DUMPSARENA

GIAC Systems and Network Auditor

GIAC GSNA

Version Demo

Total Demo Questions: 20

Total Premium Questions: 413

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	101
Topic 2, Volume B	99
Topic 3, Volume C	100
Topic 4, Volume D	113
Total	413

QUESTION NO: 1

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site.

Which of the following techniques is he using to accomplish his task?

A. Eavesdropping

B. Fingerprinting

C. Web ripping

D. TCP FTP proxy scanning

ANSWER: C

Explanation:

Web ripping is a technique in which the attacker copies the whole structure of a Web site to the local disk and obtains all files of the Web site. Web ripping helps an attacker to trace the loopholes of the Web site.

- Active fingerprinting
- 2.Passive fingerprinting

In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system.

QUESTION NO: 2

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities.

Which of the following vulnerabilities can be fixed using Nessus?

A. Vulnerabilities that allow a remote cracker to control sensitive data on a system

B. Misconfiguration (e.g. open mail relay, missing patches, etc.)

C. Vulnerabilities that allow a remote cracker to access sensitive data on a system

D. Vulnerabilities that help in Code injection attacks

ANSWER: A B C

Explanation:

Nessus is a proprietary comprehensive vulnerability scanning program. It is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on the tested systems.

For example: Vulnerabilities that allow a remote cracker to control or access sensitive data on a system. Misconfiguration (e.g. open mail relay, missing patches, etc). Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack. Denials of service against the TCP/IP stack by using mangled packets. On UNIX (including Mac OS X), it consists of nessusd, the Nessus daemon, which does the scanning, and nessus, the client, which controls scans and presents the vulnerability results to the user. For Windows, Nessus 3 installs as an executable and has a self-contained scanning, reporting, and management system.

Operations: In typical operation, Nessus begins by doing a port scan with one of its four internal portscanners (or it can optionally use Amap or Nmap) to determine which ports are open on the target and then tries various exploits on the open ports. The vulnerability tests, available as subscriptions, are written in NASL (Nessus Attack Scripting Language), a scripting language optimized for custom network interaction. Tenable Network Security produces several dozen new vulnerability checks (called plugins) each week, usually on a daily basis. These checks are available for free to the general public; commercial customers are not allowed to use this Home Feed any more. The Professional Feed (which is not free) also gives access to support and additional scripts (audit and compliance tests). Optionally, the results of the scan can be reported in various formats, such as plain text, XML, HTML, and LaTeX. The results can also be saved in a knowledge base for debugging. On UNIX, scanning can be automated through the use of a command-line client. There exist many different commercial, free and open source tools for both UNIX and Windows to manage individual or distributed Nessus scanners. If the user chooses to do so (by disabling the option' safe checks'), some of Nessus's vulnerability tests may try to cause vulnerable services or operating systems to crash. This lets a user test the resistance of a device before putting it in production. Nessus provides additional functionality beyond testing for known network vulnerabilities. For instance, it can use Windows credentials to examine patch levels on computers running the Windows operating system, and can perform password auditing using dictionary and brute force methods. Nessus 3 and later can also audit systems to make sure they have been configured per a specific policy, such as the NSA's guide for hardening Windows servers.

QUESTION NO: 3 - (DRAG DROP)

DRAG DROP

You work as a Security Administrator in Tech Perfect Inc. The company has a TCP/IP based network. Three Cisco IOS routers- router1, router2, and router3 are currently working in the network. You want to accomplish the following tasks:

