



# JK0-018<sup>Q&As</sup>

CompTIA Security+ E2C (2011 Edition)

## Pass CompTIA JK0-018 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.lead4pass.com/JK0-018.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers







**QUESTION 1**



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

**QUESTION 2**

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:



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
Attacker gains confidential company information	Targeted CEO and board members	<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"/>
Attacker posts link to fake AV software	Multiple social networks Broad set of victims	<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"/>
Attacker collecting credit card details	Phone-based victim	<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"/>
Attacker mass-mails product information to parties that have already opted out of receiving advertisements	Broad set of recipients	<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"/>
Attacker redirects name resolution entries from legitimate site to fraudulent site	Victims <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid red; padding: 2px; color: red;">Fraudulent site</div> <div style="border: 1px solid green; padding: 2px; color: green;">Legitimate site</div> </div>	<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"/>











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>	<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>	<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>

### QUESTION 3

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:



1

2

3

4

RAM

CPU cache

Swap

Hard drive

Correct Answer:

1 CPU cache

2 RAM

3 Swap

4 Hard drive



#### QUESTION 4

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.

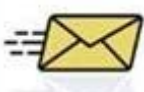









### QUESTION 5

Determine the types of Attacks from right to specific action.

Select and Place:

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

#### Types of attacks

	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.

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

2. Pharming

5. X-Mas

6. Spoofing

7. Hoax

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](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

## 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> 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> 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> 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.  
Copyright © lead4pass, All Rights Reserved.