GSNA 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.leads4pass.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

eBox Platform is an open source unified network server (or a Unified Network Platform) for SMEs. In which of the following forms can eBox Platform be used?

A. Unified Communications Server

B. Network Infrastructure Manager

C. Gateway

D. Sandbox

Correct Answer: ABC

eBox Platform is an open source unified network server (or a Unified Network Platform) for SMEs. eBoxPlatform can act as a Gateway, Network Infrastructure Manager, Unified Threat Manager, Office Server, Unified Communications Server or a combination of them. Besides, eBox Platform includes a development framework to ease the development of new Unix-based services. Answer: D is incorrect. eBox Platform cannot act as a sandbox. A sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs, from unverified third-parties, suppliers, and untrusted users.

QUESTION 2

You work as a Network Administrator for Infonet Inc. The company\\'s network has an FTP server. You want to secure the server so that only authorized users can access it.

What will you do to accomplish this?

A. Disable anonymous authentication.

B. Stop the FTP service on the server.

C. Disable the network adapter on the server.

D. Enable anonymous authentication.

Correct Answer: A

You will have to disable anonymous authentication. This will prevent unauthorized users from accessing the FTP server. Anonymous authentication (anonymous access) is a method of authentication for Websites. Using this method, a user can establish a Web connection to the IIS server without providing a username and password. Hence, this is an insecure method of authentication. This method is generally used to permit unknown users to access the Web or FTP server directories. Answer: D is incorrect. Enabling anonymous authentication will allow all the users to access the server. Answer: B is incorrect. Stopping the FTP service on the server will prevent all the users from accessing the FTP server. Answer: C is incorrect. Disabling the network adapter on the FTP server will disconnect the server from the network.

QUESTION 3

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.

Correct Answer: BCD

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.

Answer: A is incorrect. Security risks can never be removed completely but can be mitigated by taking proper actions.

QUESTION 4

Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system.

Which of the following are the most likely threats to his computer? (Choose two)

A. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.

B. Attacker can use the Ping Flood DoS attack if WZC is used.

C. Attacker by creating a fake wireless network with high power antenna cause Victor\\'s computer to associate with his network to gain access.

D. It will not allow the configuration of encryption and MAC filtering. Sending information is not secure on wireless network.

Correct Answer: AC

Wireless Zero Configuration (WZC), also known as Wireless Auto Configuration, or WLAN AutoConfig is a wireless connection management utility included with Microsoft Windows XP and later operating systems as a service that dynamically selects a wireless network to connect to based on a user\\'s preferences and various default settings. This can be used instead of, or in the absence of, a wireless network utility from the manufacturer of a computer\\'s wireless networking device. The drivers for the wireless adapter query the NDIS Object IDs and pass the available network names to the service. WZC also introduce some security threats, which are as follows: WZC will probe for networks that are already connected. This information can be viewed by anyone using a wireless analyzer and can be used to set up fake access points to connect. WZC attempts to connect to the wireless network with the strongest signal. Attacker can create fake wireless networks with high- power antennas and cause computers to associate with his access point. Answer: D is incorrect. WZC does not interfere in the configuration of encryption and MAC filtering. Answer: B is incorrect. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs.

QUESTION 5

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.