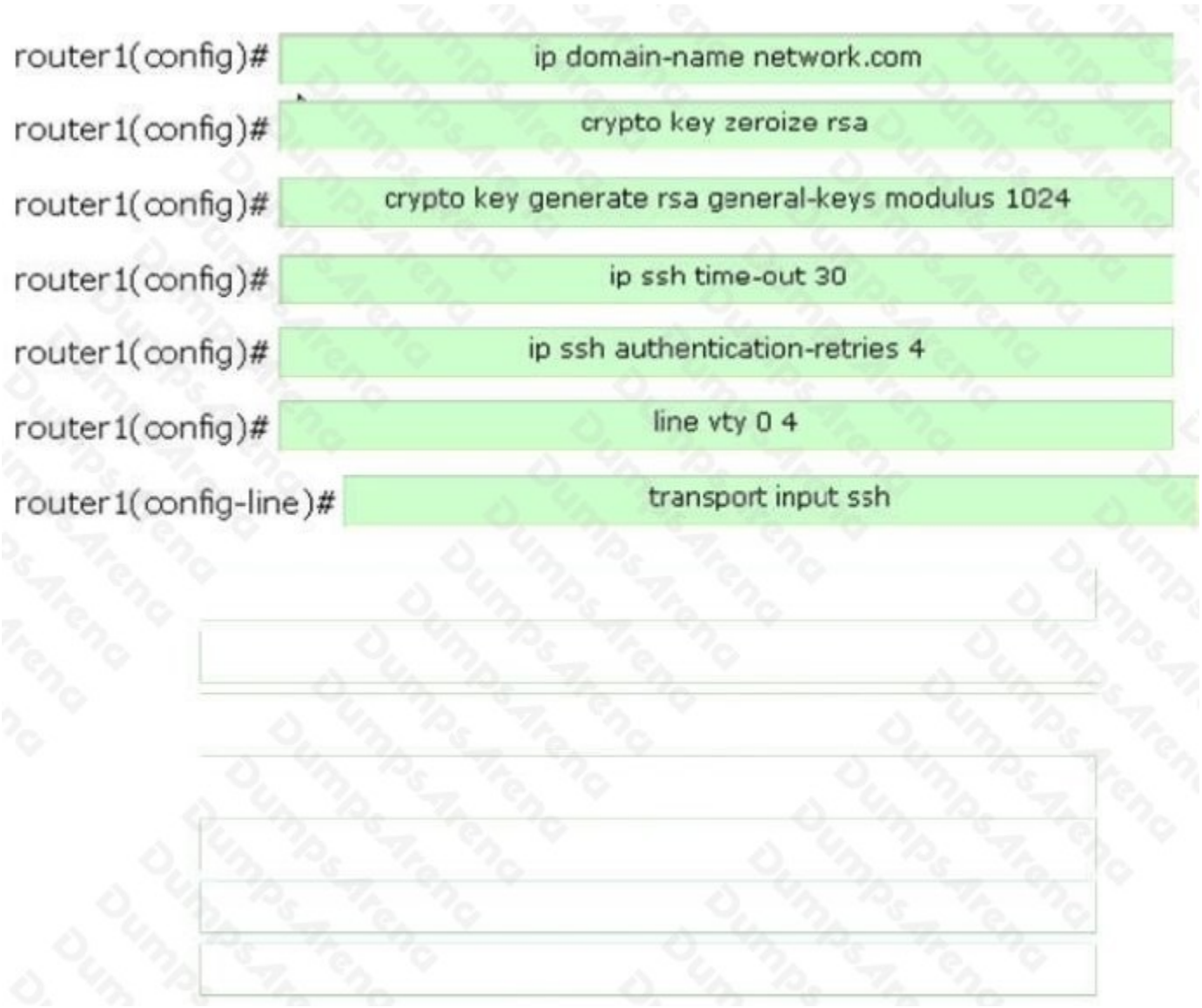
- Configure router1 to act as an SSH server.
- Configure domain name 'network.com'.
- Generate a general-purpose RSA key pair and specify the IP key size of 1024.
- Configure SSH time-out of 30 seconds and SSH authentication retries value 4.

Drag and drop the appropriate commands beside their respective command prompts in order to accomplish the tasks.

Select and Place:


router1(config)# Drop Here
router1(config)# Drop Here
router1(config)# Drop Here
router1(config)# Drop Here
router1(config)# Drop Here
router1(config)# Drop Here
router1(config-line)# Drop Here
ip domain-name network.com
crypto key zeroize rsa
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 30
ip ssh authentication-retries 4
line vty 0 4
transport input ssh

ANSWER:



Explanation:

In order to accomplish the given tasks, you will have to use the following commands: router1(config)#ip domain-name network.com router1(config)#crypto key zeroize rsa

router1(config)#crypto key generate rsa general-keys modulus 1024 router1(config)#ip ssh time-out 30 router1(config)#ip ssh authentication-retries 4 router1(config)#line vty 0 4 router1(config-line)#transport input ssh

QUESTION NO: 4

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows: It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc. It is commonly used for the following purposes:

a.War driving

b.Detecting unauthorized access points

c. Detecting causes of interference on a WLAN d.WEP ICV error tracking

e. Making Graphs and Alarms on 802.11 Data, including Signal Strength This tool is known as _____.

