



**Vendor:** CompTIA

**Exam Code:** SY0-301

**Exam Name:** CompTIA Security+ Certification Exam

**Version:** DEMO

**Added 11 Drag and Drop Questions & Simulator Questions. (See Full Version)**

**QUESTION 1**

Which of the following digital certificate management practices will ensure that a lost certificate is not compromised?

- A. Key escrow
- B. Non-repudiation
- C. Recovery agent
- D. CRL

**Answer: D**











**QUESTION 2**

Hotspot Question

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   |
|---|---|---|
|  <p>Attacker gains confidential company information</p>  |  <p>Targeted CEO and board members</p> | <div>SPEAR PUSHING</div> <div>HOAX</div> <div>VISHING</div> <div>PHISHING</div> <div>PHARMING</div> |
|  <p>Attacker posts link to fake AV software</p>  |  <p>Multiple social networks</p>       | <div>SPEAR PUSHING</div> <div>HOAX</div> <div>VISHING</div> <div>PHISHING</div> <div>PHARMING</div> |
|  <p>Attacker collecting credit card details</p>  |  <p>Phone-based victim</p>             | <div>SPEAR PUSHING</div> <div>HOAX</div> <div>VISHING</div> <div>PHISHING</div> <div>PHARMING</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>SPEAR PUSHING</div> <div>HOAX</div> <div>VISHING</div> <div>PHISHING</div> <div>PHARMING</div> |
|  <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>                         |  <p>Victims</p>                        | <div>SPEAR PUSHING</div> <div>HOAX</div> <div>VISHING</div> <div>PHISHING</div> <div>PHARMING</div> |

Reset All

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

Reset All

### QUESTION 3

A company recently implemented a TLS on their network. The company is MOST concerned with:

- A. Confidentiality
- B. Availability
- C. Integrity
- D. Accessibility

**Answer: A**

### QUESTION 4

Which of the following describes how an attacker can send unwanted advertisements to a mobile device?

- A. Man-in-the-middle
- B. Bluejacking
- C. Bluesnarfing
- D. Packet sniffing

**Answer: B**

### QUESTION 5

A network device that protects an enterprise based only on source and destination addresses is BEST described as:

- A. IDS.
- B. ACL.
- C. Stateful packet filtering.
- D. Simple packet filtering.

**Answer: D**

#### QUESTION 6

A human resources employee receives an email from a family member stating there is a new virus going around. In order to remove the virus, a user must delete the Boot.ini file from the system immediately. This is an example of which of the following?

- A. Hoax
- B. Spam
- C. Whaling
- D. Phishing

**Answer: A**

#### QUESTION 7

A third party application has the ability to maintain its own user accounts or it may use single sign-on. To use single sign-on, the application is requesting the following information: OU=Users, DC=Domain, DC=COM. This application is requesting which of the following authentication services?

