Vendor:GIAC

Exam Code:GNSA

Exam Name:GIAC Systems and Network Auditor

Version: Demo

QUESTION 1

You are the Network Administrator for a software development company. Your company creates various utilities and tools. You have noticed that some of the files your company creates are getting deleted from systems. When one is deleted,

it seems to be deleted from all the computers on your network.

Where would you first look to try and diagnose this problem?

A. Antivirus log

B. IDS log

C. System log

D. Firewall log

Correct Answer: A

Check the antivirus log and see if it is detecting your file as a virus and deleting it. All antivirus programs have a certain rate of false positives. Since the file is being deleted from all computers, it seems likely that your antivirus has mistakenly

identified that file as a virus.

Answer: D is incorrect. The firewall log can help you identify traffic entering or leaving your network, but won\\'t help with files being deleted. Answer: B is incorrect. An IDS log would help you identify possible attacks, but this scenario is unlikely

to be from an external attack.

Answer: C is incorrect. Your system log can only tell you what is happening on that individual computer.

QUESTION 2

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

Correct Answer: B

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.

Answer: D is incorrect. It deletes next char on the right.

Answer: A is incorrect. It deletes the current line and one line above.

Answer: C is incorrect. It deletes from the cursor till the end of the line.

QUESTION 3

Which of the following tools hides information about IIS Webservers so that they can be prevented from various attacks performed by an attacker?

A. httprint

B. ServerMask

C. Whisker

D. WinSSLMiM

Correct Answer: B

ServerMask is a tool that is used to hide information about IISWebservers. Since IIS Webservers are vulnerable to various attacks, such as, code red worm, is unicode exploit, etc., to mitigate such attacks, ServerMask removes all unnecessary HTTP headers and response data, and file extensions like .asp or .aspx, whichare clear indicators that a site is running on a Microsoft server. Besides this, ServerMask modifies the ASP session ID cookies values, default messages, pages and scripts of all kinds to misguide an attacker. Answer: A is incorrect. httprint is a fingerprinting tool that is based on Web server characteristics to accurately identify Web servers. It works even when Web server may have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask. Answer: C is incorrect. Whisker is an HTTP/Web vulnerability scanner that is written in the PERL language. Whisker runs on both the Windows and UNIX environments. It provides functions for testing HTTP servers for many known security holes, particularly the presence of dangerous CGIs. Answer: D is incorrect. WinSSLMiM is an HTTPS Man in the Middle attacking tool. It includes FakeCert, a tool used to make fake certificates. It can be used to exploit the Certificate Chain vulnerability in Internet Explorer. The tool works under Windows 9x/2000.

QUESTION 4

Which of the following commands is most useful for viewing large files?

A. cat

B. less

C. touch

D. cp

Correct Answer: B

The less command is most useful for viewing large files. The less command displays the output of a file one page at a time. Viewing large files through cat may take more time to scroll pages, so it is better to use the less command to see the

content of large files.

Answer: A is incorrect. The cat command is also used to view the content of a file, but it is most useful for viewing short files.

Answer: D is incorrect. The cp command is used to copy files and directories from one location to another.

