

**100%** Money Back  
**Guarantee**

**Vendor:**CompTIA

**Exam Code:**JK0-018

**Exam Name:**CompTIA Security+ E2C (2011 Edition)

**Version:**Demo

### QUESTION 1

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:

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

#### 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

Correct Answer:

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

### Office

### Data Center

### Employee laptop

#### Security Controls

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

Reset All

### QUESTION 2

For each of the given items, select the appropriate authentication category from the dropdown choices. Instructions: When you have completed the simulation, please select the Done button to submit.

Hot Area:

## Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

| Item             | Response  |
|------------------|---|
| Retina scan      | <div style="border: 1px solid black; padding: 5px;"><div style="text-align: right; border-bottom: 1px solid black; margin-bottom: 5px;">▼</div><p>Something you have</p><p>Something you know</p><p>Something you are</p><p>All given authentication categories</p></div> |
| Smart card       | <div style="border: 1px solid black; padding: 5px;"><div style="text-align: right; border-bottom: 1px solid black; margin-bottom: 5px;">▼</div><p>Something you have</p><p>Something you know</p><p>Something you are</p><p>All given authentication categories</p></div> |
| Hardware Token   | <div style="border: 1px solid black; padding: 5px;"><div style="text-align: right; border-bottom: 1px solid black; margin-bottom: 5px;">▼</div><p>Something you have</p><p>Something you know</p><p>Something you are</p><p>All given authentication categories</p></div> |
| Password         | <div style="border: 1px solid black; padding: 5px;"><div style="text-align: right; border-bottom: 1px solid black; margin-bottom: 5px;">▼</div><p>Something you have</p><p>Something you know</p><p>Something you are</p><p>All given authentication categories</p></div> |
| PIN number       | <div style="border: 1px solid black; padding: 5px;"><div style="text-align: right; border-bottom: 1px solid black; margin-bottom: 5px;">▼</div><p>Something you have</p><p>Something you know</p><p>Something you are</p><p>All given authentication categories</p></div> |
| Fingerprint scan | <div style="border: 1px solid black; padding: 5px;"><div style="text-align: right; border-bottom: 1px solid black; margin-bottom: 5px;">▼</div><p>Something you have</p><p>Something you know</p><p>Something you are</p><p>All given authentication categories</p></div> |

Correct Answer:



## Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit



Select the appropriate authentication type for the following items:

| Item             | Response   |
|------------------|--|
| Retina scan      | <input type="text"/><br>Something you have<br>Something you know<br>Something you are<br>All given authentication categories |
| Smart card       | <input type="text"/><br>Something you have<br>Something you know<br>Something you are<br>All given authentication categories |
| Hardware Token   | <input type="text"/><br>Something you have<br>Something you know<br>Something you are<br>All given authentication categories |
| Password         | <input type="text"/><br>Something you have<br>Something you know<br>Something you are<br>All given authentication categories |
| PIN number       | <input type="text"/><br>Something you have<br>Something you know<br>Something you are<br>All given authentication categories |
| Fingerprint scan | <input type="text"/><br>Something you have<br>Something you know<br>Something you are<br>All given authentication categories |



**QUESTION 3**

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.

Select and Place:

| Controls            | Company Manager<br>Smart Phone  | Data Center<br>Terminal Server  |
|---------------------|---|---|
| Scerren Locks       |   |   |
| Strong Password     |  |  |
| Device Encryption   |   |   |
| Remote Wipe         |   |   |
| GPS Tracking        |   |   |
| Pop-up Blocker      |   |   |
| Cable Locks         |   |   |
| Antivirus           |   |   |
| Host Based Firewall |   |   |
| Proximity Reader    |   |   |
| Sniffer             |   |   |
| Mantor ap           |   |   |