A. THC-Scan

B. NetStumbler

C. Absinthe

D. Kismet

ANSWER: B

Explanation:

NetStumbler is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of NetStumbler are as follows: It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc. It is commonly used for the following purposes: a.War driving

b.Detecting unauthorized access points

c.Detecting causes of interference on a WLAN

d.WEP ICV error tracking e.Making Graphs and Alarms on 802.11 Data, including Signal Strength Answer D is incorrect. Kismet is an IEEE 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.

QUESTION NO: 5

In an IT organization, some specific tasks require additional detailed controls to ensure that the workers perform their job correctly.

What do these detailed controls specify? (Choose three)

A. How the department handles acquisitions, security, delivery, implementation, and support of IS services

B. How to lock a user account after unsuccessful logon attempts

C. How output data is verified before being accepted into an application

D. The way system security parameters are set

ANSWER: A B D

Explanation:

Some of the specific tasks require additional detailed controls to ensure that the workers perform their job correctly. These controls refer to some specific tasks or steps to be performed such as:

- The way system security parameters are set.

- How input data is verified before being accepted into an application.
- How to lock a user account after unsuccessful logon attempts.
- How the department handles acquisitions, security, delivery, implementation, and support of IS services.

QUESTION NO: 6

You work as a Software Developer for UcTech Inc. You want to create a new session.

Which of the following methods can you use to accomplish the task?

A. getNewSession(true)

B. getSession(false)

C. getSession()

D. getSession(true)

E. getNewSession()

ANSWER: C D

Explanation:

The getSession() method of the HttpServletRequest interface returns the current session associated with the request, or creates a new session if no session exists. The method has two syntaxes as follows:

- public HttpSession getSession(): This method creates a new session if it does not exist.
- public HttpSession getSession(boolean create): This method becomes similar to the above method if create is true, and returns the current session if create is false. It returns null if no session exists.

QUESTION NO: 7

On which of the following does a CGI program execute?

A. Router

B. Web server

C. Client

D. Client and Web server

ANSWER: B

Explanation:

The Common Gateway Interface (CGI) specification is used for creating executable programs that run on a Web server. CGI defines the communication link between a Web server and Web applications. It gives a network or Internet resource access

to specific programs. For example, when users submit an HTML form on a Web site, CGI is used to pass this information to a remote application for processing, and retrieve the results from the application. It then returns these results to the user by means of an HTML page.

QUESTION NO: 8

You work as a Software Developer for Cinera Softwares Inc. You create a DHTML page that contains ten TextBox controls to get information from the users who use your application. You want all the components placed on the DHTML page to be repositioned dynamically, when a user resizes the browser window.

Which of the following will you use for this?

A. Use the position attribute of the Cascading Style Sheet.

B. Use the OnResize event for the DHTML page object.

C. Use the Resize event of the Document object.

D. Use the OnResize event of the Cascading Style Sheet.

ANSWER: A

Explanation:

position attribute of the Cascading Style Sheet. The DHTML page object modal gives access to styles and style sheets. Therefore, you can easily set and change the position of an element.

Reference: MSDN, Index "Dynamic HTML(DHTML), in DHTML Applications", "Elements Positioning in DHTML Application", Search "Positioning", "Dynamic HTML"

QUESTION NO: 9 - (HOTSPOT)

HOTSPOT

You work as a Network Administrator for McRobert Inc. The company has a Windows Active Directory-based single domain single forest network. The network includes fifty client computers running different Windows client operating systems.

A member server named MRIFS is configured as a file server on the network. You are required to implement the following:

The data communication must be encrypted whenever possible.

Each client computer must be able to access the server.

Configure the required options in the dialog box given below in order to accomplish the task.