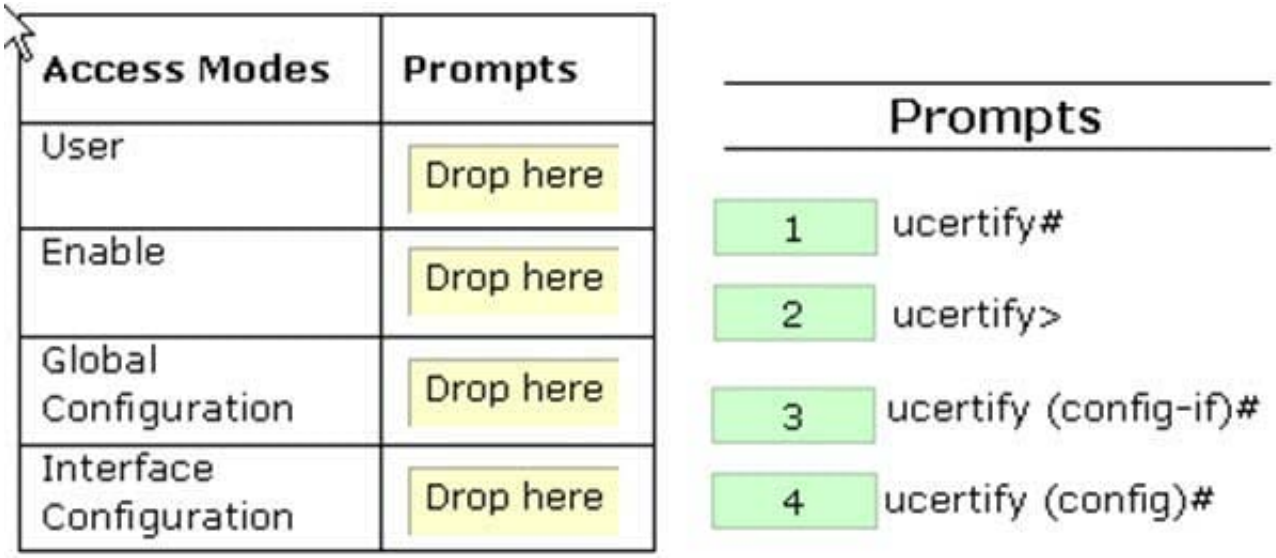
Answer: C is incorrect. The touch command is not used to view the content of a file. It is used to create empty files or to update file timestamps.

QUESTION 5

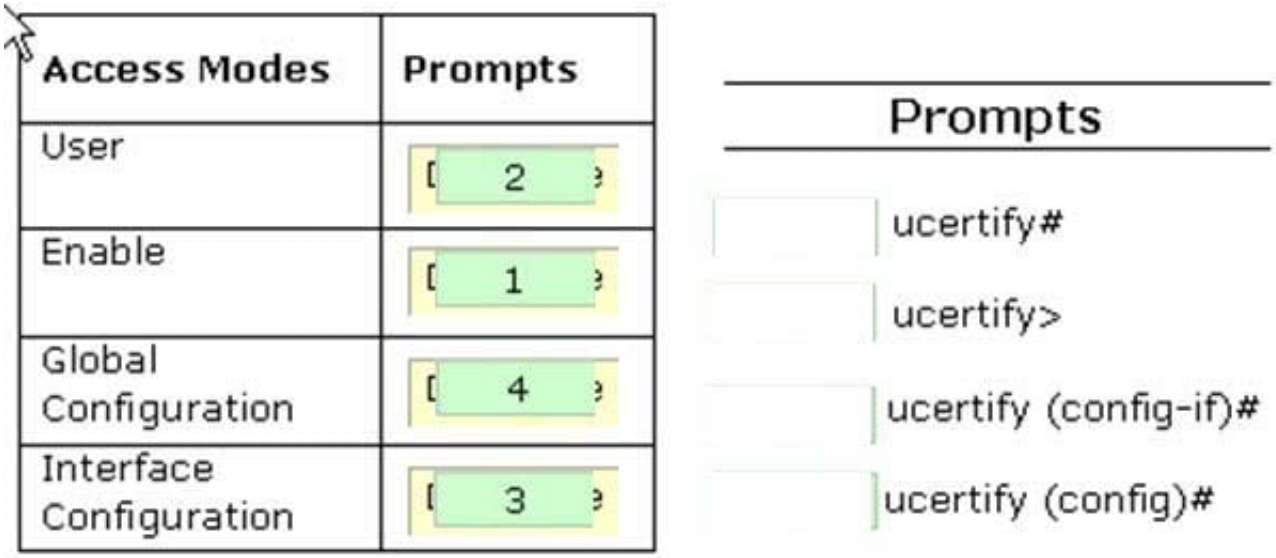
DRAG DROP

Drag and drop the corresponding prompt that is displayed in the command-line interface of a Cisco switch IOS for different access modes.