Correct Answer:

| Controls         | Company Manager<br>Smart Phone  | Data Center<br>Terminal Server  |
|------------------|---|---|
|                  |  |  |
|                  | Screen Locks  | Cable Locks   |
|                  | Strong Password   | Antivirus   |
|                  | Device Encryption   | Host Based Firewall   |
|                  | Remote Wipe   | Sniffer   |
|                  | GPS Tracking  | Mantor ap   |
|                  | Pop-up Blocker  |   |
| Proximity Reader |   |   |
|                  |   |   |
|                  |   |   |

**QUESTION 4**

For each of the given items, select the appropriate authentication category from the drop down choices. Select the appropriate authentication type for the following items:

Hot Area:



| Item             | Response  |
|------------------|---|
| Fingerprint scan | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Hardware token   | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Smart card       | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Password         | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| PIN number       | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Retina Scan      | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |

www.Password.com

Correct Answer:

| Item             | Response  |
|------------------|---|
| Fingerprint scan | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Hardware token   | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Smart card       | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Password         | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| PIN number       | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |
| Retina Scan      | <input type="text"/><br>Biometric authentication<br>One Time Password<br>Multi-factor<br>PAP authentication<br>PAP authentication<br>Biometric authentication |

**QUESTION 5**

You are the security administrator. You need to determine the types of security. Drag the items "Types of Security" to appropriate Security devices.

Select and Place:

**Types of Security**

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

- 1. GPS Tracking
- 2. Mantrap
- 3. Remote wipe
- 4. Strong Passwords
- 5. Cable lock
- 6. Biometrics
- 7. Proximity Badges
- 8. FM-200
- 9. HVAC
- 10. Device Encryption
- 11. Antivirus



| Mobile Device Security | Server in Data Center Security |
|------------------------|--------------------------------|
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |

Correct Answer:

## Types of Security

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.



5. Cable lock

9. HVAC

11. Antivirus

| Mobile Device Security | Server in Data Center Security |
|------------------------|--------------------------------|
| 1. GPS Tracking        | 8. FM-200                      |
| 3. Remote wipe         | 6. Biometrics                  |
| 10. Device Encryption  | 7. Proximity Badges            |
| 4. Strong Passwords    | 2. Mantrap                     |
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |
|                        |                                |

### QUESTION 6

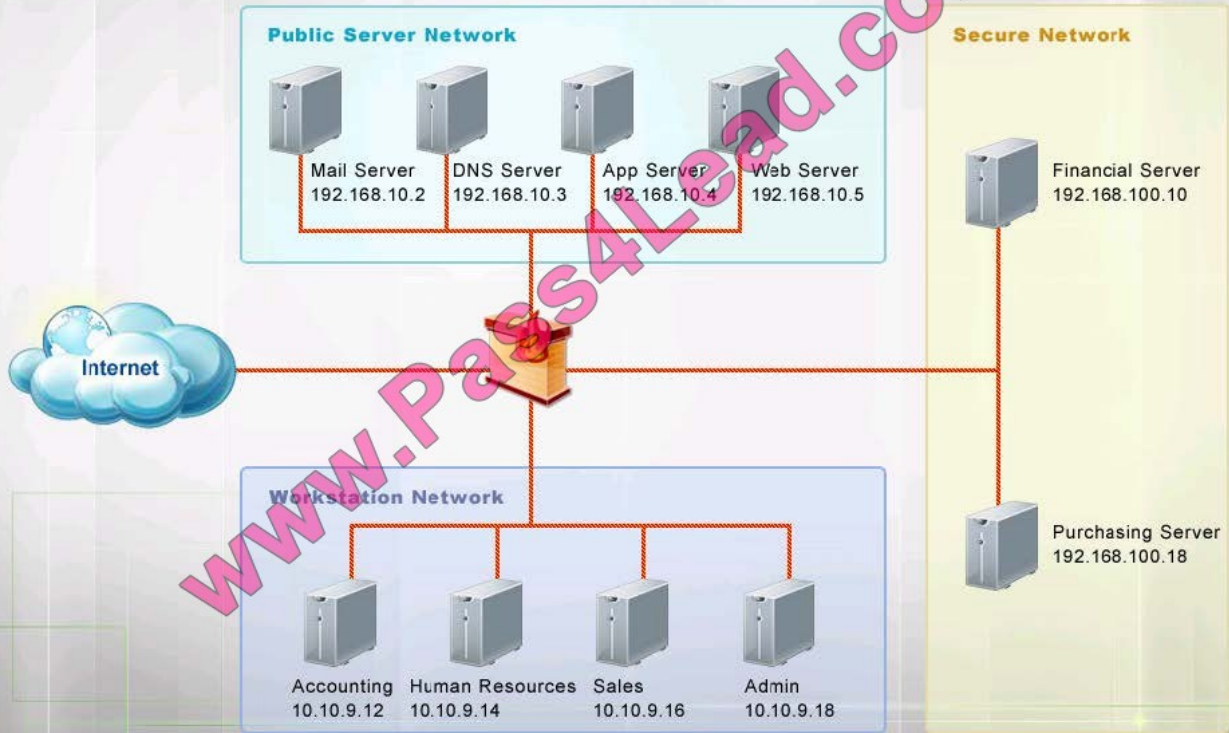
The security administrator has installed a new firewall which implements an implicit DENY policy by default Click on the firewall and configure it to allow ONLY the following communication.