Hot Area:


Permit Properties
Security Methods
General
Permit
Block
Negotiate security:
Security method preference order:
Type
AH Integrity
ESP Confidential...
ES
Encrypti...
<None>
3DES
SH
Integrity...
<None>
<None>
SH
Custom
MD5
3DES
SH
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPSec
Allow unsecured communication with non-IPSec-aware computers
Use session key perfect forward secrecy (PFS)
OK
Cancel
Apply

ANSWER:

Explanation:

In order to accomplish the task, you will have to select the Allow unsecured communication with non-IPSec -aware computers check box.

By enabling this option, IPSec will allow unsecured communication, if necessary. Disabling the option blocks communication with computers that cannot initiate IPSec, such as legacy systems.

This option should be disabled to secure computers connected to the Internet.

QUESTION NO: 10

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests.

Which of the following tools can an attacker use to perform a DNS zone transfer?

A. DSniff

B. Dig

C. Host

D. NSLookup

ANSWER: B C D

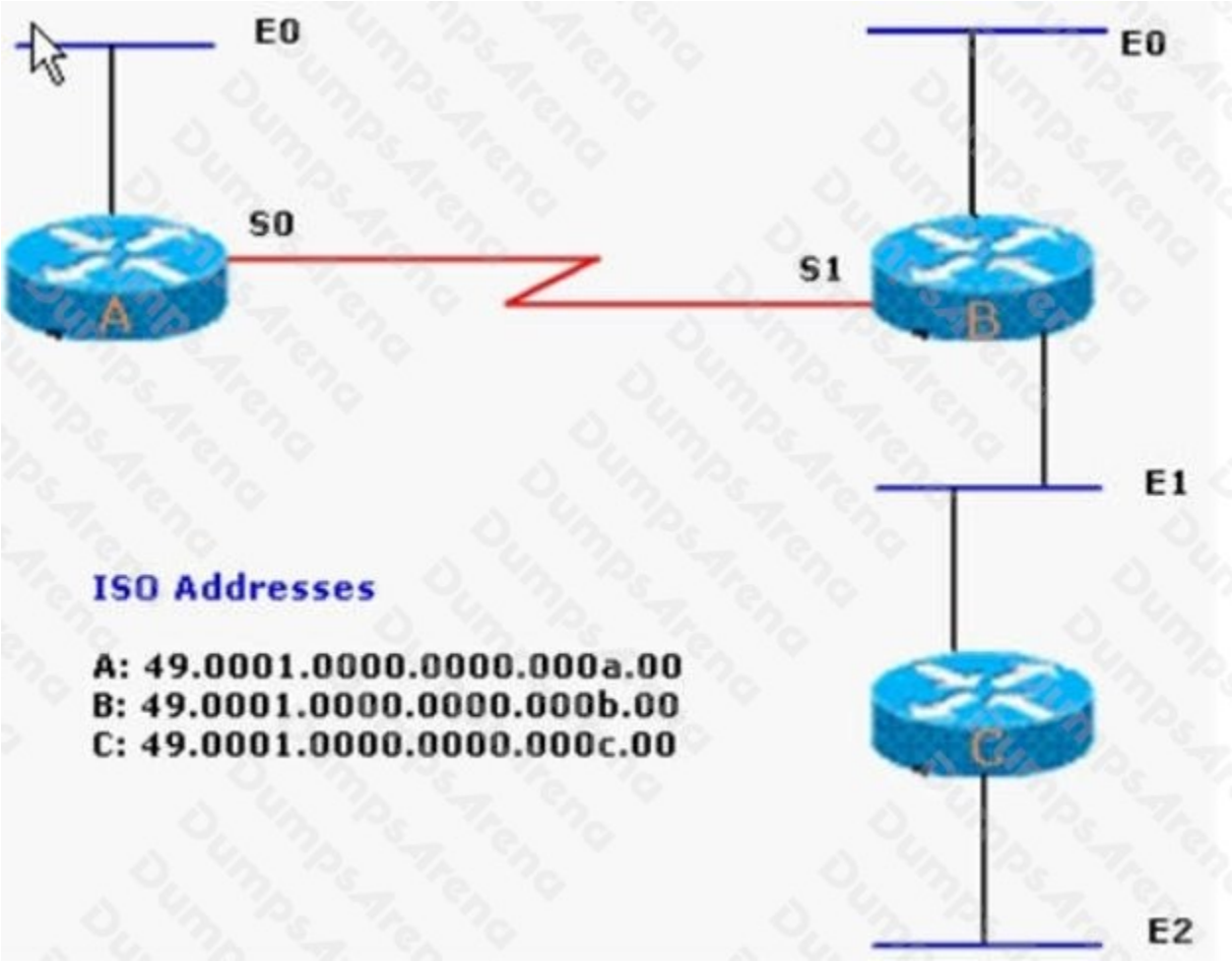
Explanation:

An attacker can use Host, Dig, and NSLookup to perform a DNS zone transfer.

