GNSA$^{\text{Q\&As}}$

GIAC Systems and Network Auditor

Pass GIAC GNSA Exam with 100% Guarantee

QUESTION 1

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

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.

Correct Answer: AD

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.

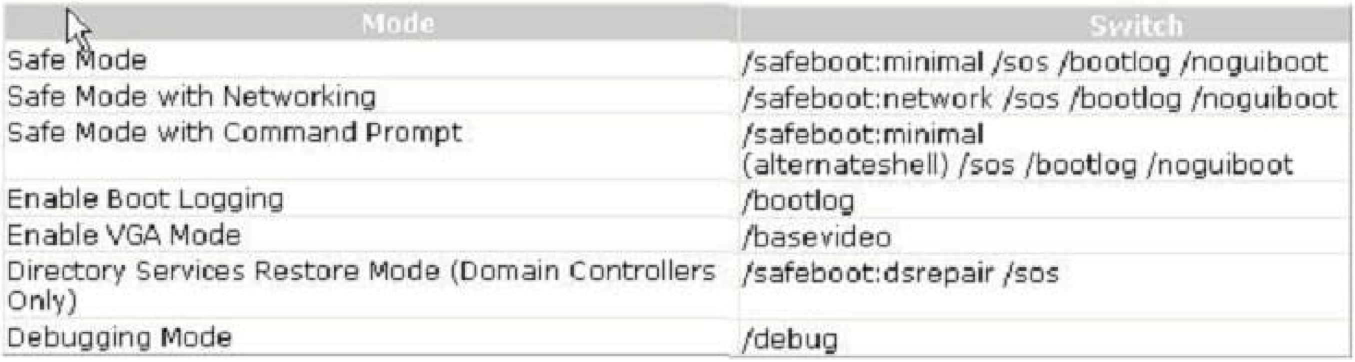
It supports CVE standards.

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.



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 2

Mark works as a project engineer in Tech Perfect Inc. His office is configured with Windows XP-based computers. The computer that he uses is not configured with a default gateway. He is able to access the Internet, but is not able to use email services via the Internet. However, he is able to access e-mail services via the intranet of the company.

Which of the following could be the reason of not being able to access e-mail services via the Internet?

A. Proxy server

B. IP packet filter

C. Router

D. Protocols other than TCP/IP

Correct Answer: A

A proxy server exists between a client\\'s Web-browsing program and a real Internet server. The purpose of the proxy server is to enhance the performance of user requests and filter requests. A proxy server has a database called cache where the most frequently accessed Web pages are stored. The next time such pages are requested, the proxy server is able to suffice the request locally, thereby greatly reducing the access time. Only when a proxy server is unable to fulfill a request locally does it forward the request to a real Internet server. The proxy server can also be used for filtering user requests. This may be done in order to prevent the users from visiting non-genuine sites. Answer: D is incorrect. Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of standard protocols that govern how data passes between networks. It can be used to provide communication between the basic operating systems on local and wide-area networks (WANs). TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). It is considered the primary protocol of the Internet and the World Wide Web. Answer: B is incorrect. IP packet filters allow or block packets from passing through specified ports. They can filter packets based on service type, port number, source computer name, or destination computer name. When packet filtering is enabled, all packets on the external interface are dropped unless they are explicitly allowed, either statically by IP packet filters or dynamically by access policy or publishing rules. Answer: C is incorrect. A router is a device that routes data packets between computers in different networks. It is used to connect multiple networks, and it determines the path to be taken by each data packet to its destination computer. A router maintains a routing table of the available routes and their conditions. By using this information, along with distance and cost algorithms, the router determines the best path to be taken by the data packets to the destination computer. A router can connect dissimilar networks, such as Ethernet, FDDI, and Token Ring, and route data packets among them. Routers operate at the network layer (layer 3) of the Open Systems Interconnection (OSI) model.

QUESTION 3

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You want to configure the ACL with a Cisco router.

Which of the following router prompts can you use to accomplish the task?

A. router(config-if)#

B. router(config)#

C. router(config-ext-nacl)#

D. router#

Correct Answer: C

The auditor of a Cisco router should be familiar with the variety of privilege modes. The current privilege mode can be quickly identified by looking at the current router prompt. The prime modes of a Cisco router are as follows:

#Nonprivileged mode: router>

#Priviledged mode: router#

#Global configuration mode: router(config)#

#Interface configuration mode: router(config-if)#

#ACL configuration mode: router(config-ext-nacl)#

#Boot loader mode: router(boot)

#Remote connectivity config mode: router(config-line)#

QUESTION 4

Which of the following statements about session tracking is true?

A. When using cookies for session tracking, there is no restriction on the name of the session tracking cookie.

B. When using cookies for session tracking, the name of the session tracking cookie must be jsessionid.

C. A server cannot use cookie as the basis for session tracking.

D. A server cannot use URL rewriting as the basis for session tracking.

Correct Answer: B

If you are using cookies for session tracking, the name of the session tracking cookie must be jsessionid. A jsessionid can be placed only inside a cookie header. You can use HTTP cookies to store information about a session. The servlet container takes responsibility of generating the session ID, making a new cookie object, associating the session ID into the cookie, and setting the cookie as part of response.

QUESTION 5

In which of the following scanning techniques does a scanner connect to an FTP server and request that server to start data transfer to the third system?

A. Xmas Tree scanning

B. TCP FIN scanning

C. TCP SYN scanning

D. Bounce attack scanning

Correct Answer: D

In the TCPFTP proxy (bounce attack) scanning, a scanner connects to an FTP server and requests that server to start data transfer to the third system. Now, the scanner uses the PORT FTP command to declare whether or not the data

transfer process is listening to the target system at the certain port number. Then the scanner uses LIST FTP command to list the current directory. This result is sent over the server. If the data transfer is successful, it is clear that the port is

open. If the port is closed, the attacker receives the connection refused ICMP error message.

Answer: A is incorrect. Xmas Tree scanning is just the opposite of null scanning. In Xmas Tree scanning, all packets are turned on. If the target port is open, the service running on the target port discards the packets without any reply.

According to RFC 793, if the port is closed, the remote system replies with the RST packet. Active monitoring of all incoming packets can help system network administrators detect an Xmas Tree scan. Answer: B is incorrect. TCP FIN

scanning is a type of stealth scanning, through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If

the port is open, the FIN packet will be ignored and the port will drop that packet. TCP FIN scanning is useful only for identifying ports of non Windows operating system because Windows operating systems send only RST packets

irrespective of whether the port is open or closed.

Answer: C is incorrect. TCP SYN scanning is also known as half-open scanning because in this a full TCP connection is never opened. The steps of TCP SYN scanning are as follows:

1.The attacker sends SYN packet to the target port.

2.If the port is open, the attacker receives SYN/ACK message.

3.Now the attacker breaks the connection by sending an RST packet.

4.If the RST packet is received, it indicates that the port is closed.

This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.