DUMPSQUEEN

GIAC Systems and Network Auditor

GIAC GSNA

Version Demo

Total Demo Questions: 20

Total Premium Questions: 413

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

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

Data access auditing is a surveillance mechanism that watches over access to all sensitive information contained within the database.

What are the questions addressed in a perfect data access auditing solution?

A. Who accessed the data?

B. When was the data accessed?

C. For whom was the data accessed?

D. What was the SQL query that accessed the data?

ANSWER: A B D

Explanation:

The perfect data access auditing solution would address the following six questions:

1. Who accessed the data? 2.

When was the data accessed?

3.Which computer program or client software was used to access the data?

4.From what location on the network was the data accessed?

5.What was the SQL query that accessed the data?

QUESTION NO: 2

Which of the following mechanisms is closely related to authorization?

A. Sending secret data such as credit card information.

B. Allowing access to a particular resource.

C. Verifying username and password.

D. Sending data so that no one can alter it on the way.

ANSWER: B

QUESTION NO: 3

You work as a Database Administrator for Dolliver Inc. The company uses Oracle 11g as its database. You have used the LogMiner feature for auditing purposes.

Which of the following files store a copy of the data dictionary? (Choose two)

A. Online redo log files

B. Operating system flat file

C. Dump file

D. Control file

ANSWER: A B

Explanation:

LogMiner requires a dictionary to translate object IDs into object names when it returns redo data to you. You have the following three options to retrieve the data dictionary:

The Online catalog: It is the most easy and efficient option to be used. It is used when a database user have access to the source database from which the redo log files were created. The other condition that should qualify is that there should be no changes to the column definitions in the desired tables.

The Redo Log Files: This option is used when a database user does not have access to the source database from which the redo log files were created and if there are any chances of changes to the column definitions of the desired tables.

An operating system flat file: Oracle does not recommend to use this option, but it is retained for backward compatibility. The reason for not preferring the option is that it does not guarantee transactional consistency. LogMiner is capable to access the Oracle redo logs. It keeps the complete record of all the activities performed on the database, and the associated data dictionary, which is used to translate internal object identifiers and types to external names and data formats. For offline analysis, LogMiner can be run on a separate database, using archived redo logs and the associated dictionary from the source database.

QUESTION NO: 4

Which of the following statements about invalidating a session is true?

A. The getCreationTime() method can be called on an invalidated session.

B. The invalidate() method belongs to the HttpServletRequest interface.

C. A session can be invalidated programmatically as well as using the deployment descriptor.

D. The getAttribute(String name) method throws an IllegalArgumentException if called on an invalidated session.

ANSWER: C

Explanation:

An existing session can be invalidated in the following two ways:

Setting timeout in the deployment descriptor:

This can be done by specifying timeout between the tags as follows: 10 This will set the time for session timeout to be ten minutes.

Setting timeout programmatically: This will set the timeout for a specific session.

The syntax for setting the timeout programmatically is as follows: session.setMaxInactiveInterval(10*60)

In this method, the timeout is specified in seconds. Hence, this will set the time for the session timeout to be ten minutes.

QUESTION NO: 5 - (SIMULATION)

SIMULATION

Fill in the blanks with the appropriate protocol.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an IEEE encryption protocol created to replace both TKIP and ______.

ANSWER: WEP

Explanation:

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an IEEE 802.11i encryption protocol created to replace both TKIP, the mandatory protocol in WPA, and WEP, the earlier, insecure protocol. CCMP is a mandatory part of the WPA2 standard, an optional part of the WPA standard, and a required option for Robust Security Network (RSN) Compliant networks. CCMP is also used in the ITU-T home and business networking standard. CCMP, part of the 802.11i standard, uses the Advanced Encryption Standard (AES) algorithm. Unlike in TKIP, key management and message integrity is handled by a single component built around AES using a 128-bit key, a 128-bit block, and 10 rounds of encoding per the FIPS 197 standard.

QUESTION NO: 6

You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?

A. Manual penetration testing

B. Automated penetration testing

C. Vulnerability scanning

D. Code review

ANSWER: C

Explanation:

Vulnerability scanning will be the best method to find flaws in applications allowing some attacker to get into your network. There are a number of tools available that will check Web applications for security flaws. They examine the application and identify any potential flaws due to improper coding, such as SQL injection attacks.

Answer D is incorrect. A code review might well discover some issues with the Web applications. But it is long, tedious, and depends on the human reviewer noticing the coding flaws. So it is not as good a solution as vulnerability scanning.

QUESTION NO: 7

Which of the following statements are true about security risks? (Choose three)

A. They can be removed completely by taking proper actions.

B. They are considered an indicator of threats coupled with vulnerability.

C. They can be mitigated by reviewing and taking responsible actions based on possible risks.

D. They can be analyzed and measured by the risk analysis process.

ANSWER: B C D

Explanation:

In information security, security risks are considered an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. These risks can be analyzed and measured by the risk analysis process.

