Free Questions for GSNA by actualtestdumps

Shared by Frazier on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

A sequence number is a 32-bit number ranging from 1 to 4,294,967,295. When data is sent over the network, it is broken into fragments

(packets) at the source and reassembled at the destination system. Each packet contains a sequence number that is used by the destination

system to reassemble the data packets in the correct order.

The Initial Sequence Number of your computer is 24171311 at login time. You connect your computer to a computer having the IP address

210.213.23.21. This whole process takes three seconds. What will the value of the Initial Sequence Number be at this moment?

Options:

A- 24171811

B- 24619311

C- 24171111

D- 24171311

Answer:

B

Explanation:

You took 3 seconds to establish a connection. During this time, the value of the Initial Sequence Number would become [24171311 + (1 * 64000) + (3 * 128000)], i.e., 24619311.

Question 2

Question Type: MultipleChoice

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

Options:

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 port security, this will help to protect network from both the MAC Flood and MAC Spoofing attacks.

Answer D is incorrect. Quality of Service (QoS) feature is useful for prioritizing VOIP traffic. Switches are offering the ability to assign a

device a Quality of Service (QoS) value or a rate limiting value based on the RADIUS response.

Answer A is incorrect. Multi-Authentication feature is used to allow multiple devices to use a single port.

Answer C is incorrect. MAC Authentication Bypass feature is used to allow the RADIUS server to specify the default VLAN/ACL for every

device that doesn't authenticate by 802.1X.

Question 3

Question Type: **MultipleChoice**

Which of the following Web authentication techniques uses a single sign-on scheme?

Options:

A- NTLM authentication

B- Digest authentication

C- Microsoft Passport authentication

D- Basic authentication

Answer:

C

Explanation:

Microsoft Passport authentication is based on single sign-on authentication in which a user needs to remember only one username and

password to be authenticated for multiple services. The Passport is a suite of services for authenticating users across a number of

applications. The Passport single sign-on service is an authentication service allowing users to create a single set of credentials that will

enable them to sign in to any participating site that supports the Passport service. It enables the use of one set of credentials to access any

Passport-enabled site such as MSN, Hotmail, and MSN Messenger.

Question 4

Question Type: MultipleChoice

You work as a Desktop Support Technician for uCertify Inc. The company uses a Windows-based network comprising 50 Windows XP

Professional computers. You want to include the Safe Mode with Command Prompt feature into the boot.ini file of a Windows XP Professional

computer. Which of the following switches will you use?

Options:

A- /safeboot:network /sos /bootlog /noguiboot

B- /safeboot:minimal /sos /bootlog /noguiboot

C- /safeboot:minimal(alternateshell) /sos /bootlog /noguiboot

D- /safeboot:dsrepair /sos

Answer:

C

Explanation:

Safe-mode boot switches are used in the Windows operating systems to use the afe-mode boot feature. To use this feature the user should

press F8 during boot. These modes are available in the Boot.ini file. Users can also automate the boot process using this feature. Various

switches used for various modes are given below:

Mode	Switch
Safe Mode	/safeboot:minimal /sos /bootlog /noguiboot
Safe Mode with Networking	/safeboot:network /sos /bootlog /noguiboot
Safe Mode with Command Prompt	/safeboot:minimal (alternateshell) /sos /bootlog /noguiboot
Enable Boot Logging	/bootlog
Enable VGA Mode	/basevideo
Directory Services Restore Mode (Domain Controllers Only)	/safeboot:dsrepair /sos
Debugging Mode	/debug

Question 5

The Security Auditor's Research Assistant (SARA) is a third generation network security analysis tool. Which of the following statements are true about SARA?

Each correct answer represents a complete solution. Choose two.

Options:

A- It operates under Unix, Linux, MAC OS/X, or Windows (through coLinux) OS.

B- It cannot be used to perform exhaustive XSS tests.

C- It cannot be used to perform SQL injection tests.

D- It supports plug-in facility for third party apps.