Select and Place:



Correct Answer:



There are four major CLI access modes: User: When a user accesses the command-line interface (CLI) of a Cisco switch IOS, the IOS puts the user in user mode. The user mode allows the user to look around; it does not permit the user to change or break any configuration. When the user enters a command, the switch executes the command and displays the command result. A Limited set of commands is available for use in the user mode. User mode is also called user EXEC mode. The prompt in this mode is displayed as hostname > Enable: Privileged EXEC mode is an area from where more powerful commands can be run while accessing CLI of a switch IOS. In this mode, more commands are added to the set of commands available in user mode. Privileged EXEC mode is also known as privileged mode or enable mode. For reaching privileged EXEC mode, the enable command is required to be run from user mode. By default, a user cannot get into privileged EXEC mode through SSH and Telnet sessions. The prompt changes from hostname > to hostname # when a user moves to privileged EXEC mode from user mode. Global configuration: Global configuration mode is an access mode of Cisco command-line interface (CLI). The configuration commands can be run in this mode only. Commands run in this mode update the active configuration file as soon as the Enter key is pressed at the end of a command. The config command is required to be run from the enable mode to switch to the global configuration mode. The prompt changes to hostname (config)# from hostname# when access mode is changed to global configuration mode from enable mode. Interface configuration: Interface configuration mode is a subcommand mode of the global configuration access mode of Cisco command-line interface (CLI). The interface command is used to move from global configuration mode to the interface configuration mode. The prompt changes to hostname (config-if)# from hostname (config)# when a user moves from global configuration mode to interface configuration mode. After entering the interface configuration mode, the commands executed affects only the interface that the user has selected. For example, the interface FastEthernet 0/1 command will put a user in the interface configuration mode. Commands executed afterwards will affect only the FastEthernet 0/1.

QUESTION 6

You work as an IT Technician for XYZ CORP. You have to take security measures for the wireless network of the company. You want to prevent other computers from accessing the company\\'s wireless network.

On the basis of the hardware address, which of the following will you use as the best possible method to accomplish the task?

A. RAS

B. MAC Filtering

C. SSID

D. WEP

Correct Answer: B

MAC filtering is a security access control technique that allows specific network devices to access, or prevents them from accessing, the network. MAC filtering can also be used on a wireless network to prevent certain network devices from accessing the wireless network. MAC addresses are allocated only to hardware devices, not to persons.

QUESTION 7

Which of the following statements is true about the Digest Authentication scheme?

A. A valid response from the client contains a checksum of the username, the password, the given random value, the HTTP method, and the requested URL.

B. In this authentication scheme, the username and password are passed with every request, not just when the user first types them.

C. The password is sent over the network in clear text format.

D. It uses the base64 encoding encryption scheme.

Correct Answer: A

The Digest Authentication scheme is a replacement of the Basic Authentication scheme. This authentication scheme is based on the challenge response model. In Digest authentication, the password is never sent across the network in clear text format but is always transmitted as an MD5 digest of the user\\'s password. In this way, the password cannot be determined with the help of a sniffer. How does it work? In this authentication scheme, an optional header allows the server to specify the algorithm used to create the checksum or digest (by default, the MD5 algorithm). The Digest Authentication scheme provides the challenge using a randomly chosen value. This randomly chosen value is a server-specified data string which may be uniquely generated each time a 401 response is made. A valid response contains a checksum (by default, the MD5 checksum) of the username, the password, the given random value, the HTTP method, and the requested URL. In this way, the password is never sent in clear text format. Drawback: Although the password is not sent in clear text format, an attacker can gain access with the help of the digested password, since the digested password is really all the information needed to access the web site. Answer: B, C, D are incorrect. These statements are true about the Basic Authentication scheme.

QUESTION 8

You work as a Software Developer for UcTech Inc. You want to encode a URL, so that it can be used with the sendRedirect() method to send the response to the client. In order to accomplish this, you have to use a method of the HttpServletResponse interface.

Which of the following methods will you use?

A. encodeResponseURL()

B. encodeRedirectURL()

C. encodeURL()

D. encodeURLResponse()

Correct Answer: B

The encodeRedirectURL() method of the HttpServletResponse interface, returns a URL by including a session ID in it for use in the sendRedirect() method. If the encoding is not required, the URL is returned unchanged. If browser supports

cookies, the encodeRedirectURL() method returns the input URL unchanged, since the session ID will be persisted as a cookie. This method is different from the encodeURL as this method redirects the request to a different URL in the same

session. The syntax of the encodeRedirectURL() method is as follows:

public String encodeRedirectURL(String urlstring)Here, urlstring is the URL to be encoded.

