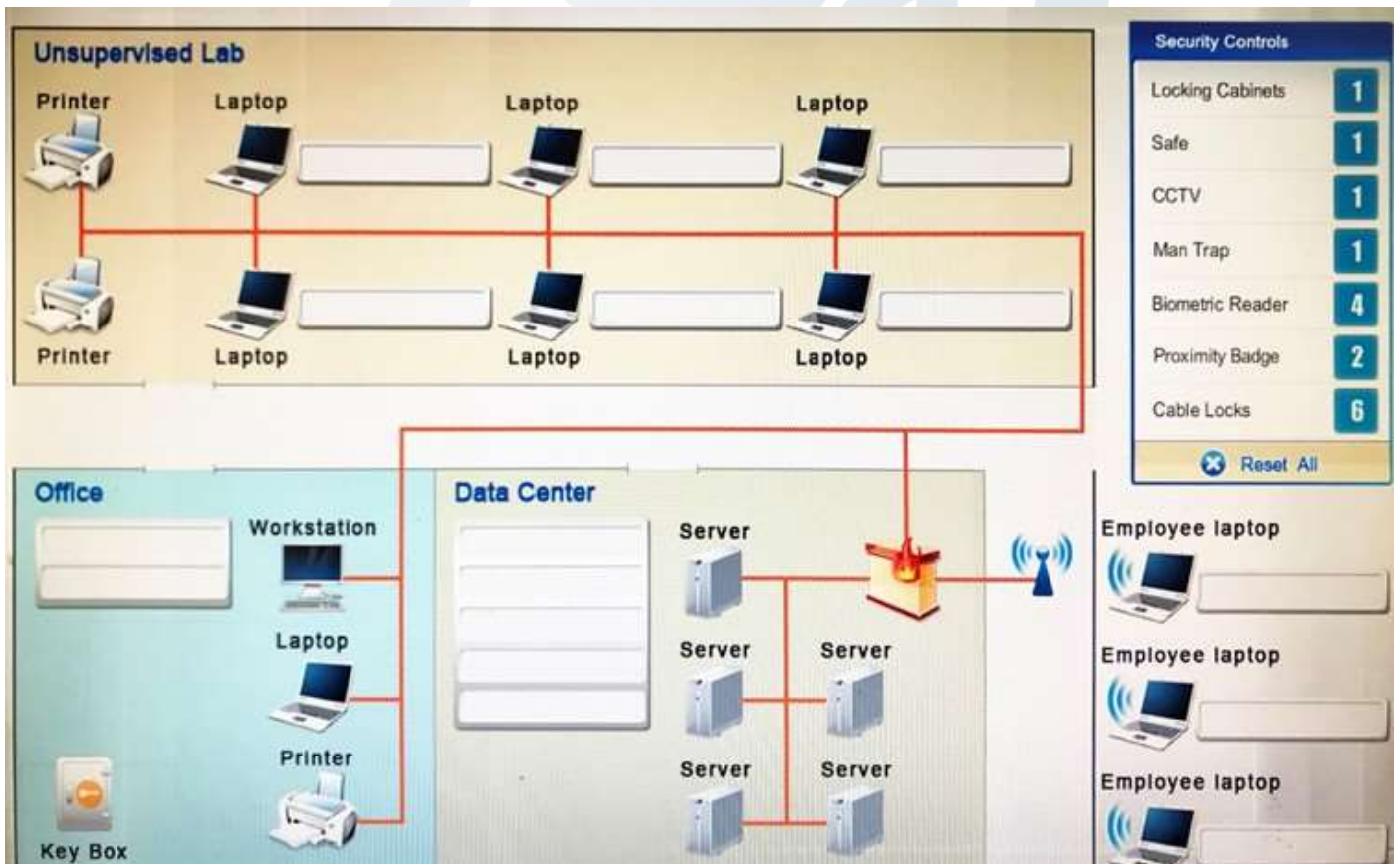
Question 2

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.

