



# 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.passapply.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

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"/> SPEAR PUSHING HOAX VISHING PHISHING PHARMING
 Attacker posts link to fake AV software	 Multiple social networks  Broad set of victims	<input type="text"/> SPEAR PUSHING HOAX VISHING PHISHING PHARMING
 Attacker collecting credit card details	 Phone-based victim	<input type="text"/> SPEAR PUSHING HOAX VISHING PHISHING PHARMING
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	<input type="text"/> SPEAR PUSHING HOAX VISHING PHISHING 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"/> SPEAR PUSHING HOAX VISHING PHISHING PHARMING











Correct Answer:



Question  
Show

### Attacks

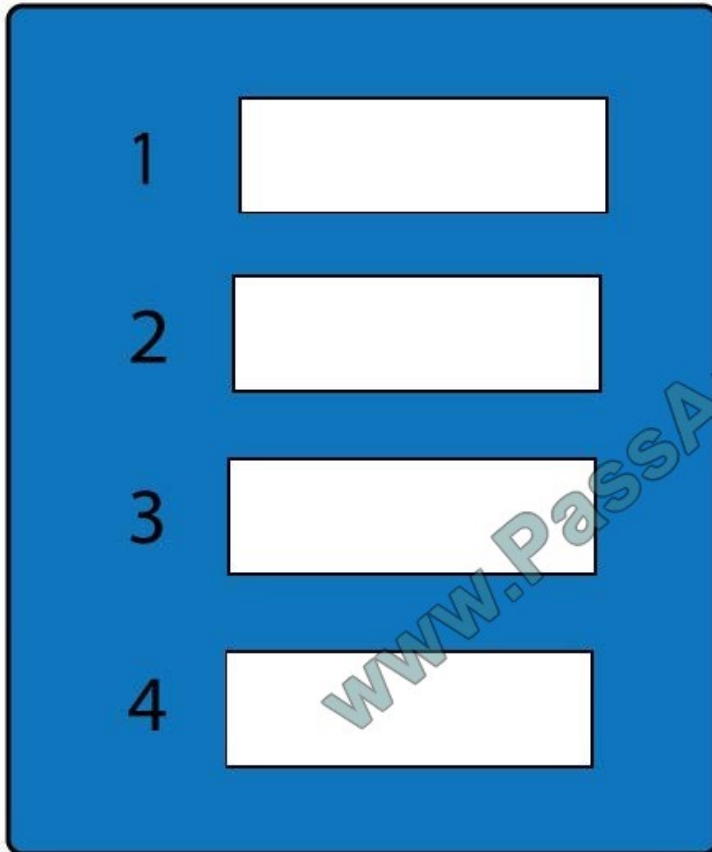
**Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.**

Attack Vector	Target	Identified Attack
 <p>Attacker gains confidential company information</p>	 <p>Targeted CEO and board members</p>	<div style="border: 1px solid gray; padding: 5px;"> <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"/> </div>
 <p>Attacker posts link to fake AV software</p>	 <p>Multiple social networks</p>	<div style="border: 1px solid gray; padding: 5px;"> <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"/> </div>
 <p>Attacker collecting credit card details</p>	 <p>Phone-based victim</p>	<div style="border: 1px solid gray; padding: 5px;"> <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"/> </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 gray; padding: 5px;"> <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"/> </div>
 <p>Attacker redirects name resolution entries from legitimate site to fraudulent site</p>	 <p>Victims</p>	<div style="border: 1px solid gray; padding: 5px;"> <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"/> </div>

### QUESTION 2

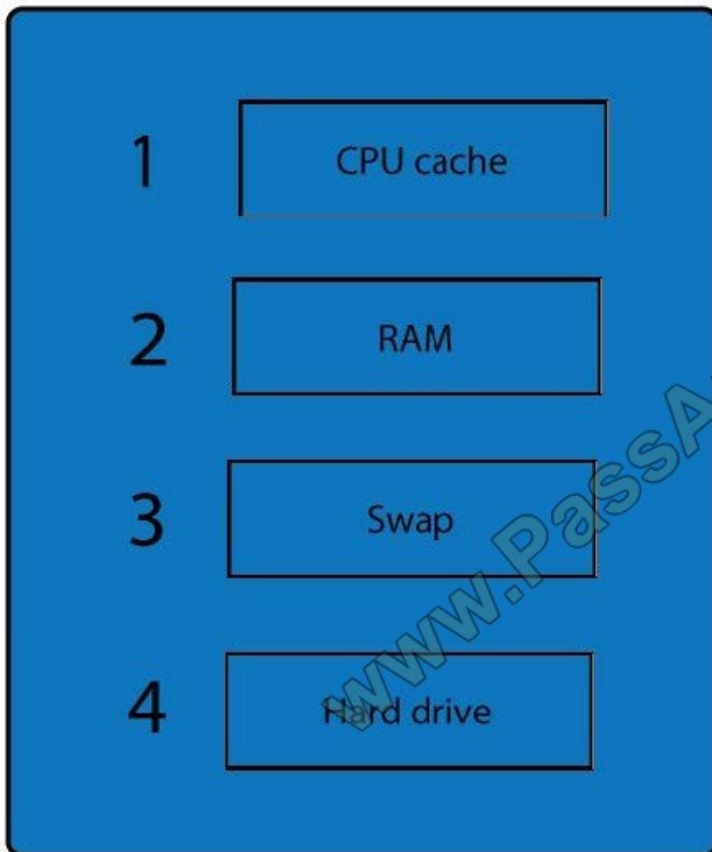
A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:



- RAM
- CPU cache
- Swap
- Hard drive

Correct Answer:



- [ ]
- [ ]
- [ ]
- [ ]



**QUESTION 3**

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

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



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.