QUESTION NO: 8

An attacker wants to connect directly to an unsecured station to circumvent the AP security or to attack the station.

Which of the following tools can be used to accomplish the task?

A. Wireless card

B. MacChanger

C. SirMACsAlot

D. USB adapter

ANSWER: A D

Explanation:

Ad Hoc Association is a type of attack in which an attacker tries to connect directly to an unsecured station to circumvent the AP security or to attack the station. Any wireless card or USB adapter can be used to perform this attack.

QUESTION NO: 9

You work as a Network Administrator for XYZ CORP. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest network.

You configure a new Windows Server 2008 server in the network. The new server is not yet linked to Active Directory. You are required to accomplish the following tasks:

Add a new group named "Sales".

Copy the "Returns" group from the older server to the new one.

Rename the "Returns" group to "Revenue".

View all group members, including for multiple groups/entire domain. You use Hyena to simplify and centralize all of these tasks.

Which of the assigned tasks will you be able to accomplish?

A. Copy the "Returns" group to the new server.

B. Rename the "Returns" group to "Revenue".

C. Add the new group named "Sales".

D. View and manage all group members, including for multiplegroups/entire domain.

ANSWER: A B C

Explanation:

Hyena supports the following group management functions:

Full group administration such as add, modify, delete, and copy

Rename groups

Copy groups from one computer to another

View both direct and indirect (nested) group members for one or more groups [only for Active Directory]

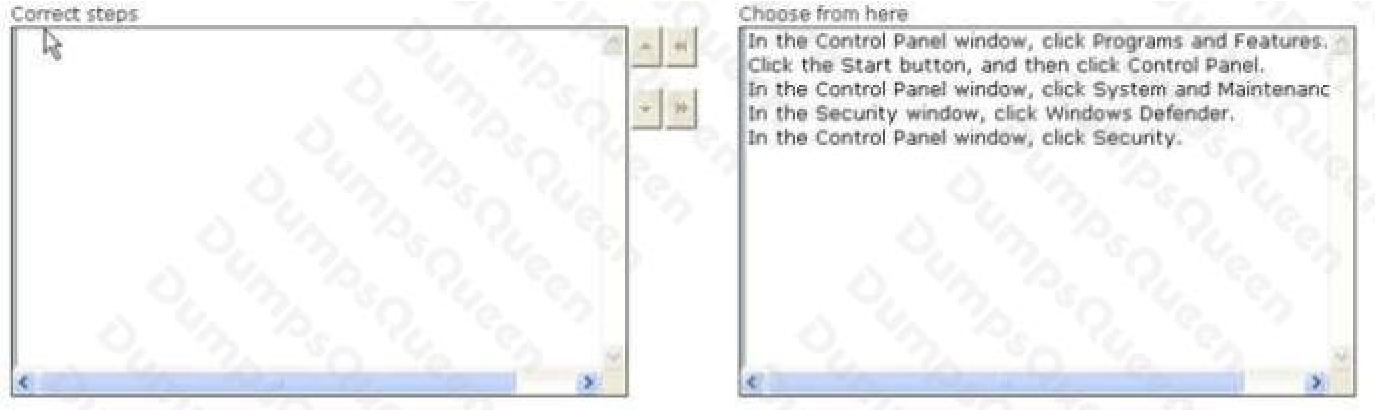
QUESTION NO: 10 - (DRAG DROP)

DRAG DROP

John works as a Network Administrator for Blue Well Inc. All client computers in the company run the Windows Vista operating system.

He wants to view the status of Windows Defender. What steps will he take to accomplish the task?

Select and Place:

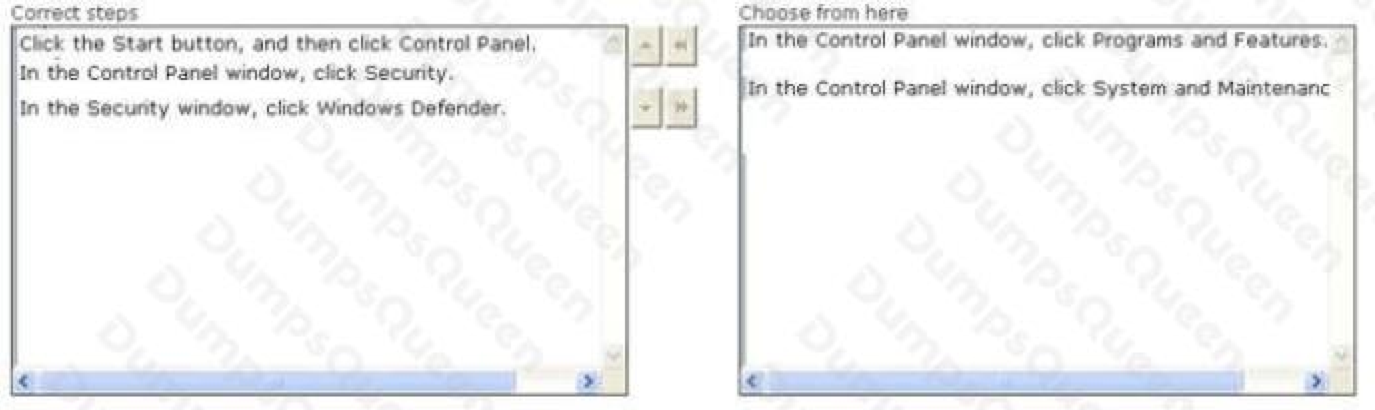


Correct steps

Choose from here

In the Control Panel window, click Programs and Features.
Click the Start button, and then click Control Panel.
In the Control Panel window, click System and Maintenanc
In the Security window, click Windows Defender.
In the Control Panel window, click Security.

ANSWER:



Correct steps

Click the Start button, and then click Control Panel.
In the Control Panel window, click Security.
In the Security window, click Windows Defender.

Choose from here

In the Control Panel window, click Programs and Features.
In the Control Panel window, click System and Maintenanc

Explanation:

Windows Defender is a software product designed by Microsoftto provide continuous security against malware. If it detects anything suspicious, an alert will appear on the screen. Windows Defender can also be used to scan a computer for suspicious software. It can remove or quarantine any malware or spyware it finds.

Clicking on the Security Center icon will show the status of malware protection, status of firewall, and other security settings.

Clicking on the Windows Firewall icon will open the Windows Firewall dialog box and allow a user to configure the Windows Firewall settings.

QUESTION NO: 11

You work as the Network Administrator for XYZ CORP. The company has a Linux-based network. You are a root user on the Red Hat operating system. You want to see first five lines of the file / etc/passwd.

Which of the following commands should you use to accomplish the task?

A. head -n 5 /etc/passwd

B. head 5 -n /etc/passwd

C. tail -n 5 /etc/passwd

D. head /etc/passwd

ANSWER: A

Explanation:

The head -n 5 /etc/passwd command will show the first 5 lines of the file /etc/passwd.

QUESTION NO: 12

Which of the following are the goals of risk management? (Choose three)

A. Identifying the risk

B. Assessing the impact of potential threats

C. Finding an economic balance between the impact of the risk and the cost of the countermeasure

D. Identifying the accused

ANSWER: A B C

Explanation:

There are three goals of risk management as follows:

- Identifying the risk
- Assessing the impact of potential threats
- Finding an economic balance between the impact of the risk and the cost of the countermeasure

QUESTION NO: 13

Zorp is a proxy firewall suite developed by Balabit IT Security.

Which of the following statements are true about Zorp?

A. It allows the administrators to fine-tune proxy decisions.

B. Zorp aims for compliance with the Common Criteria/Application Level Firewall Protection Profile for Medium Robustness.

C. It allows full analysis of embedded protocols.

D. The GPL versionof Zorp lacks much of the usability and functions from the other versions.

ANSWER: A B C

Explanation:

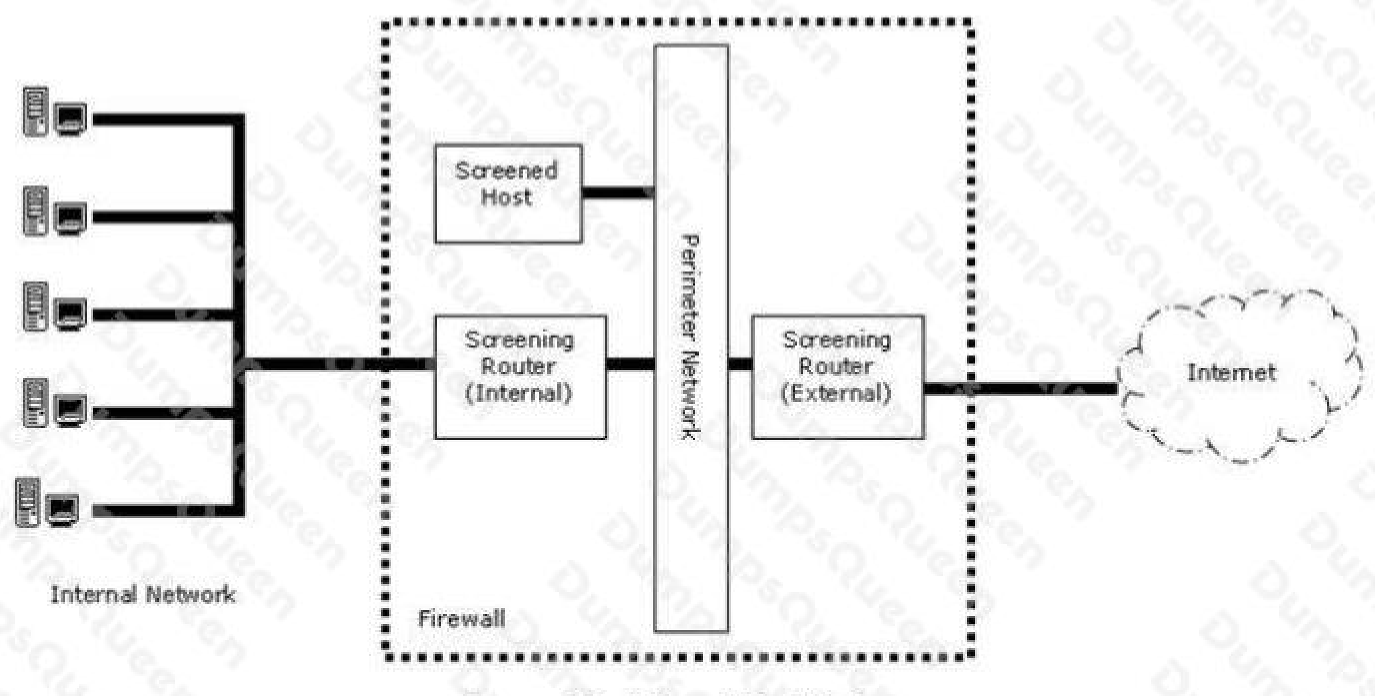
Zorp is a proxy firewall suite developed by Balabit IT Security. Its core framework allows the administrator to fine-tune proxy decisions (with its built-in script language), and fully analyze embedded protocols (such as SSL with an embedded POP3 or HTTP protocol). The FTP, HTTP, FINGER, WHOIS, TELNET, and SSL protocols are fully supported with an application-level gateway. Zorp aims for compliance with the Common Criteria/Application Level Firewall Protection Profile for Medium Robustness. Zorp is released under GNU/GPL and commercial license too. The GPL version is completely usable and functional; however, it lacks some of the more advanced functions available in the commercially available version only. Some of the Zorp supported protocols are Finger, Ftp, Http, Pop3, NNTP, IMAP4, RDP, RPC, SIP, SSL, SSH, Telnet, Whois, LDAP, RADIUS, TFtp, SQLNet NET8, Rsh, etc.

QUESTION NO: 14 - (HOTSPOT)

HOTSPOT

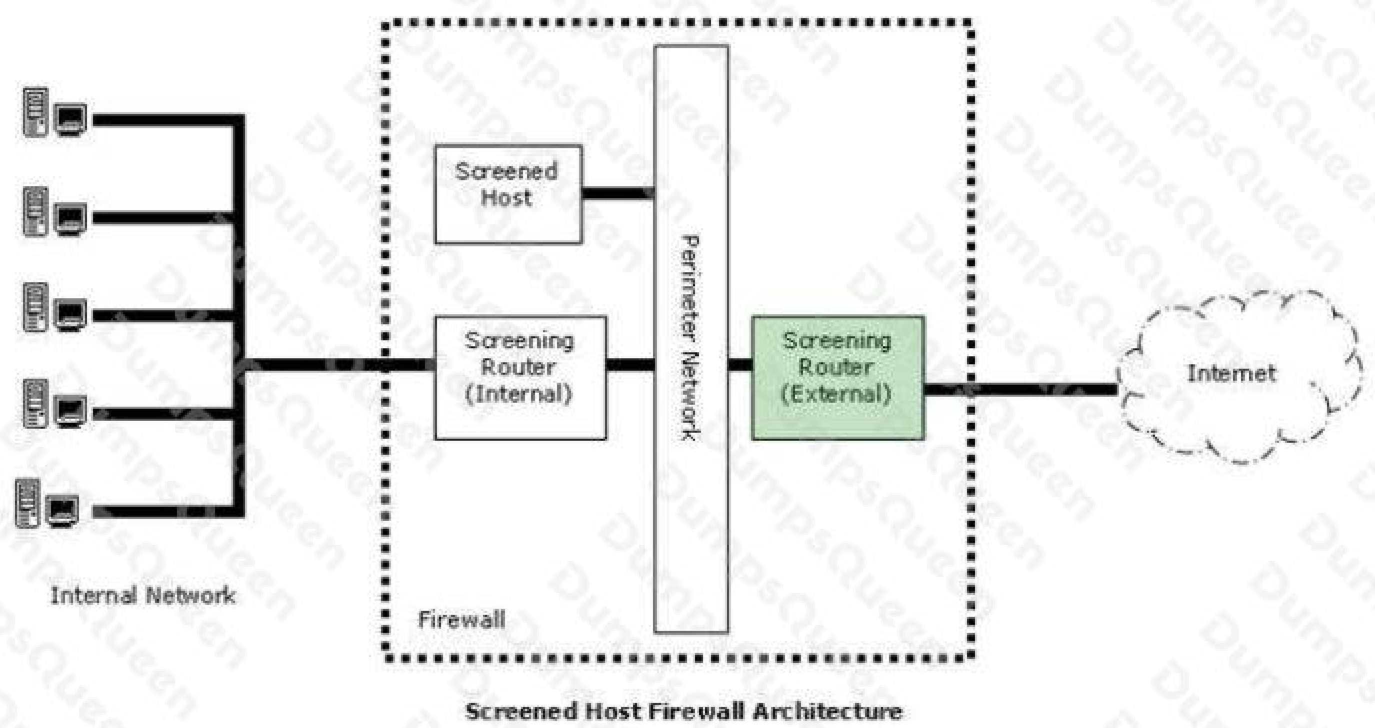
In the image of the Screened Host Firewall Architecture given below, select the element that is commonly known as the access router.