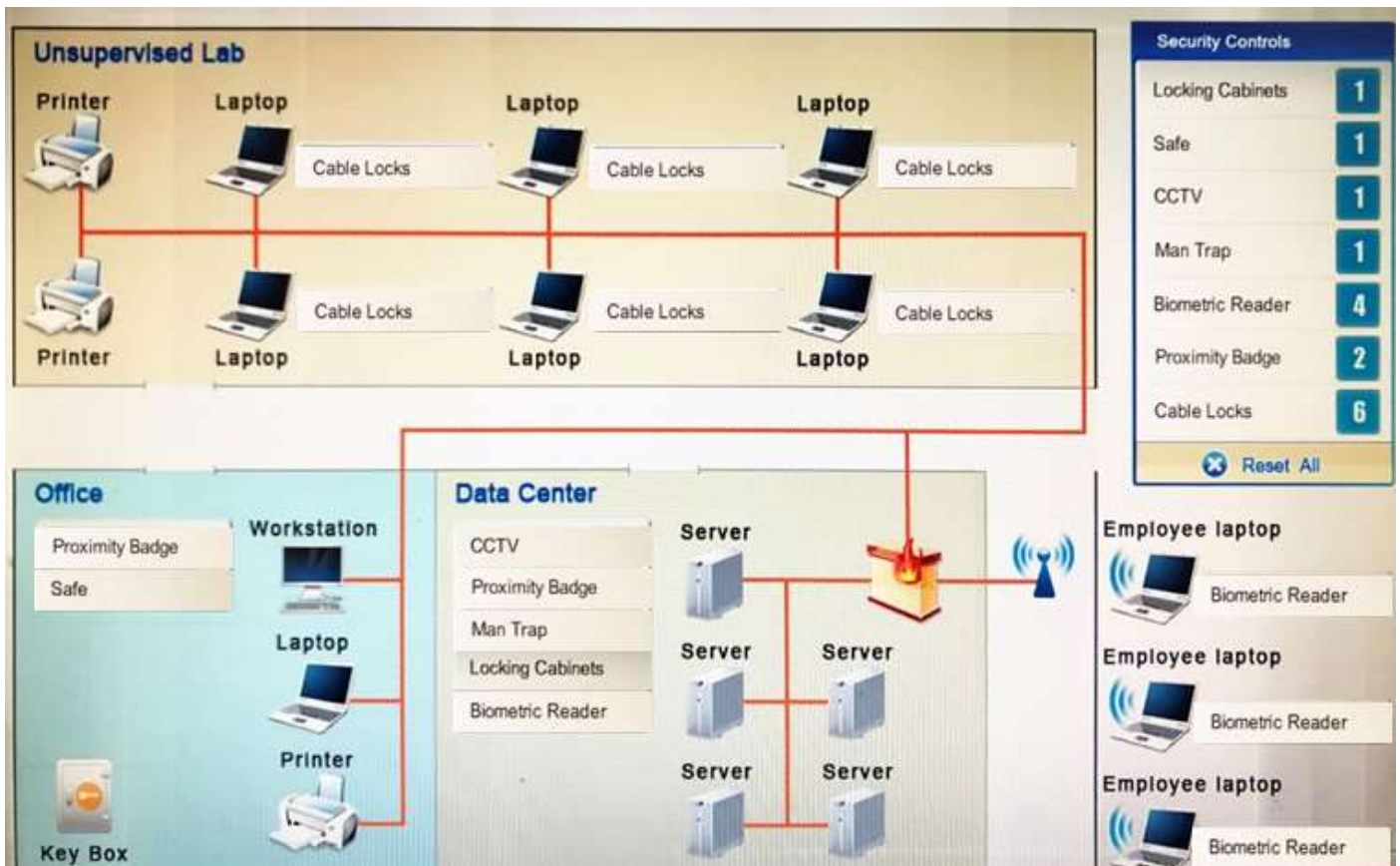
Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.

Select and Place:



Options:

A.



Answer: A

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.

Question 3

In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has

requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

Options:

- A. Elasticity
- B. Scalability
- C. High availability
- D. Redundancy

Answer: A

Explanation:

Elasticity is defined as "the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible".

Question 4

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.

Select and Place:

Controls	Company Managed Smart Phone	Data Center Terminal Server
Screen Lock		
Strong Password		
Device Encryption		
Remote Wipe		
GPS Tracking		
Pop-up blocker		
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mantrap		
	Reset All	

Options:

A.

Controls	Company Managed Smart Phone	Data Center Terminal Server
Screen Lock	Screen Lock	Cable Locks
Strong Password	Strong Password	Antivirus
Device Encryption	Device Encryption	Host Based Firewall
Remote Wipe	Remote Wipe	Proximity Reader
GPS Tracking	GPS Tracking	Sniffer
Pop-up blocker	Pop-up blocker	Mantrap
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mantrap		

Reset All

Answer: A

Explanation:

:

Question 5

Which of the following would a security specialist be able to determine upon examination of a server's certificate?

Options:

- A. CA public key
- B. Server private key
- C. CSR

D. OID

Answer: D

Question 6

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?

Options:

A. tracert

B. netstat

C. ping

D. nslookup

Answer: B

Question 7

Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

Options:

A. Shibboleth

B. RADIUS federation

C. SAML

D. OAuth

E. OpenID connect

Answer: B

Explanation:

Explanation: <http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html>

Question 8

Which of the following BEST describes an important security advantage yielded by implementing vendor

diversity?

Options:

- A. Sustainability
- B. Homogeneity
- C. Resiliency
- D. Configurability

Answer: C

Question 9

A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

Options:

- A. PFX
- B. PEM
- C. DER
- D. CER

Answer: B

Question 10

Which of the following attacks specifically impact data availability?

Options:

- A. DDoS
- B. Trojan
- C. MITM
- D. Rootkit

Answer: A

Explanation:

Reference: <https://www.netscout.com/what-is-ddos>

Would you like to see more? Don't miss our SY0-501 PDF file at:

<https://www.certification-questions.com/comptia-pdf/sy0-501-pdf.html>

