



examkill
affordable exams preparation material

Comptia

RC0-501

CompTIA Security+ Recertification Exam

For More Information – Visit link below:

<http://www.examkill.com/>

Version product

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.

Question
Show

Attacks













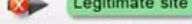
Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.

Attack Vector		Target	Identified Attack
 <p>Attacker gains confidential company information</p>	➔	 <p>Targeted CEO and board members</p>	<input type="text"/>
 <p>Attacker posts link to fake AV software</p>	➔	 <p>Multiple social networks</p>	
	➔	 <p>Broad set of victims</p>	<input type="text"/>
 <p>Attacker collecting credit card details</p>	➔	 <p>Phone-based victim</p>	<input type="text"/>
 <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"/>
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>	➔	 <p> ➔ Fraudulent site ➔ Legitimate site Victims </p>	<input type="text"/>

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.

















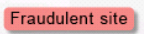
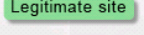

Attack Vector	Target	Identified Attack
 <p>Attacker gains confidential company information</p>	 <p>Targeted CEO and board members</p>	<input type="text" value="SPEAR PUSHING"/> <input type="text" value="HOAX"/> <input type="text" value="VISHING"/> <input type="text" value="PHISHING"/> <input type="text" value="PHARMING"/>
 <p>Attacker posts link to fake AV software</p>	 <p>Multiple social networks</p>  <p>Broad set of victims</p>	<input type="text" value="SPEAR PUSHING"/> <input type="text" value="HOAX"/> <input type="text" value="VISHING"/> <input type="text" value="PHISHING"/> <input type="text" value="PHARMING"/>
 <p>Attacker collecting credit card details</p>	 <p>Phone-based victim</p>	<input type="text" value="SPEAR PUSHING"/> <input type="text" value="HOAX"/> <input type="text" value="VISHING"/> <input type="text" value="PHISHING"/> <input type="text" value="PHARMING"/>
 <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="SPEAR PUSHING"/> <input type="text" value="HOAX"/> <input type="text" value="VISHING"/> <input type="text" value="PHISHING"/> <input type="text" value="PHARMING"/>
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>	 <p>Victims</p>  	<input type="text" value="SPEAR PUSHING"/> <input type="text" value="HOAX"/> <input type="text" value="VISHING"/> <input type="text" value="PHISHING"/> <input type="text" value="PHARMING"/>

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>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>	    <p>Victims</p>	<input type="text" value="PHARMING"/>

Explanation:

1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data

a. 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.

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 Laptop Laptop
Printer Laptop Laptop Laptop

Office

Workstation
Laptop
Printer
Key Box

Data Center

Server Server
Server Server
Server Server

Security Controls

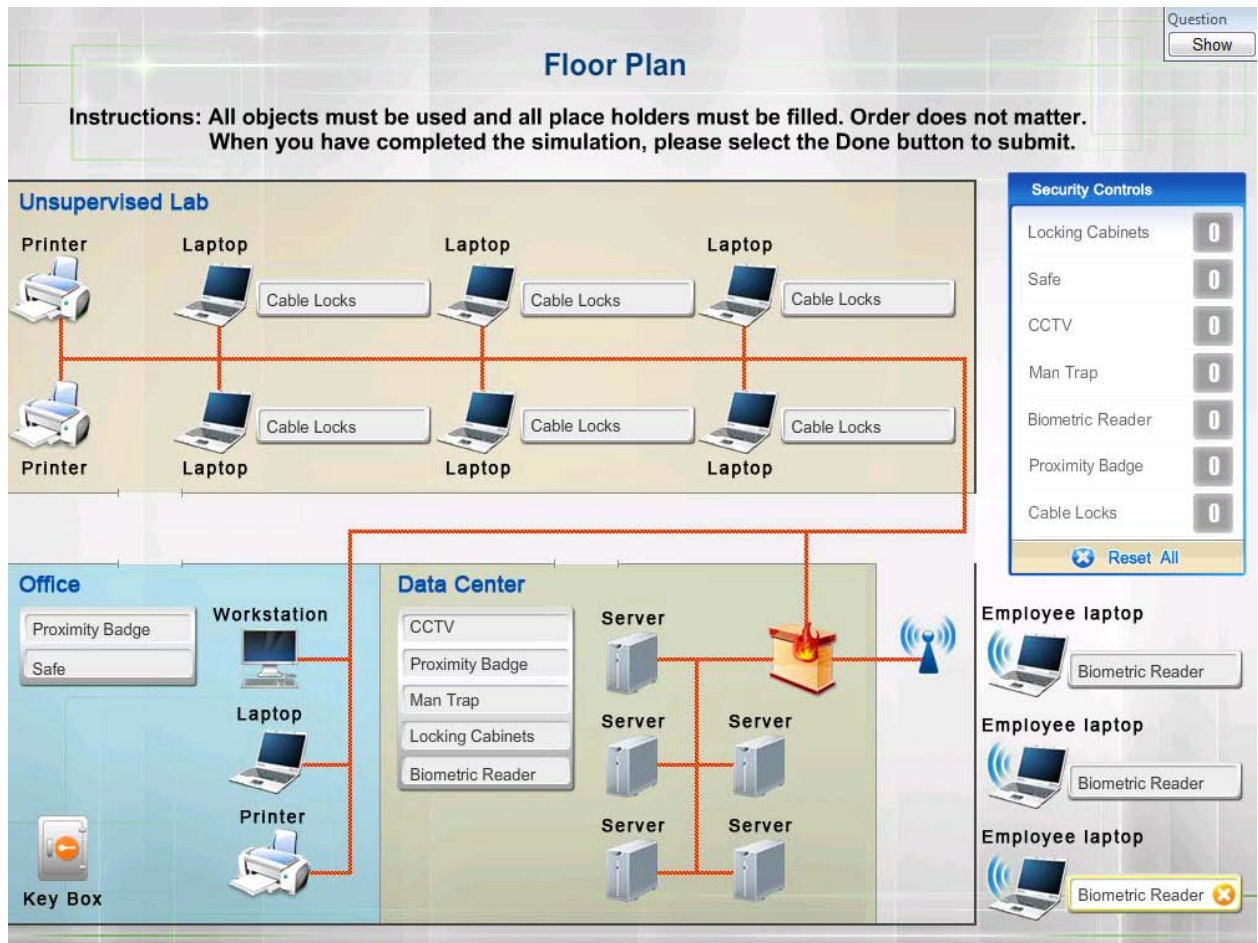
Locking Cabinets	1
Safe	1
CCTV	1
Man Trap	1
Biometric Reader	4
Proximity Badge	2
Cable Locks	6

