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

GIAC Systems and Network Auditor

Pass GIAC GSNA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/gsna.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

You are concerned about rogue wireless access points being connected to your network.

What is the best way to detect and prevent these?

A. Network anti-spyware software

B. Network anti-virus software

C. Protocol analyzers

D. Site surveys

Correct Answer: D

Routinely doing site surveys (or better still, having them automatically conducted frequently) is the only way to know what is connected to your network. And it will reveal any rogue access points. Answer: B is incorrect. While antivirus software

is always a good idea, it will do nothing to prevent rogue access points.

Answer: A is incorrect. While anti-spyware software is always a good idea, it will do nothing to prevent rogue access points.

Answer: C is incorrect. A protocol analyzer will help you analyze the specific traffic on a given node, but won\\'t be much help in directly detecting rogue access points.

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 is a type of web site monitoring that is done using web browser emulation or scripted real web browsers?

A. Route analytics

B. Passive monitoring

C. Network tomography

D. Synthetic monitoring

Correct Answer: D

Synthetic monitoring is an active Web site monitoring that is done using Web browser emulation or scripted real Web browsers. Behavioral scripts (or paths) are created to simulate an action or path that a customer or end-user would take on a site. Those paths are then continuously monitored at specified intervals for availability and response time measures. Synthetic monitoring is valuable because it enables a Webmaster to identify problems and determine if his Web site or Web application is slow or experiencing downtime before that problem affects actual end-users or customers. Answer: B is incorrect. Passive monitoring is a technique used to analyze network traffic by capturing traffic from a network by generating a copy of that traffic. It is done with the help of a span port, mirror port, or network tap. Once the data (a stream of frames or packets) has been extracted, it can be used in many ways. Passive monitoring can be very helpful in troubleshooting performance problems once they have occurred. Passive monitoring relies on actual inbound Web traffic to take measurements, so problems can only be discovered after they have occurred. Answer: A is incorrect. Route analytics is an emerging network monitoring technology specifically developed to analyze the routing protocols and structures in meshed IP networks. Their main mode of operation is to passively listen to the Layer 3 routing protocol exchanges between routers for the purposes of network discovery, mapping, real-time monitoring, and routing diagnostics. Answer: C is incorrect. Network tomography is an important area of network measurement that deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/Internet.

QUESTION 4

Which of the following statements are true about locating rogue access points using WLAN discovery software such as NetStumbler, Kismet, or MacStumbler if you are using a Laptop integrated with Wi-Fi compliant MiniPCI card? (Choose two)

A. These tools can determine the rogue access point even when it is attached to a wired network.

B. These tools can determine the authorization status of an access point.

C. These tools cannot detect rogue access points if the victim is using data encryption.

D. These tools detect rogue access points if the victim is using IEEE 802.11 frequency bands.

Correct Answer: BD

WLAN discovery software such as NetStumbler, Kismet, or MacStumbler can be used to detect rogue access points if the victim is using IEEE 802 frequency bands. However, if the victim is using non-IEEE 802.11 frequency bands or

unpopular modulations, these tools might not detect rogue access. NetStumbler, kismet, or MacStumbler also gives the authorization status of an access point. A Rogue access point (AP) is set up by the attackers in an Enterprise\\'s network.

The attacker captures packets in the existing wireless LAN (WLAN) and finds the SSID and security keys (by cracking). Then the attacker sets up his own AP using the same SSID and security keys. The network clients unknowingly use this

AP and the attacker captures their usernames and passwords. This can help the attacker to intrude the security and have access to the Enterprise data.

Answer: A, C are incorrect. The WLAN software such as NetStumbler, Kismet, or MacStumbler can search rogue access points even when the victim is using data encryption. However, these tools cannot determine the rogue access point

even when it is attached to a wired network.

QUESTION 5

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You are concerned about the vulnerabilities existing in the network of the company.

Which of the following can be a cause for making the network vulnerable? (Choose two)

A. Use of well-known code

B. Use of uncommon code

C. Use of uncommon software

D. Use of more physical connections

Correct Answer: AD

In computer security, the term vulnerability is a weakness which allows an attacker to reduce a system\\'s Information Assurance. A computer or a network can be vulnerable due to the following reasons:

Complexity: Large, complex systems increase the probability of flaws and unintended access points. Familiarity: Using common, well-known code, software, operating systems, and/or hardware increases the probability an attacker has or can

find the knowledge and tools to exploit the flaw. Connectivity: More physical connections, privileges, ports, protocols, and services and time each of those are accessible increase vulnerability.

Password management flaws: The computer user uses weak passwords that could be discovered by brute force. The computer user stores the password on the computer where a program can access it. Users re- use passwords between

many programs and websites.

Fundamental operating system design flaws: The operating system designer chooses to enforce sub optimal policies on user/program management. For example, operating systems with policies such as default permit grant every program

and every user full access to the entire computer. This operating system flaw allows viruses and malware to execute commands on behalf of the administrator. Internet Website Browsing: Some Internet websites may contain harmful Spyware

or Adware that can be installed automatically on the computer systems. After visiting those websites, the computer systems become infected and personal information will be collected and passed on to third party individuals. Software bugs:

The programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.

Unchecked user input: The program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands or SQL statements (known as Buffer overflows, SQL injection or other non-

validated inputs).

Answers B, C are incorrect. Use of common software and common code can make a network vulnerable.