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 4

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

### 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.





### 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 6





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 7**

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:



### 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](#)

Correct Answer:



### 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 8

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



Correct Answer:



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





### QUESTION 9

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



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

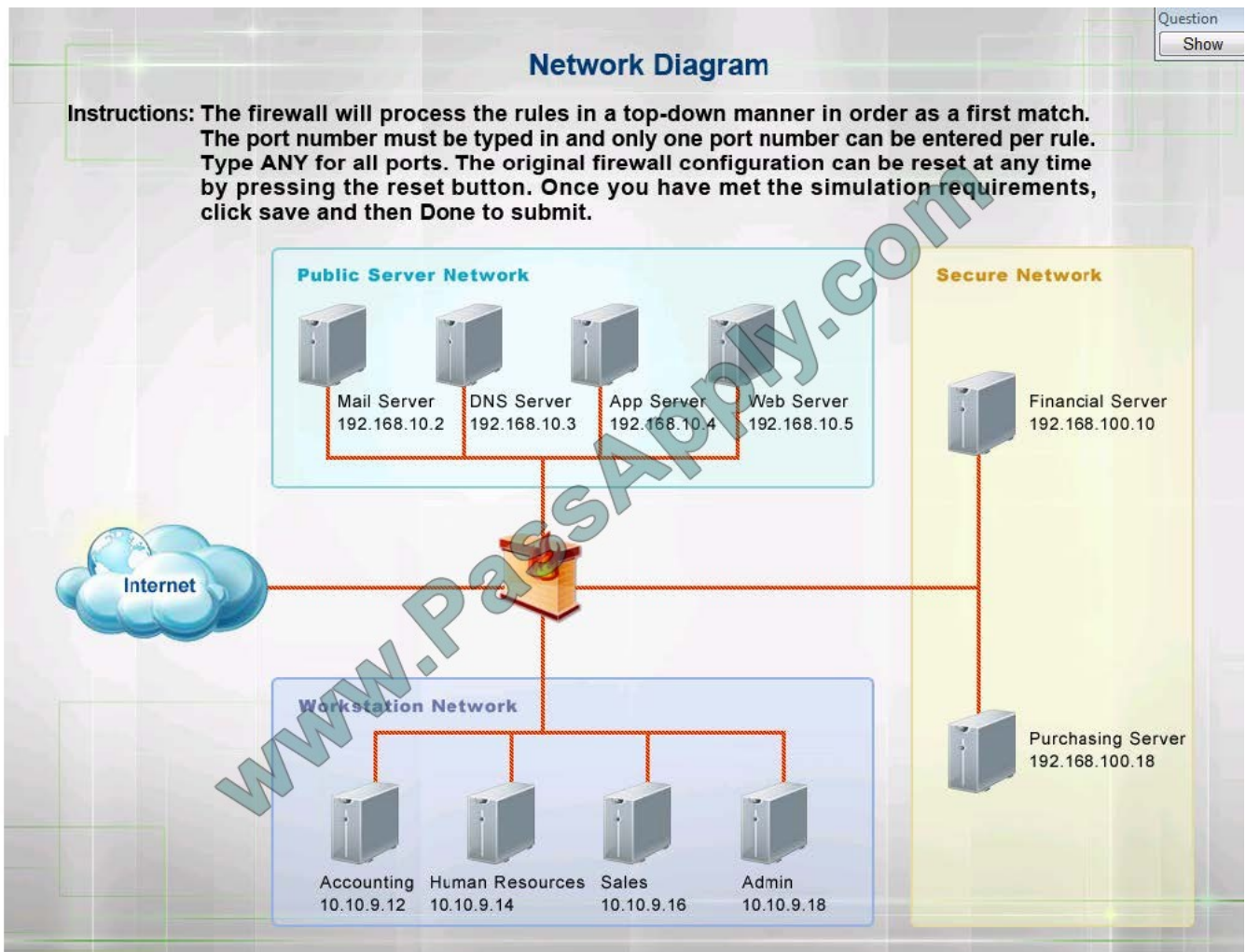


### QUESTION 10

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.



Hot Area:



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

Correct Answer:



Firewall Rules					
Rule #	Source	Destination	Port (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 11**

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



[Latest JK0-018 Dumps](#)

[JK0-018 PDF Dumps](#)

[JK0-018 Practice Test](#)



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.passapply.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 © passapply, All Rights Reserved.