Reset All

Employee laptop

Employee laptop
Employee laptop
Employee laptop

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

Question: 3

DRAG DROP

Drag and drop the correct protocol to its default port.

FTP	<input type="checkbox"/>
Telnet	<input type="checkbox"/>
SMTP	<input type="checkbox"/>
SNMP	<input type="checkbox"/>
SCP	<input type="checkbox"/>
TFTP	<input type="checkbox"/>

161

22

21

69

25

23

Answer:

FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

Explanation:

FTP uses TCP port 21.

Telnet uses port 23.

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

SMTP uses TCP port 25.

Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162.

References:

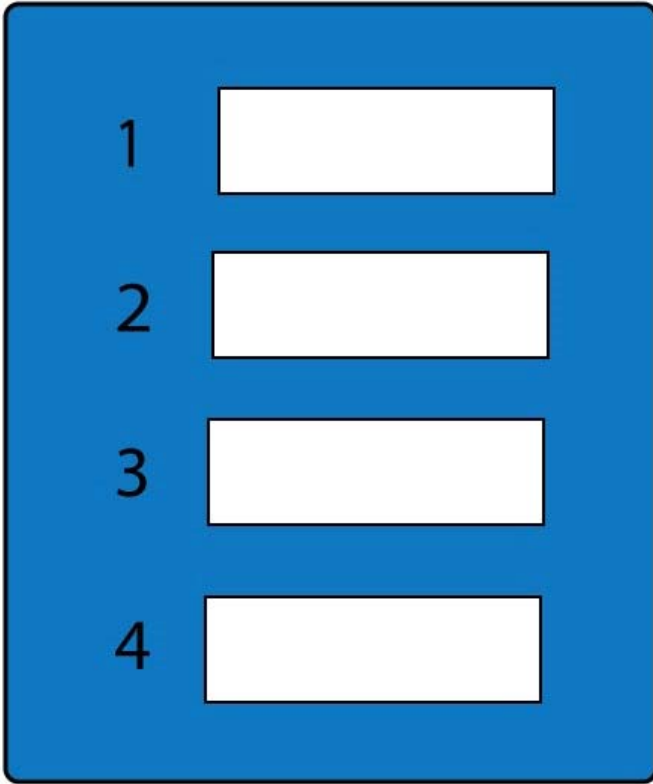
Stewart, James Michael, *CompTIA Security+ Review Guide*, Sybex, Indianapolis, 2014, pp. 42, 45, 51

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Question: 4

DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.