1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port.
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.

## Network Diagram

**Instructions:** The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Hot Area:



## Firewall Rules

| Rule # | Source  | Destination   | Port<br>(Only One Per Rule)             | Protocol                                  | Action                                 |
|--------|---|---|---|---|--|
| 1      | <input type="text"/><br>192.168.10.2/32<br>192.168.10.3/32<br>192.168.10.4/32<br>192.168.10.5/32<br>10.10.9.12/32<br>10.10.9.14/32<br>10.10.9.18/32 | <input type="text"/><br>Any<br>192.168.10.2/32<br>192.168.10.3/32<br>192.168.10.4/32<br>192.168.10.5/32<br>192.168.100.10/32<br>192.168.100.18/32 | <input type="text"/><br>443<br>22<br>69 | <input type="text"/><br>ANY<br>TCP<br>UDP | <input type="text"/><br>Permit<br>Deny |
| 2      | <input type="text"/><br>192.168.10.2/32<br>192.168.10.3/32<br>192.168.10.4/32<br>192.168.10.5/32<br>10.10.9.12/32<br>10.10.9.14/32<br>10.10.9.18/32 | <input type="text"/><br>Any<br>192.168.10.2/32<br>192.168.10.3/32<br>192.168.10.4/32<br>192.168.10.5/32<br>192.168.100.10/32<br>192.168.100.18/32 | <input type="text"/><br>443<br>22<br>69 | <input type="text"/><br>ANY<br>TCP<br>UDP | <input type="text"/><br>Permit<br>Deny |
| 3      | <input type="text"/><br>192.168.10.2/32<br>192.168.10.3/32<br>192.168.10.4/32<br>192.168.10.5/32<br>10.10.9.12/32<br>10.10.9.14/32<br>10.10.9.18/32 | <input type="text"/><br>Any<br>192.168.10.2/32<br>192.168.10.3/32<br>192.168.10.4/32<br>192.168.10.5/32<br>192.168.100.10/32<br>192.168.100.18/32 | <input type="text"/><br>443<br>22<br>69 | <input type="text"/><br>ANY<br>TCP<br>UDP | <input type="text"/><br>Permit<br>Deny |
| 4      | <input type="text"/><br>192.168.10.2/32<br>192.168.10.3/32<br>192.168.10.4/32<br>192.168.10.5/32<br>10.10.9.12/32<br>10.10.9.14/32<br>10.10.9.18/32 | <input type="text"/><br>Any<br>192.168.10.2/32<br>192.168.10.3/32<br>192.168.10.4/32<br>192.168.10.5/32<br>192.168.100.10/32<br>192.168.100.18/32 | <input type="text"/><br>443<br>22<br>69 | <input type="text"/><br>ANY<br>TCP<br>UDP | <input type="text"/><br>Permit<br>Deny |