QUESTION NO: 11 - (DRAG DROP)

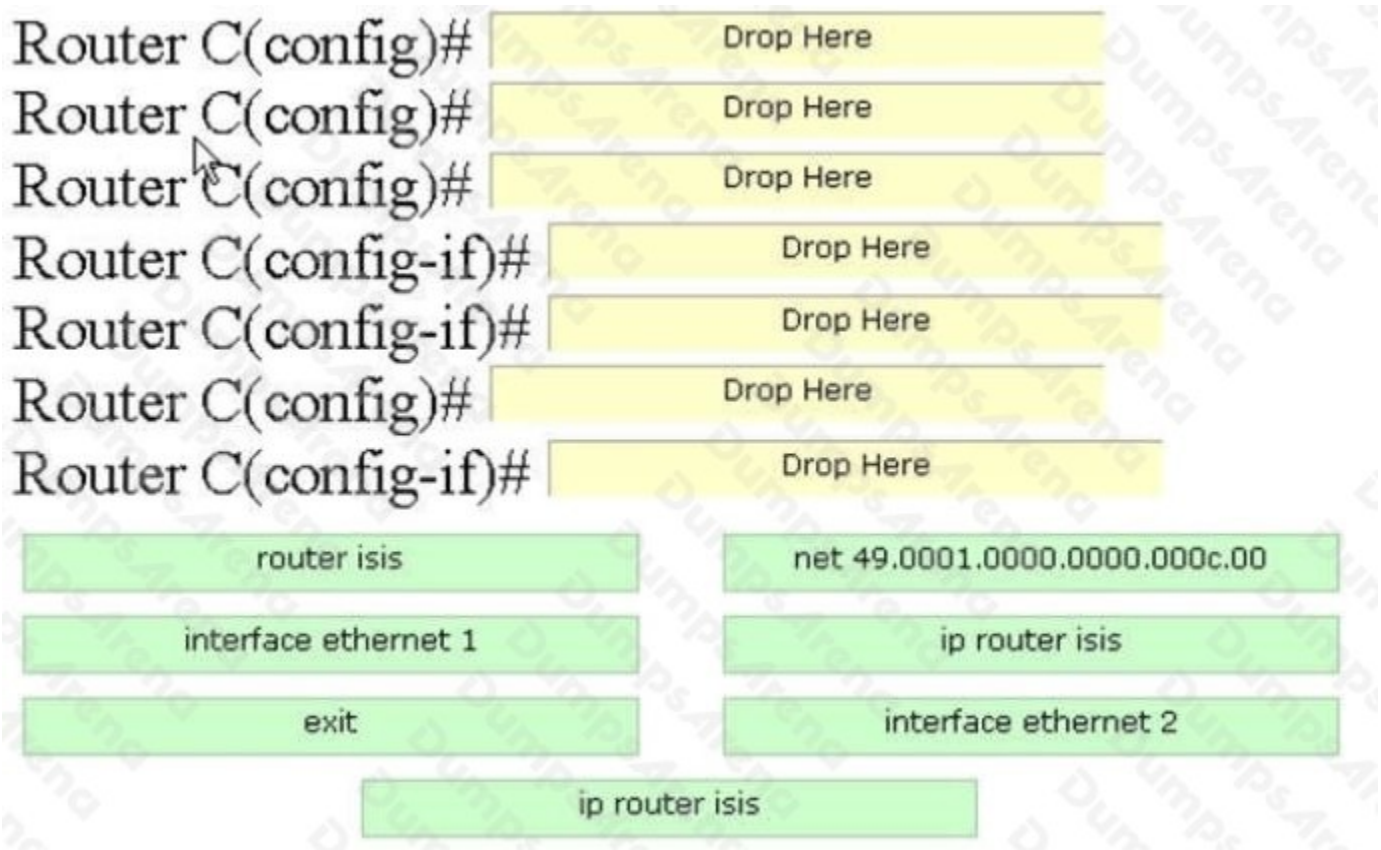
DRAG DROP

You have designed a TCP/IP based routed network. Diagram of the network is given below:

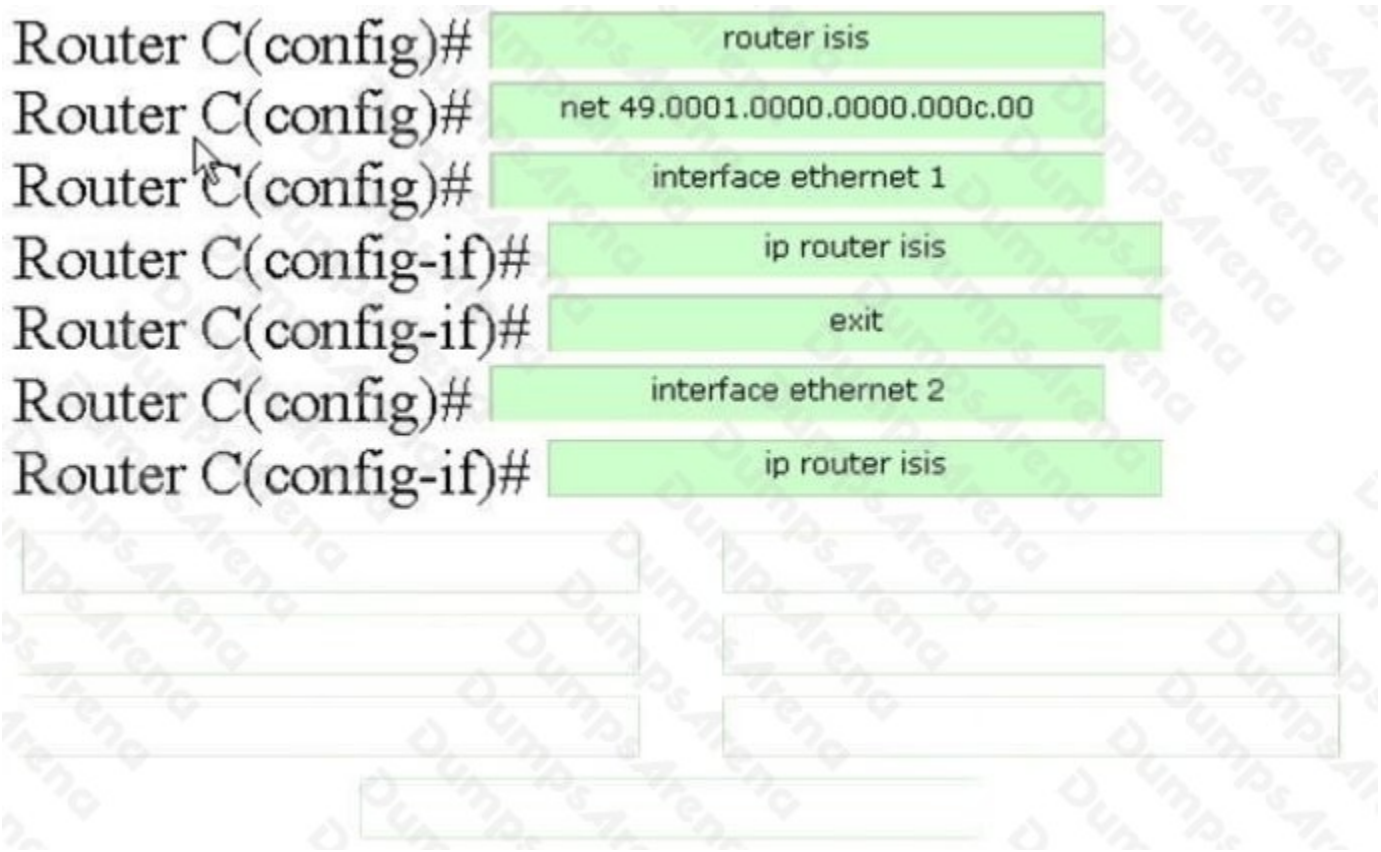


You are configuring IS-IS protocol as an IP routing protocol in the given network. Drag and drop the appropriate commands beside their respective command prompts which you are using at router C.