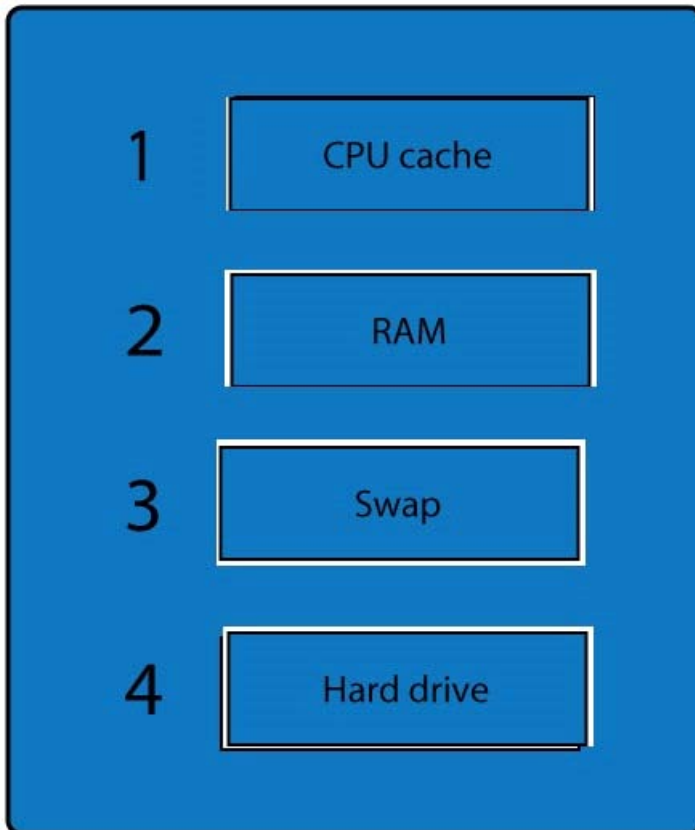
RAM

CPU cache

Swap

Hard drive

Answer:



Explanation:

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/ hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 453

Question: 5

The compute resource center issued smartphones to all first-level and above managers. The managers have the ability to install mobile tools. Which of the following tools should be implemented to control the types of tools the managers install?

- A. Download manager
- B. Content manager
- C. Segmentation manager
- D. Application manager

Answer: D

Question: 6

A security analyst reviews the following output:

```
File name: somefile.pdf
File MD5:E289F21CD33E4F57890DDEA5CF267ED2
File size: 1.9Mb
Created by: Jan Smith
Deleted by: Jan Smith
Date deleted: October 01, 2015 8:43:21 EST
```

The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the SIEM reports the following.

File hash: E289F21CD33E4F57890DDEA5CF267ED2

File found: somestuff.xls, somefile.pdf, nofile.doc

Which of the following is the MOST likely cause of the hash being found in other areas?

- A. Jan Smith is an insider threat.
- B. There are MD5 has collisions
- C. The file is encrypted.
- D. Shadow copies are present.

Answer: D

Question: 7

A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would Best prevent this type of attack?

- A. Faraday cage
- B. Smart cards
- C. infrared detection
- D. Alarms

Answer: A

Question: 8

A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to FIRST:

- A. maintain the chain of custody
- B. preserve the data
- C. obtain a legal hold
- D. recover data at a later time

Answer: A

Question: 9

A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

- A. Implement time-of-day restrictions.
- B. Audit file access times.
- C. Secretly install a hidden surveillance camera
- D. Require swipe-card access to enter the lab

Answer: D

Question: 10

A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public C

A. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide. Which of the following solution would be BEST for the security administrator to implement to most efficiently assist with this issue?

- A. SSL
- B. CRL
- C. PKI
- D. ACL

Answer: A

Question: 11

A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

- A. Pre-shared key
- B. Enterprise
- C. WiFi Protected Setup
- D. Captive Portal

Answer: C

Question: 12

A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief information Office (CIO) wants to detect theft of datacenter equipment. Which of the following controls should be implemented?

- A. Biometrics
- B. Cameras
- C. Motion detectors
- D. Mantraps

Answer: C

Question: 13

A security analyst receives a notification from the IDS after working hours, indicating a spike in network traffic. Which of the following BEST describes this type of IDS?

- A. Anomaly-based
- B. Stateful
- C. Host-based
- D. Signature-based

Answer: D

Question: 14

Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

- A. Remote exploit
- B. Amplification
- C. Sniffing
- D. Man-in-the-middle

Answer: C

Question: 15

A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

- A. Open wireless network and SSL VPN
- B. WPA using a preshared key
- C. WPA2 using a RADIUS back-end for 802.1x authentication
- D. WEP with a 40-bit key

Answer: C

For More Information – **Visit link below:**

<http://www.examkill.com>

FEATURES:

- 100% Pass Guarantee
- 30 Days Money Back Guarantee
- 24/7 Live Chat Support (Technical & Sales)
- Instant Download or Email Attachment
- 50,000 +ve Reviews
- 100% Success Rate
- Discounts Available for Bulk Orders