Hot Area:



Screened Host Firewall Architecture

ANSWER:

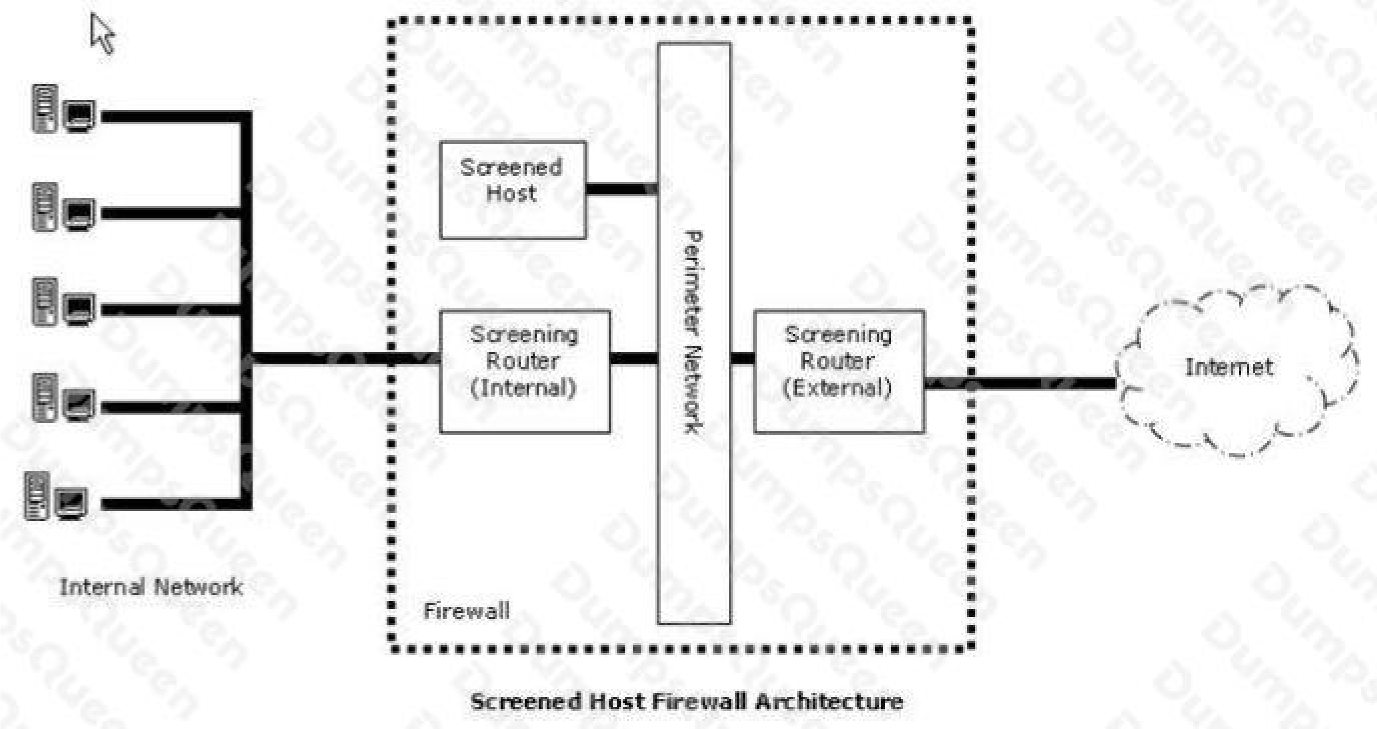

Screened Host
Screening Router (Internal)
Perimeter Network
Screening Router (External)
Internet
Internal Network
Firewall
Screened Host Firewall Architecture

Explanation:

An access router is the common name of the exterior router present in the screened host firewall architecture. It is attached to the perimeter network and the Internet. An access router is used to protect both the perimeter network and the internal network from the Internet. It allows anything that is outbound from the perimeter network. Access routers seldom do packet filtering. The rules for packet filtering regarding the protection of internal machines are always the same on both the interior router and the exterior router.