Select and Place:


Router C(config)#
Drop Here
Router C(config)#
Drop Here
Router C(config)#
Drop Here
Router C(config-if)#
Drop Here
Router C(config-if)#
Drop Here
Router C(config)#
Drop Here
Router C(config-if)#
Drop Here
router isis
net 49.0001.0000.0000.000c.00
interface ethernet 1
ip router isis
exit
interface ethernet 2
ip router isis

ANSWER:



Explanation:

The commands that are configured on router C are as follows:

Router C(config)#router isis

Router C(config)#net 49.0001.0000.0000.000c.00

RouterC(config)#interface ethernet 1

Router C(config-if)#ip router isis

Router C(config-if)#exit

Router C(config)#interface ethernet 2

Router C(config-if)#ip router isis

QUESTION NO: 12 - (SIMULATION)

SIMULATION

Fill in the blank with the appropriate command.

You want to search the most recent command that starts with the string 'user'. For this, you will enter the _____ command to get the desired result.

ANSWER: history !user

Explanation:

Here, you will use the history !user command to search the most recent command that starts with the string 'user'. In the bash shell, the history command is used to view the recently executed commands. History is on by default. A user can turn off history using the command set +o history and turn it on using set -o history. An environment variable HISTSIZE is used to inform bash about how many history lines should be kept. The following commands are frequently used to view and manipulate history:

Command	Description
history	Used to see the entire history
history N	Used to display last N lines of the history
history -d N	Used to delete line N from the history
history !!	Used to display the most recent history command
history !n	Used to view the Nth history command

QUESTION NO: 13

The employees of EWS Inc. require remote access to the company's Web servers. In order to provide solid wireless security, the company uses EAP-TLS as the authentication protocol.

Which of the following statements are true about EAP-TLS?

A. It uses password hash for client authentication.

B. It uses a public key certificate for server authentication.

C. It is supported by all manufacturers of wireless LAN hardware and software.

D. It provides a moderate level of security.

ANSWER: B C

Explanation:

EAP-TLS can use only a public key certificate as the authentication technique. It is supported by all manufacturers of wireless LAN hardware and software. The requirement for a client-side certificate, however unpopular it may be, is what gives EAP-TLS its authentication strength and illustrates the classic convenience vs. security trade-off.

QUESTION NO: 14

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He executes the following command in the terminal: echo $USER, $UID.

Which of the following will be displayed as the correct output of the above command?

A. John, 0

B. root, 0

C. root, 500

D. John, 502

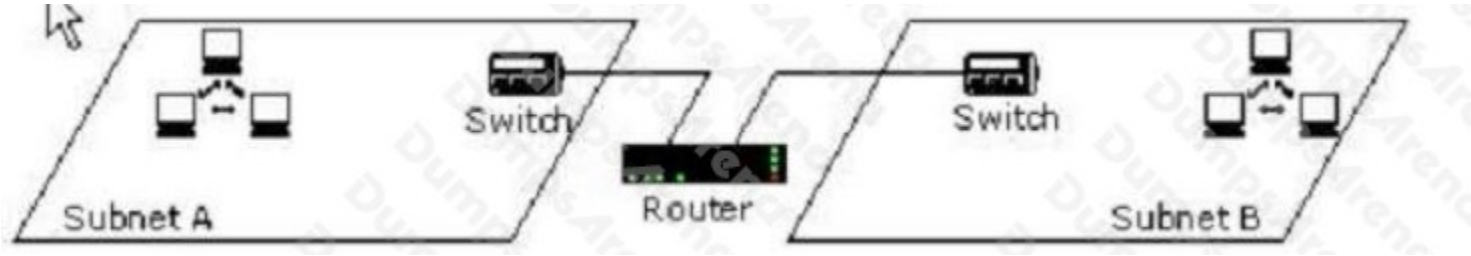
ANSWER: B

Explanation:

According to the scenario, John is a root user. Hence, the value of the environmental variables $USER and $UID will be root and 0, respectively.