Correct Answer:

## Firewall Rules

| Rule # | Source  | Destination   | Port<br>(Only One Per Rule)   | Protocol  | Action   |
|--------|---|---|---|---|--|
| 1      | <ul style="list-style-type: none"> <li>192.168.10.2/32</li> <li>192.168.10.3/32</li> <li>192.168.10.4/32</li> <li>192.168.10.5/32</li> <li>10.10.9.12/32</li> <li>10.10.9.14/32</li> <li>10.10.9.18/32</li> </ul> | <ul style="list-style-type: none"> <li>Any</li> <li>192.168.10.2/32</li> <li>192.168.10.3/32</li> <li>192.168.10.4/32</li> <li>192.168.10.5/32</li> <li>192.168.100.10/32</li> <li>192.168.100.18/32</li> </ul> | <ul style="list-style-type: none"> <li>443</li> <li>22</li> <li>69</li> </ul> | <ul style="list-style-type: none"> <li>ANY</li> <li>TCP</li> <li>UDP</li> </ul> | <ul style="list-style-type: none"> <li>Permit</li> <li>Deny</li> </ul> |
| 2      | <ul style="list-style-type: none"> <li>192.168.10.2/32</li> <li>192.168.10.3/32</li> <li>192.168.10.4/32</li> <li>192.168.10.5/32</li> <li>10.10.9.12/32</li> <li>10.10.9.14/32</li> <li>10.10.9.18/32</li> </ul> | <ul style="list-style-type: none"> <li>Any</li> <li>192.168.10.2/32</li> <li>192.168.10.3/32</li> <li>192.168.10.4/32</li> <li>192.168.10.5/32</li> <li>192.168.100.10/32</li> <li>192.168.100.18/32</li> </ul> | <ul style="list-style-type: none"> <li>443</li> <li>22</li> <li>69</li> </ul> | <ul style="list-style-type: none"> <li>ANY</li> <li>TCP</li> <li>UDP</li> </ul> | <ul style="list-style-type: none"> <li>Permit</li> <li>Deny</li> </ul> |
| 3      | <ul style="list-style-type: none"> <li>192.168.10.2/32</li> <li>192.168.10.3/32</li> <li>192.168.10.4/32</li> <li>192.168.10.5/32</li> <li>10.10.9.12/32</li> <li>10.10.9.14/32</li> <li>10.10.9.18/32</li> </ul> | <ul style="list-style-type: none"> <li>Any</li> <li>192.168.10.2/32</li> <li>192.168.10.3/32</li> <li>192.168.10.4/32</li> <li>192.168.10.5/32</li> <li>192.168.100.10/32</li> <li>192.168.100.18/32</li> </ul> | <ul style="list-style-type: none"> <li>443</li> <li>22</li> <li>69</li> </ul> | <ul style="list-style-type: none"> <li>ANY</li> <li>TCP</li> <li>UDP</li> </ul> | <ul style="list-style-type: none"> <li>Permit</li> <li>Deny</li> </ul> |
| 4      | <ul style="list-style-type: none"> <li>192.168.10.2/32</li> <li>192.168.10.3/32</li> <li>192.168.10.4/32</li> <li>192.168.10.5/32</li> <li>10.10.9.12/32</li> <li>10.10.9.14/32</li> <li>10.10.9.18/32</li> </ul> | <ul style="list-style-type: none"> <li>Any</li> <li>192.168.10.2/32</li> <li>192.168.10.3/32</li> <li>192.168.10.4/32</li> <li>192.168.10.5/32</li> <li>192.168.100.10/32</li> <li>192.168.100.18/32</li> </ul> | <ul style="list-style-type: none"> <li>443</li> <li>22</li> <li>69</li> </ul> | <ul style="list-style-type: none"> <li>ANY</li> <li>TCP</li> <li>UDP</li> </ul> | <ul style="list-style-type: none"> <li>Permit</li> <li>Deny</li> </ul> |

**QUESTION 7**

Drag and drop the correct protocol to its default port.

