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.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 work as a Network Administrator for XYZ CORP. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company\\'s management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks: The wireless network communication should be secured. The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps: Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication.

What will happen after you have taken these steps?

A. Both tasks will be accomplished.

B. The laptop users will be able to use smart cards for getting authenticated.

C. The wireless network communication will be secured.

D. None of the tasks will be accomplished.

Correct Answer: C

As 802.1xand WEP are configured, this step will enable the secure wireless network communication. For authentication, you have configured the PEAP-MS-CHAP v2 protocol. This protocol can be used for authentication on wireless networks, but it cannot use a public key infrastructure (PKI). No certificate can be issued without a PKI. Smart cards cannot be used for authentication without certificates. Hence, the laptop users will not be able to use smart cards for getting authenticated.

QUESTION 2

Which of the following responsibilities does not come under the audit process?

A. Reporting all facts and circumstances of their regular and illegal acts.

B. Planning the IT audit engagement based on the assessed level of risk.

C. Reviewing the results of the audit procedures.

D. Applying security policies.

Correct Answer: ABC

According to the standards of ISACA, an auditor should hold the following responsibilities: Planning the IT audit engagement based on an assessed level of risk. Designing audit procedures of irregular and illegal acts. Reviewing the results of the audit procedures. Assuming that acts are not isolated. Determining why the internal control system failed for that act. Conducting additional audit procedures. Evaluating the results of the expanded audit procedures. Reporting all facts and circumstances of the irregular and illegal acts. Distributing the report to the appropriate internal parties, such as managers. Answer: D is incorrect. The auditor is not responsible for applying security policies.

QUESTION 3

You are concerned about attackers simply passing by your office, discovering your wireless network, and getting into your network via the wireless connection.

Which of the following are NOT steps in securing your wireless connection? (Choose two.)

A. Hardening the server OS

B. Using either WEP or WPA encryption

C. MAC filtering on the router

D. Strong password policies on workstations.

E. Not broadcasting SSID

Correct Answer: AD

Both hardening the server OS and using strong password policies on workstations are good ideas, but neither has anything to do with securing your wireless connection. Answer: B is incorrect. Using WEP or WPA is one of the most basic security steps in securing your wireless.

QUESTION 4

You work as a Web Deployer for UcTech Inc. You write the element for an application in which you write the sub-element as follows: * Who will have access to the application?

A. Only the administrator

B. No user

C. All users

D. It depends on the application.

Correct Answer: C

The element is a sub-element of the element. It defines the roles that are allowed to access the Web resources specified by the sub-elements. The element

is written in the deployment descriptor as follows:

---------- Administrator Writing Administrator within the

element will allow only the administrator to have access to the resource defined within the element.

QUESTION 5

Which of the following internal control components provides the foundation for the other components and encompasses such factors as management\\'s philosophy and operating style?

A. Information and communication

B. Risk assessment

C. Control activities

D. Control environment

Correct Answer: D

COSO defines internal control as, "a process, influenced by an entity\\'s board of directors, management, and other personnel, that is designed to provide reasonable assurance in the effectiveness and efficiency of operations, reliability of financial reporting, and the compliance of applicable laws and regulations". The auditor evaluates the organization\\'s control structure by understanding the organization\\'s five interrelated control components, which are as follows:

1.

Control Environment: It provides the foundation for the other components and encompasses such factors as management\\'s philosophy and operating style.

2.

Risk Assessment: It consists of risk identification and analysis.

3.

Control Activities: It consists of the policies and procedures that ensure employees carry out management\\'s directions.

The types of control activities an organization must implement are preventative controls (controls intended to stop an error from occurring), detective controls (controls intended to detect if an error has occurred), and mitigating controls (control

activities that can mitigate the risks associated with a key control not operating effectively).

4.

Information and Communication: It ensures the organization obtains pertinent information, and then communicates it throughout the organization.

5.

Monitoring: It involves reviewing the output generated by control activities and conducting special evaluations. In addition to understanding the organization\\'s control components, the auditor must also evaluate the organization\\'s General

and Application controls. There are three audit risk components:

control risk, detection risk, and inherent risk.