A Screened Host Firewall Architecture is used to provide services from a host that is attached only to the internal network by using a separate router. In this type of firewall architecture, the key security is provided by packet filtering.

The host exists in the internal network. The packet filtering on the screening router is configured in such a way that the bastion host is the only system in the internal network that is open to the Internet connections. If any external system tries to access internal systems or services, then it will connect only to this host. The bastion host therefore needs to be at a high level of security.



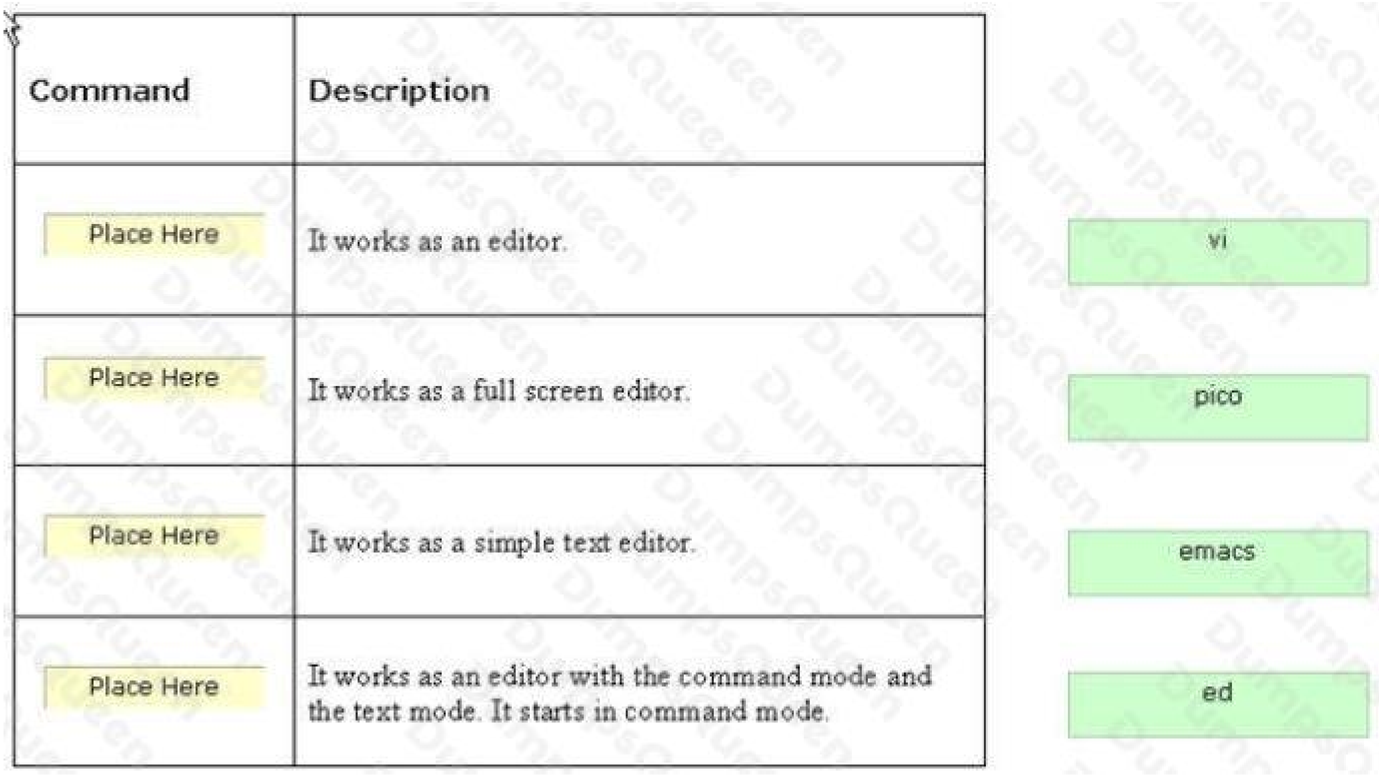
Screened Host Firewall Architecture

QUESTION NO: 15 - (DRAG DROP)

DRAG DROP

In Unix, there are different commands used for editing and viewing files. Drag and drop the appropriate commands (available in Unix) in front of their respective functions that they perform.

Select and Place:



Command	Description
Place Here	It works as an editor.
Place Here	It works as a full screen editor.
Place Here	It works as a simple text editor.
Place Here	It works as an editor with the command mode and the text mode. It starts in command mode.