Select and Place:

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

Correct Answer:

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

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |

www.Pass4Lead.com

**QUESTION 8**

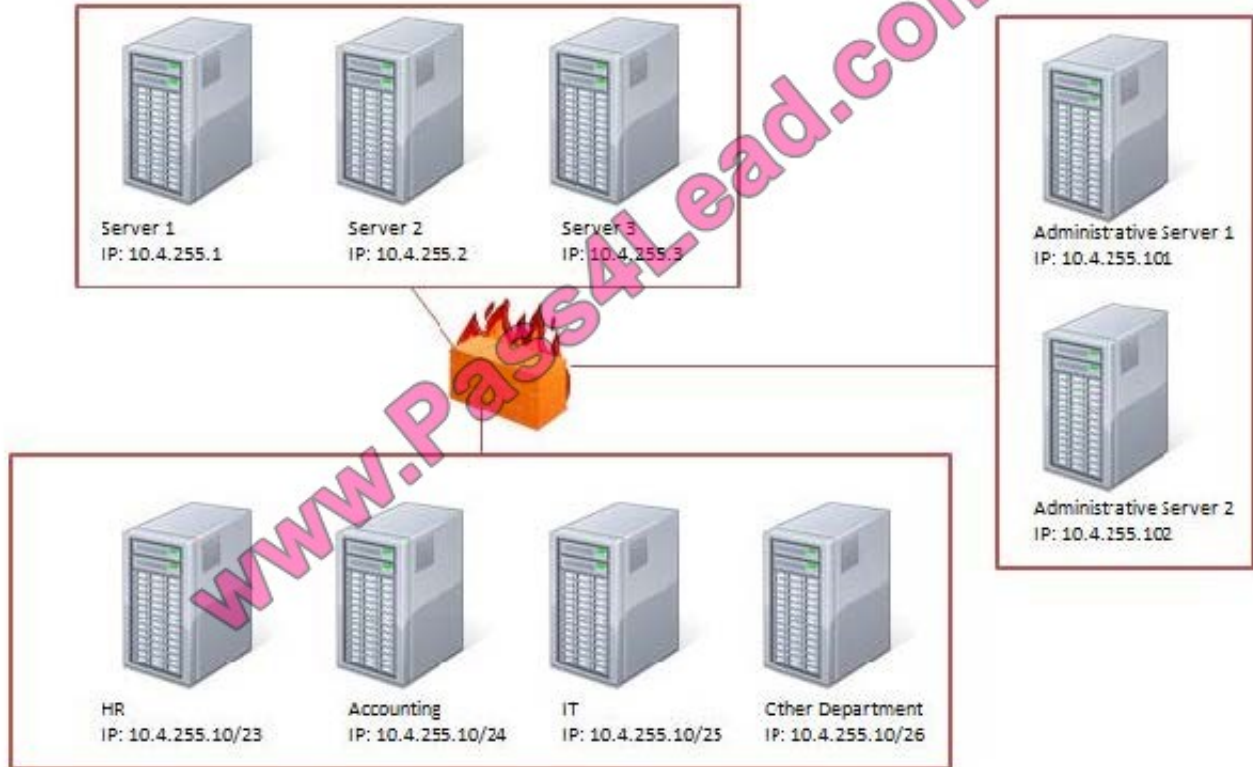
You are the security administrator. You need to determine the types of security. Drag the items "Types of Security" to appropriate Security devices.



## Configure the Firewall

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

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



Correct Answer: Use the following answer for this simulation task.