QUESTION NO: 15

You work as a Network Administrator for Blue Well Inc. The company has a TCP/IP-based routed network. Two segments have been configured on the network as shown below:



One day, the switch in Subnet B fails. What will happen?

A. Communication between the two subnets will be affected.

B. The whole network will collapse.

C. Workstations on Subnet A will become offline

D. Workstations on Subnet B will become offline.

ANSWER: A D

Explanation:

According to the question, the network is a routed network where two segments have been divided and each segment has a switch. These switches are connected to a common router. All workstations in a segment are connected to their respective subnet's switches.

Failure of the switch in Subnet B will make all workstations connected to it offline. Moreover, communication between the two subnets will be affected, as there will be no link to connect to Subnet B.

QUESTION NO: 16

Which of the following key combinations in the vi editor is used to copy the current line?

A. dk

B. yy

C. d$

D. dl

ANSWER: B

Explanation:

The yy key combination in the vi editor is used to copy the current line. The vi editor is an interactive, cryptic, and screen-based text editor used to create and edit a file. It operates in either Input mode or Command mode. In Input mode, the vi editor accepts a keystroke as text and displays it on the screen, whereas in Command mode, it interprets keystrokes as commands. As the vi editor is case sensitive, it interprets the same character or characters as different commands, depending upon whether the user enters a lowercase or uppercase character. When a user starts a new session with vi, he must put the editor in Input mode by pressing the "I" key. If he is not able to see the entered text on the vi editor's screen, it means that he has not put the editor in Insert mode. The user must change the editor to Input mode before entering any text so that he can see the text he has entered.

QUESTION NO: 17

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement? (Choose two)

A. Using WPA encryption

B. MAC filtering the router

C. Not broadcasting SSID

D. Using WEP encryption

ANSWER: A D

Explanation:

With either encryption method (WEP or WPA) you can give the password to customers who need it, and even change it frequently (daily if you like). So this won't be an inconvenience for customers.

QUESTION NO: 18

Which of the following commands can be used to format text files?

A. wc

B. ps

C. tail

D. pr

ANSWER: D

Explanation:

The pr command is used to format text files according to the specified options. This command is usually used to paginate or columnate files for printing.

QUESTION NO: 19

You have to move the whole directory /foo to /bar. Which of the following commands will you use to accomplish the task?

A. mv /bar /foo

OPTION	DESCRIPTION
-f	It never asks before overwriting.
-i	It asks before overwriting.
-b	It makes a backup of each file that would otherwise be overwritten.
-v	It prints the name of each file before moving it.

C. mv /foo /bar

D. mv -r /bar /foo

ANSWER: C

Explanation:

You will use the mv /foo /bar command to move the whole directory /foo to /bar. The mv command moves files and directories from one directory to another or renames a file or directory. mv must always be given at least two arguments.

The first argument is given as a source file.

The second argument is interpreted as the destination.

If destination is an existing directory, the source file is moved to that directory with the same name as the source. If the destination is any other directory, the source file is moved and/or renamed to that destination name.

Syntax : mv [options] source destination Some important options used with mv command are as follows:

QUESTION NO: 20

Which of the following is a basic feature of the Unix operating system? (Choose three)

A. It is highly portable across hardware.

B. All files can be individually protected using read, write, and execute permissions for the user, group, and others.

C. It allows all the modules to be loaded into memory.

D. A user can execute multiple programs at the same time from a single terminal.

ANSWER: A B D

Explanation:

The basic features of Unix are as follows:

- Multi-user: It supports more than one user to access the system simultaneously through a set of terminals attached to a system.
- Multi-tasking: A user can execute multiple programs at the same time from a single terminal.
- Time sharing: The operating system shares CPU time among tasks.
- Portability: It is highly portable across hardware.
- Modularity: It allows only needed modules to be loaded into the memory.
- File structure: It has an inverted tree like file structure, with files and directories created within the file structure.
- Security: All files can be individually protected using read, write, and execute permissions for the user, group, and others.
- Network support: It uses the TCP/IP protocol.
- Advanced graphics: CAD-CAM applications perform the best in a Unix System with its varied support for graphics card.