Answer:

A, D

Explanation:

The Security Auditor's Research Assistant (SARA) is a third generation network security analysis tool. It has the following functions:

It operates under Unix, Linux, MAC OS/X, or Windows (through coLinux) OS.

It integrates the National Vulnerability Database (NVD).

It can be used to perform SQL injection tests.

It can be used to perform exhaustive XSS tests.

It can be adapted to multiple firewalled environments.

It supports remote self scan and API facilities.

It is used for CIS benchmark initiatives.

It also supports plug-in facility for third party apps.

It supports CVE standards.

It works as an enterprise search module.

It works in both standalone or demo mode.

Answer C is incorrect. SARA can be used to perform SQL injection tests.

Answer B is incorrect. SARA can be used to perform exhaustive XSS tests.

Question 6

Which of the following wireless security standards supported by Windows Vista provides the highest level of security?

Options:

A- WPA-EAP

B- WEP

C- WPA-PSK

D- WPA2

Answer:

D

Explanation:

WPA2 is an updated version of WPA. This standard is also known as IEEE 802.11i. WPA2 offers enhanced protection to wireless networks

than WPA and WEP standards. It is also available as WPA2-PSK and WPA2-EAP for home and enterprise environment respectively.

Answer B is incorrect.

Answer C and A are incorrect. WPA stands for Wi-Fi Protected Access. It is a wireless security standard. It provides better security

than WEP (Wired Equivalent Protection). Windows Vista supports both WPA-PSK and WPA-EAP. Each of these is described as follows:

WPA-PSK: PSK stands for Preshared key. This standard is meant for home environment. WPA-PSK requires a user to enter an 8-character to 63-character passphrase into a wireless client. The WPA converts the passphrase into a 256-bit key.

WPA-EAP: EAP stands for Extensible Authentication Protocol. This standard relies on a back-end server that runs Remote Authentication Dial-In User Service for user authentication.

Note: Windows Vista supports a user to use a smart card to connect to a WPA-EAP protected network.

Question 7

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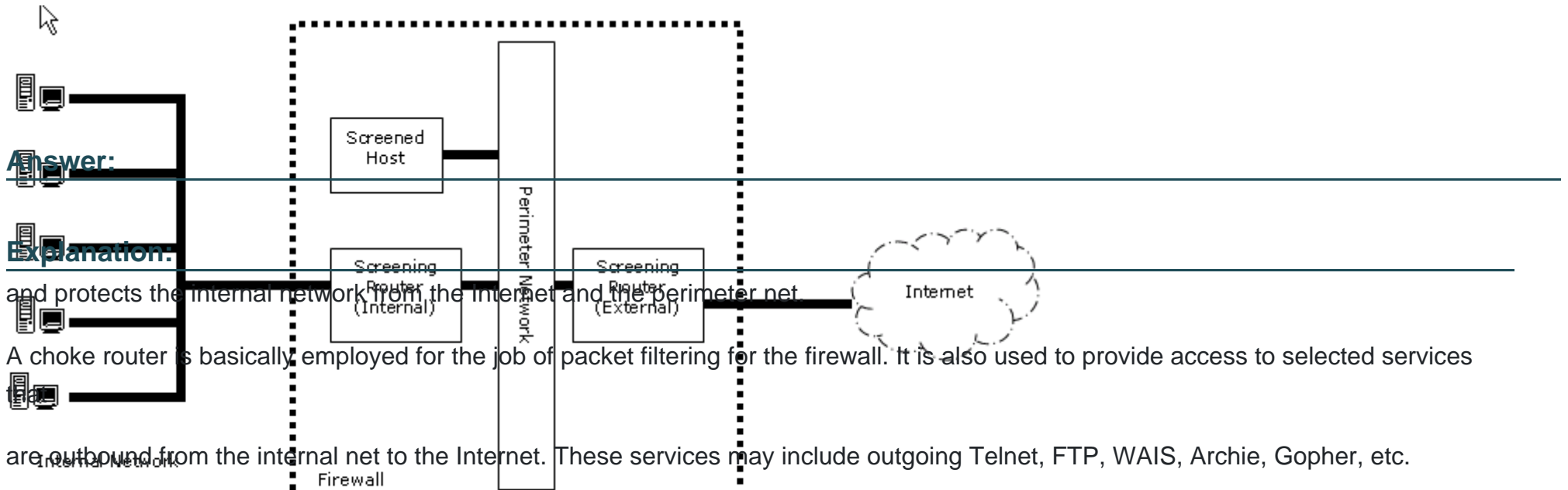
Answer:

Explanation:

and protects the internal network from the Internet and the perimeter net

A choke router is basically employed for the job of packet filtering for the firewall. It is also used to provide access to selected services that
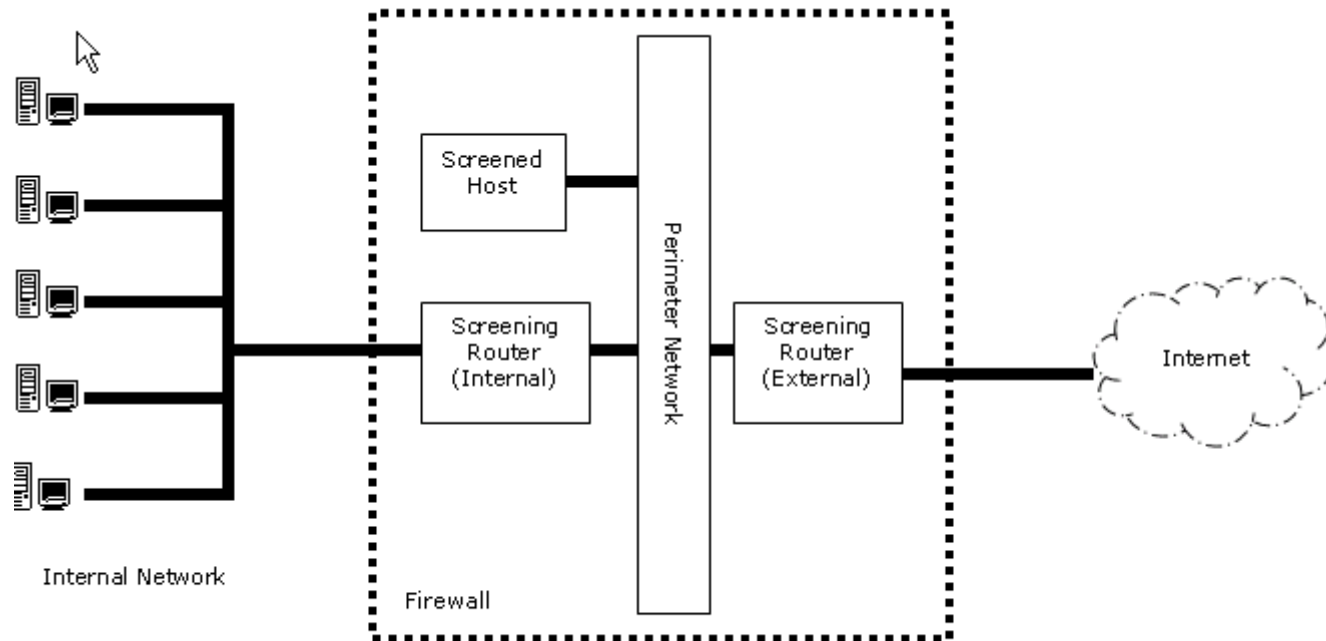
are outbound from the internal net to the Internet. These services may include outgoing Telnet, FTP, WAIS, Archie, Gopher, etc.

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

Screened Host Firewall Architecture

To Get Premium Files for GSNA Visit

https://www.p2pexams.com/products/gsna

For More Free Questions Visit

https://www.p2pexams.com/giac/pdf/gsna

20% DISCOUNT