Explanation/Reference:

| 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

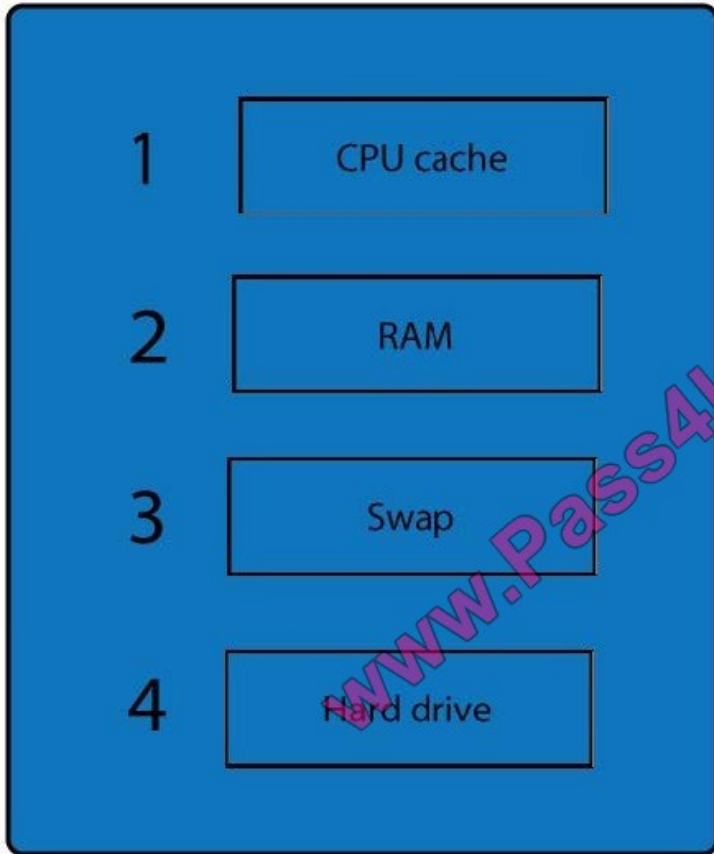
A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:

The image shows a drag-and-drop puzzle interface. On the left, there is a large blue rectangular area containing four white rectangular slots, numbered 1, 2, 3, and 4 from top to bottom. On the right, there are four blue rectangular boxes, each containing a text label: 'RAM', 'CPU cache', 'Swap', and 'Hard drive'. A diagonal watermark 'www.Pass4Lead.com' is overlaid across the center of the image.

Correct Answer:





|  |
|--|
|  |
|  |
|  |
|  |

---

**QUESTION 10**

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

Question  
Show

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"/><br><input type="text" value="HOAX"/><br><input type="text" value="VISHING"/><br><input type="text" value="PHISHING"/><br><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"/><br><input type="text" value="HOAX"/><br><input type="text" value="VISHING"/><br><input type="text" value="PHISHING"/><br><input type="text" value="PHARMING"/> |
|  <p>Attacker collecting credit card details</p>   |  <p>Phone-based victim</p>   | <input type="text" value="SPEAR PUSHING"/><br><input type="text" value="HOAX"/><br><input type="text" value="VISHING"/><br><input type="text" value="PHISHING"/><br><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"/><br><input type="text" value="HOAX"/><br><input type="text" value="VISHING"/><br><input type="text" value="PHISHING"/><br><input type="text" value="PHARMING"/> |
|  <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>                        |  <p>Victims</p> <p> <input type="text" value="Fraudulent site"/><br/> <input type="text" value="Legitimate site"/> </p>                      | <input type="text" value="SPEAR PUSHING"/><br><input type="text" value="HOAX"/><br><input type="text" value="VISHING"/><br><input type="text" value="PHISHING"/><br><input type="text" value="PHARMING"/> |