- A. TACACS+
- B. RADIUS
- C. LDAP
- D. Kerberos

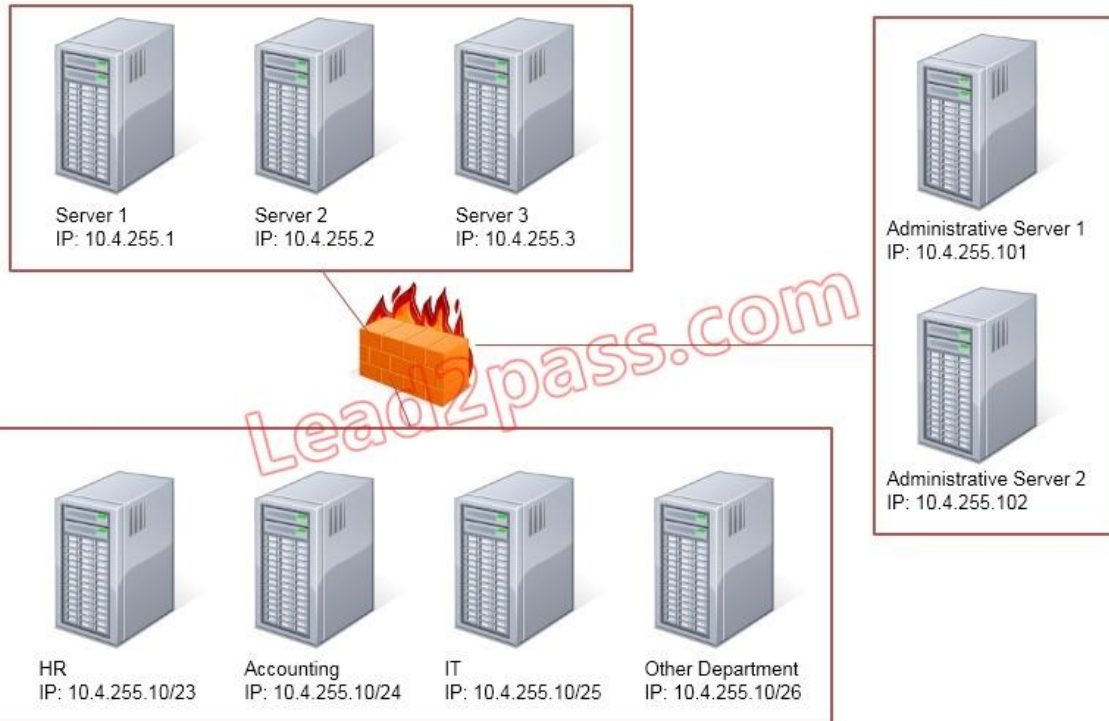
**Answer: C**

#### QUESTION 8

Lab Sim - Configure the Firewall

Task: Configure the firewall (fill out the table) to allow these four rules:

- Only allow the Accounting computer to have HTTPS access to the Administrative server.
- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



| Source IP | Destination IP | Port Number | TCP/UDP | Allow/Deny |
|-----------|----------------|-------------|---------|------------|
|           |                |             |         |            |
|           |                |             |         |            |
|           |                |             |         |            |
|           |                |             |         |            |

**Answer:**

Use the following answer for this simulation task. Below table has all the answers required for this question.

| Source IP   | Destination IP | Port number | TCP/UDP | Allow Deny |
|-------------|----------------|-------------|---------|------------|
| 10.4.255.10 | 10.4.255.101   | 443         | TCP     | Allow      |
| 10.4.255.10 | 10.4.255.2     | 22          | TCP     | Allow      |
| 10.4.255.10 | 10.4.255.101   | Any         | Any     | Allow      |
| 10.4.255.10 | 10.4.255.102   | Any         | Any     | Allow      |

Note: All servers in the bottom have the same IP address, so something is wrong with this question.

**QUESTION 9**



### Drag and Drop Question

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.

**Floor Plan**

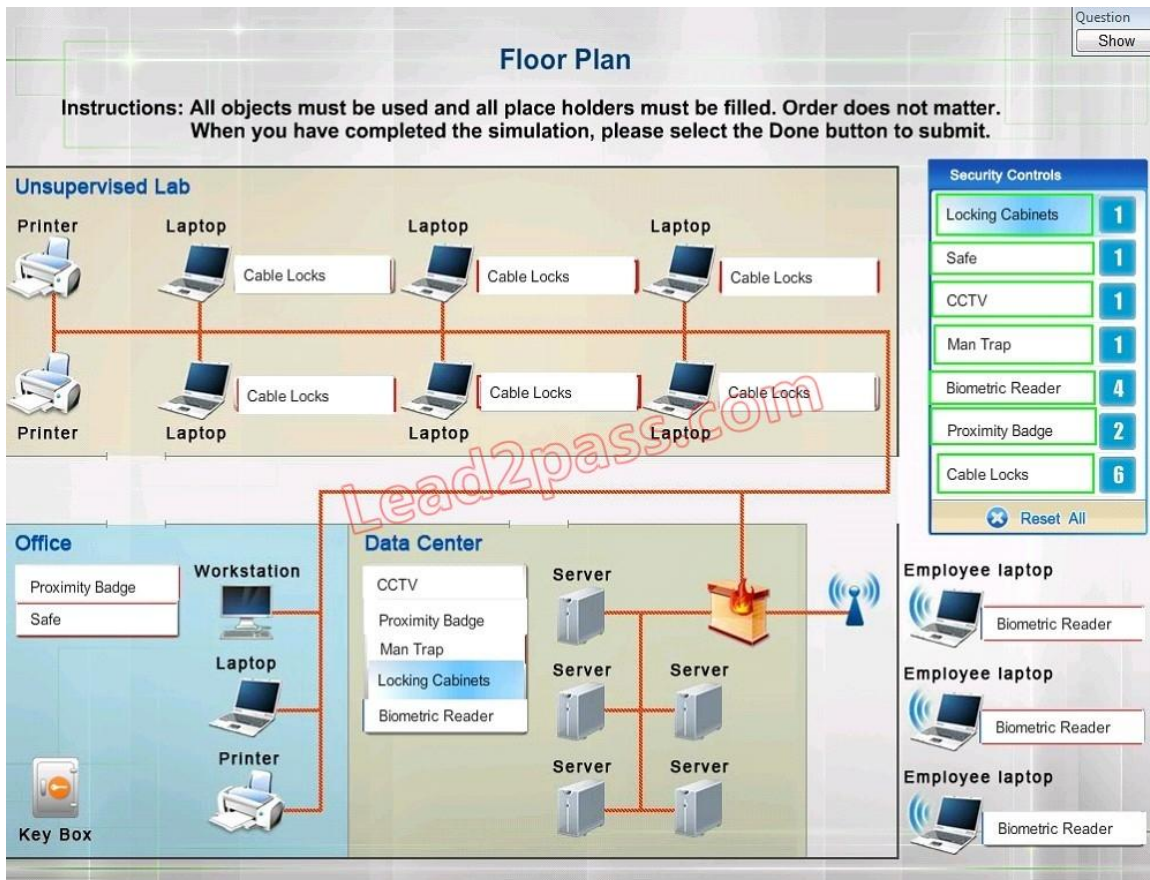
Instructions: All objects must be used and all place holders must be filled. Order does not matter.  
When you have completed the simulation, please select the Done button to submit.