Answer: C is incorrect. The encodeURL() method of the HttpServletResponse interface returns a URL by including the session ID in it. If the encoding is not required, the URL is returned unchanged. If cookies are supported by the browser,

the encodeURL() method returns the input URL unchanged since the session ID will be persisted as a cookie.

The syntax of the encodeURL() method is as follows:

public String encodeURL(String urlstring) Here, urlstring is the URL to be encoded.

QUESTION 9

Which of the following is an attempt to give false information or to deny that a real event or transaction should have occurred?

A. A DDoS attack

B. A repudiation attack

C. A reply attack

D. A dictionary attack

Correct Answer: B

A repudiation attack is an attempt to give false information or to deny that a real event or transaction should have occurred. Answer: A is incorrect. In a distributed denial of service (DDOS) attack, an attacker uses multiple computers throughout the network that has been previously infected. Such computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. TFN, TRIN00, etc. are tools used for a DDoS attack. Answer: C is incorrect. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Answer: D is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks.

QUESTION 10

Which of the following internal control components provides the foundation for the other components and encompasses such factors as management\\'s philosophy and operating style?

A. Information and communication

B. Risk assessment

C. Control activities

D. Control environment

Correct Answer: D

COSO defines internal control as, "a process, influenced by an entity\\'s board of directors, management, and other personnel, that is designed to provide reasonable assurance in the effectiveness and efficiency of operations, reliability of financial reporting, and the compliance of applicable laws and regulations". The auditor evaluates the organization\\'s control structure by understanding the organization\\'s five interrelated control components, which are as follows:

1.

Control Environment: It provides the foundation for the other components and encompasses such factors as management\\'s philosophy and operating style.

2.

Risk Assessment: It consists of risk identification and analysis.

3.

Control Activities: It consists of the policies and procedures that ensure employees carry out management\\'s directions.

The types of control activities an organization must implement are preventative controls (controls intended to stop an error from occurring), detective controls (controls intended to detect if an error has occurred), and mitigating controls (control

activities that can mitigate the risks associated with a key control not operating effectively).

4.

Information and Communication: It ensures the organization obtains pertinent information, and then communicates it throughout the organization.

5.

Monitoring: It involves reviewing the output generated by control activities and conducting special evaluations. In addition to understanding the organization\\'s control components, the auditor must also evaluate the organization\\'s General

and Application controls. There are three audit risk components: control risk, detection risk, and inherent risk.

QUESTION 11

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to check the status of the printer and set its state.

Which of the following Unix commands can you use to accomplish the task?

A. banner

B. lpq

C. lpc

D. lpr

Correct Answer: C

In Unix, the lpc command is used to check the status of the printer and set its state.

Answer: A is incorrect. In Unix, the banner command is used to print a large banner on the printer.

Answer: D is incorrect. In Unix, the lpr command is used to submit a job to the printer.

Answer: B is incorrect. In Unix, the lpq command is used to show the contents of a spool directory for a given printer.

QUESTION 12

Which of the following statements about a perimeter network are true? (Choose three)

A. It has a connection to the Internet through an external firewall and a connection to an internal network through an interior firewall.

B. It has a connection to a private network through an external firewall and a connection to an internal network through an interior firewall.

C. It is also known as a demilitarized zone or DMZ.

D. It prevents access to the internal corporate network for outside users.

Correct Answer: ACD

A perimeter network, also known as a demilitarized zone or DMZ, is a small network that lies in between the Internet and a private network. It has a connection to the Internet through an external firewall and a connection to the internal network through an interior firewall. It allows outside users access to the specific servers located in the perimeter network while preventing access to the internal corporate network. Servers, routers, and switches that maintain security by preventing the internal network from being exposed on the Internet are placed in a perimeter network. A perimeter network is commonly used for deploying e-mail and Web servers for a company.