Correct 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>  | <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> SPEAR PUSHING</li> <li><input type="checkbox"/> HOAX</li> <li><input type="checkbox"/> VISHING</li> <li><input type="checkbox"/> PHISHING</li> <li><input type="checkbox"/> PHARMING</li> </ul>            |
|  <p>Attacker posts link to fake AV software</p>  |  <p>Multiple social networks</p>  <p>Broad set of victims</p>  | <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> SPEAR PUSHING</li> <li><input checked="" type="checkbox"/> HOAX</li> <li><input type="checkbox"/> VISHING</li> <li><input type="checkbox"/> PHISHING</li> <li><input type="checkbox"/> PHARMING</li> </ul> |
|  <p>Attacker collecting credit card details</p>  |  <p>Phone-based victim</p>  | <ul style="list-style-type: none"> <li><input type="checkbox"/> SPEAR PUSHING</li> <li><input type="checkbox"/> HOAX</li> <li><input checked="" type="checkbox"/> VISHING</li> <li><input type="checkbox"/> PHISHING</li> <li><input type="checkbox"/> PHARMING</li> </ul>            |
|  <p>Attacker mass-mails product information to parties that have already opted out of receiving advertisements</p> |  <p>Broad set of recipients</p>  | <ul style="list-style-type: none"> <li><input type="checkbox"/> SPEAR PUSHING</li> <li><input type="checkbox"/> HOAX</li> <li><input type="checkbox"/> VISHING</li> <li><input checked="" type="checkbox"/> PHISHING</li> <li><input type="checkbox"/> PHARMING</li> </ul>            |
|  <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>                       |  <p>Victims</p> <p> <input checked="" type="checkbox"/> Fraudulent site<br/> <input checked="" type="checkbox"/> Legitimate site         </p> | <ul style="list-style-type: none"> <li><input type="checkbox"/> SPEAR PUSHING</li> <li><input type="checkbox"/> HOAX</li> <li><input type="checkbox"/> VISHING</li> <li><input type="checkbox"/> PHISHING</li> <li><input checked="" type="checkbox"/> PHARMING</li> </ul>            |

Reset All

**QUESTION 11**

Determine the types of Attacks from right to specific action.

Select and Place:

## Types of attacks

Task: Determine the types of attacks below by selecting an option from the dropdown list.

|  |   |  |                    |
|--|---|--|--------------------|
|   | Email sent to multiple users to a link to verify username/password on external site                                     |   | Choose Attack Type |
|   | Phone calls made to CEO of organization asking for various financial data   |   | Choose Attack Type |
|   | Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone        |   | Choose Attack Type |
|   | You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet       |   | Choose Attack Type |
|  | A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions. |  | Choose Attack Type |

1. Phishing
2. Pharming
3. Vishing
4. Whaling
5. X-Mas
6. Spoofing
7. Hoax
8. Spam
9. Spim
10. Social Engineering

Correct Answer:

## Types of attacks

Task: Determine the types of attacks below by selecting an option from the dropdown list.

|  |   |  |                        |             |
|--|---|--|------------------------|-------------|
|   | Email sent to multiple users to a link to verify username/password on external site                                     |   | 1. Phishing            | 2. Pharming |
|   | Phone calls made to CEO of organization asking for various financial data   |   | 4. Whaling             | 5. X-Mas    |
|   | Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone        |   | 3. Vishing             | 6. Spoofing |
|   | You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet       |   | 9. Spim                | 7. Hoax     |
|  | A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions. |  | 10. Social Engineering | 8. Spam     |



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

## Try our product !

**100%** Guaranteed Success

**100%** Money Back Guarantee

**365** Days Free Update

**Instant Download** After Purchase

**24x7** Customer Support

Average **99.9%** Success Rate

More than **800,000** Satisfied Customers Worldwide

Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

## Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



|   |   |  |
|---|---|--|
|  <p><b>One Year Free Update</b><br/>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p> |  <p><b>Money Back Guarantee</b><br/>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p> |  <p><b>Security &amp; Privacy</b><br/>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p> |
|---|---|--|

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.