**Security Controls**

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

Reset All

**Answer:**



#### QUESTION 10

Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

- A. Virtual switch
- B. NAT
- C. System partitioning
- D. Access-list
- E. Disable spanning tree
- F. VLAN

**Answer: AF**

#### QUESTION 11

Which of the following should Jane, the security administrator, do FIRST when an employee reports the loss of a corporate mobile device?

- A. Remotely lock the device with a PIN
- B. Enable GPS location and record from the camera
- C. Remotely uninstall all company software
- D. Remotely initiate a device wipe

**Answer: D**

**QUESTION 12**

An application company sent out a software patch for one of their applications on Monday. The company has been receiving reports about intrusion attacks from their customers on Tuesday. Which of the following attacks does this describe?

- A. Zero day
- B. Directory traversal
- C. Logic bomb
- D. Session hijacking

**Answer: A**

**QUESTION 13**

Which of the following is a hardware based encryption device?

- A. EFS
- B. TrueCrypt
- C. TPM
- D. SLE

**Answer: C**

**QUESTION 14**

Which of the following BEST describes a protective countermeasure for SQL injection?

- A. Eliminating cross-site scripting vulnerabilities
- B. Installing an IDS to monitor network traffic
- C. Validating user input in web applications
- D. Placing a firewall between the Internet and database servers

**Answer: C**

**QUESTION 15**

Which of the following MOST interferes with network-based detection techniques?

- A. Mime-encoding
- B. SSL
- C. FTP
- D. Anonymous email accounts

**Answer: B**

**QUESTION 16**

A UNIX administrator would like to use native commands to provide a secure way of connecting to other devices remotely and to securely transfer files. Which of the following protocols could be utilized? (Select TWO).



- A. RDP
- B. SNMP
- C. FTP
- D. SCP
- E. SSH

**Answer:** DE

**QUESTION 17**

Jane, an IT administrator, is implementing security controls on a Microsoft Windows based kiosk used at a bank branch. This kiosk is used by the public for Internet banking. Which of the following controls will BEST protect the kiosk from general public users making system changes?

- A. Group policy implementation
- B. Warning banners
- C. Command shell restrictions
- D. Host based firewall

**Answer:** A

**QUESTION 18**

Sara, the Chief Information Officer (CIO), has tasked the IT department with redesigning the network to rely less on perimeter firewalls, to implement a standard operating environment for client devices, and to disallow personally managed devices on the network. Which of the following is Sara's GREATEST concern?

- A. Malicious internal attacks
- B. Data exfiltration
- C. Audit findings
- D. Incident response

**Answer:** B

**QUESTION 19**

Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

- A. Error and exception handling
- B. Application hardening
- C. Application patch management
- D. Cross-site script prevention

**Answer:** B

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives<sup>®</sup>

**10% Discount Coupon Code: ASTR14**