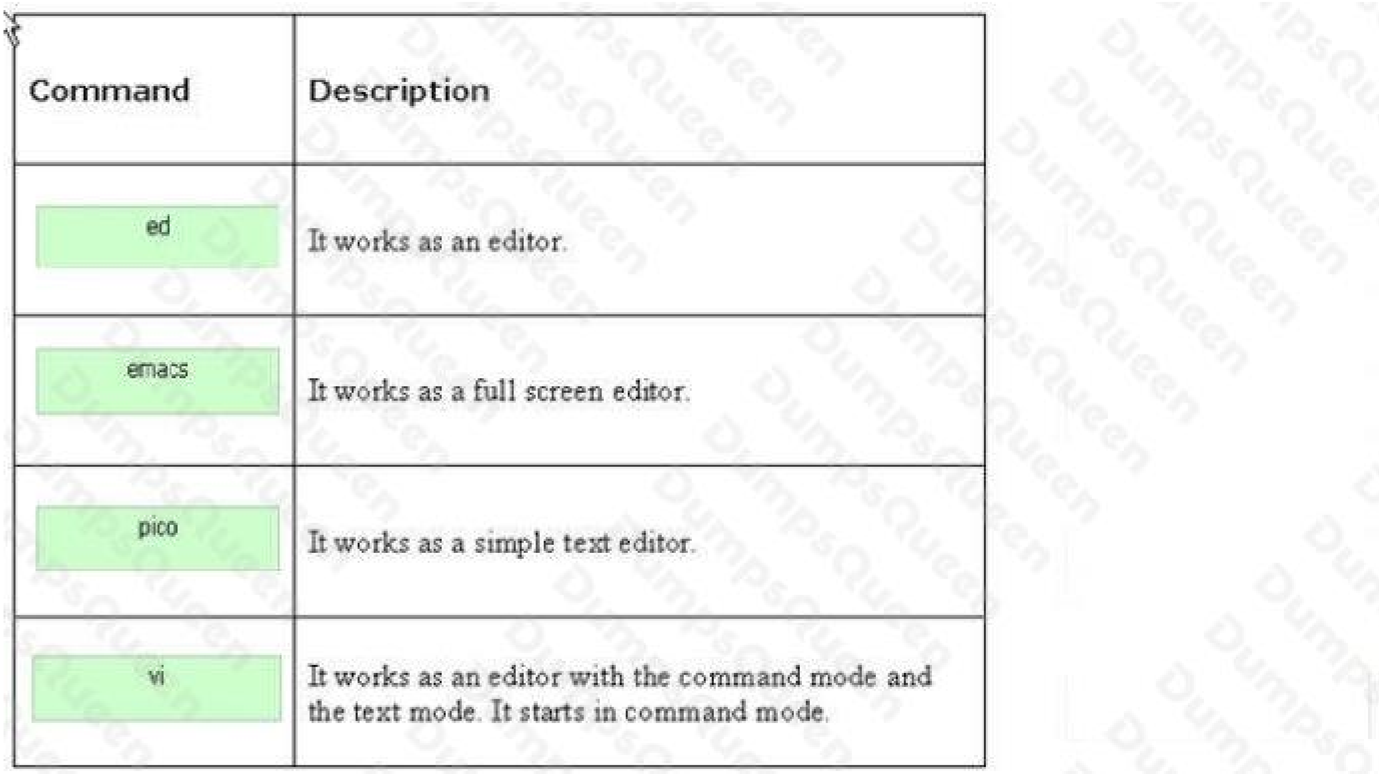
vi

pico

emacs

ed

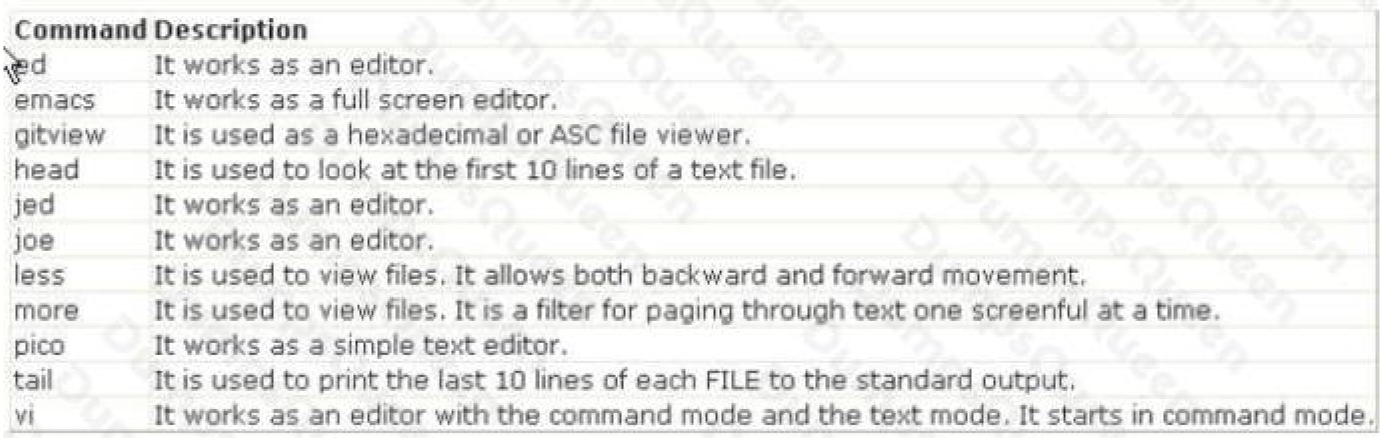
ANSWER:



Command	Description
ed	It works as an editor.
emacs	It works as a full screen editor.
pico	It works as a simple text editor.
vi	It works as an editor with the command mode and the text mode. It starts in command mode.

Explanation:

Following are the basic file editing and viewing commands in Unix:



Command	Description
ed	It works as an editor.
emacs	It works as a full screen editor.
gitview	It is used as a hexadecimal or ASC file viewer.
head	It is used to look at the first 10 lines of a text file.
jed	It works as an editor.
joe	It works as an editor.
less	It is used to view files. It allows both backward and forward movement.
more	It is used to view files. It is a filter for paging through text one screenful at a time.
pico	It works as a simple text editor.
tail	It is used to print the last 10 lines of each FILE to the standard output.
vi	It works as an editor with the command mode and the text mode. It starts in command mode.

QUESTION NO: 16

You work as a Network Administrator for NTY Inc. The company has a secure wireless network. While auditing the network for maintaining security, you find an unknown node. You want to locate that node.

Which tool will you use to pinpoint the actual physical location of the node?

A. Kismet

B. Ekahau

C. WEPCrack

D. AirSnort

ANSWER: B

Explanation:

Ekahau is an easy-to-use powerful and comprehensive tool for network site surveys and optimization. It is an auditing tool that can be used to pinpoint the actual physical location of wireless devices in the network. This tool can be used to make a map of the office and then perform the survey of the office. In the process, if one finds an unknown node, ekahau can be used to locate that node.

- To identify networks by passively collecting packets
- To detect standard named networks
- To detect masked networks
- To collect the presence of non-beaconing networks via data traffic

WeakIVGen: It allows a user to emulate the encryption output of 802.11 networks to weaken the secret key used to encrypt the network traffic.

Prism-getIV: It analyzes packets of information until ultimately matching patterns to the one known to decrypt the secret key.

WEPcrack: It pulls the all beneficial data of WeakIVGen and Prism-getIV to decipher the network encryption.

QUESTION NO: 17

You have recently joined as a Network Auditor in XYZ CORP. The company has a Windowsbased network. You have been assigned the task to determine whether or not the company's goal is being achieved.

As an auditor, which of the following tasks should you perform before conducting the data center review? Each correct answer represents a complete solution. Choose three.

A. Review the future IT organization chart.

B. Meet with IT management to determine possible areas of concern.

C. Review the company's IT policies and procedures.

D. Research all operating systems, software applications, and data center equipment operating within the data center.

ANSWER: B C D

Explanation:

The auditor should be adequately educated about the company and its critical business activities before conducting a data center review. The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes. To adequately determine if whether or not the client's goal is being achieved, the auditor should perform the following before conducting the review: Meet with IT management to determine possible areas of concern. Review the current IT organization chart. Review job descriptions of data center employees. Research all operating systems, software applications, and data center equipment operating within the data center. Review the company's IT policies and procedures. Evaluate the company's IT budget and systems planning documentation. Review the data center's disaster recovery plan.

QUESTION NO: 18

Which of the following features of a switch helps to protect network from MAC flood and MAC spoofing?

A. Multi-Authentication

B. Port security

C. MAC Authentication Bypass

D. Quality of Service (QoS)

ANSWER: B

Explanation:

If a switch has the ability to enable portsecurity, this will help to protect network from both the MAC Flood and MAC Spoofing attacks.

QUESTION NO: 19

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: 20

Which of the following methods is used to get a cookie from a client?

Note: Here, request is a reference of type HttpServletRequest, and response is a reference of type HttpServletResponse.

A. Cookie [] cookies = request.getCookies();

B. Cookie [] cookies = request.getCookie(String str)

C. Cookie [] cookies = response.getCookie(String str)

D. Cookie[] cookies = response.getCookies()

ANSWER: A

Explanation:

The getCookies() method of the HttpServletRequest interface is used to get the cookies from a client. This method returns an array of cookies.