GNSA Q&As

GIAC Systems and Network Auditor

Pass GIAC GNSA Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

Which of the following methods is used to get a cookie from a client?

Note: Here, request is a reference of type HttpServletRequest, and response is a reference of type HttpServletResponse.

A. Cookie [] cookies = request.getCookies();

B. Cookie [] cookies = request.getCookie(String str)

C. Cookie [] cookies = response.getCookie(String str)

D. Cookie[] cookies = response.getCookies()

Correct Answer: A

The getCookies() method of the HttpServletRequest interface is used to get the cookies from a client. This method returns an array of cookies.

Answer: B, C are incorrect. The getCookie(String str)method does not exist.

Answer: D is incorrect. The getCookies() method is present in the HttpServletRequest interface and not in the HttpServletResponse interface.

QUESTION 2

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities.

Which of the following vulnerabilities can be fixed using Nessus?

A. Vulnerabilities that allow a remote cracker to control sensitive data on a system

B. Misconfiguration (e.g. open mail relay, missing patches, etc.)

C. Vulnerabilities that allow a remote cracker to access sensitive data on a system

D. Vulnerabilities that help in Code injection attacks

Correct Answer: ABC

Nessus is a proprietary comprehensive vulnerability scanning program. It is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on the tested systems. For example: Vulnerabilities that allow a remote cracker to control or access sensitive data on a system. Misconfiguration (e.g. open mail relay, missing patches, etc). Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack. Denials of service against the TCP/IP stack by using mangled packets. On UNIX (including Mac OS X), it consists of nessusd, the Nessus daemon, which does the scanning, and nessus, the client, which controls scans and presents the vulnerability results to the user. For Windows, Nessus 3 installs as an executable and has a self-contained scanning, reporting, and management system. Operations: In typical operation, Nessus begins by doing a port scan with one of its four internal portscanners (or it can optionally use Amap or Nmap) to determine which ports are open on the target and then tries various exploits

on the open ports. The vulnerability tests, available as subscriptions, are written in NASL (Nessus Attack Scripting Language), a scripting language optimized for custom network interaction. Tenable Network Security produces several dozen new vulnerability checks (called plugins) each week, usually on a daily basis. These checks are available for free to the general public; commercial customers are not allowed to use this Home Feed any more. The Professional Feed (which is not free) also gives access to support and additional scripts (audit and compliance tests). Optionally, the results of the scan can be reported in various formats, such as plain text, XML, HTML, and LaTeX. The results can also be saved in a knowledge base for debugging. On UNIX, scanning can be automated through the use of a command-line client. There exist many different commercial, free and open source tools for both UNIX and Windows to manage individual or distributed Nessus scanners. If the user chooses to do so (by disabling the option\\' safe checks\\'), some of Nessus\\'s vulnerability tests may try to cause vulnerable services or operating systems to crash. This lets a user test the resistance of a device before putting it in production. Nessus provides additional functionality beyond testing for known network vulnerabilities. For instance, it can use Windows credentials to examine patch levels on computers running the Windows operating system, and can perform password auditing using dictionary and brute force methods. Nessus 3 and later can also audit systems to make sure they have been configured per a specific policy, such as the NSA\\'s guide for hardening Windows servers. Answer: D is incorrect. Nessus cannot be used to scan vulnerabilities that help in Code injection attacks.

QUESTION 3

In an IT organization, some specific tasks require additional detailed controls to ensure that the workers perform their job correctly.

What do these detailed controls specify? (Choose three)

A. How the department handles acquisitions, security, delivery, implementation, and support of IS services

B. How to lock a user account after unsuccessful logon attempts

C. How output data is verified before being accepted into an application

D. The way system security parameters are set

Correct Answer: ABD

Some of the specific tasks require additional detailed controls to ensure that the workers perform their job correctly. These controls refer to some specific tasks or steps to be performed such as:

The way system security parameters are set.

How input data is verified before being accepted into an application.

How to lock a user account after unsuccessful logon attempts.

How the department handles acquisitions, security, delivery, implementation, and support of IS services.

Answer: C is incorrect. Input data should be verified before being accepted into an application.

QUESTION 4

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 5

Which of the following statements are true about a data mart? Each correct answer represents a complete solution.

A. Most writers believe that the design of a data mart tends to start from an analysis of the data already existing.

B. Users of a data mart can expect to have data presented in terms that are familiar to them.

C. A data mart is a repository of data gathered from operational data.

D. The emphasis of a data mart is on meeting the specific demands of a particular group of knowledge users.

Correct Answer: BCD

A data mart is a repository of data gathered from operational data and other sources that is designed to serve a particular community of knowledge workers. In scope, the data may derive from an enterprise-wide database or data warehouse or be more specialized. The emphasis of a data mart is on meeting the specific demands of a particular group of knowledge users in terms of analysis, content, presentation, and ease-of-use. Users of a data mart can expect to have data presented in terms that are familiar. In practice, the terms data mart and data warehouse each tend to imply the presence of the other in some form. However, most writers using the term seem to agree that the design of a data mart tends to start from an analysis of user needs and that a data warehouse tends to start from an analysis of what data already exists and how it can be collected in such a way that the data can later be used. A data warehouse is a central aggregation of data (which can be distributed physically); a data mart is a data repository that may derive from a data warehouse or not and that emphasizes ease of access and usability for a particular designed purpose. In general, a data warehouse tends to be a strategic but somewhat unfinished concept; a data mart tends to be tactical and aimed at meeting an immediate need. Answer: A is incorrect. Writers using a data mart believe that the design of a data mart tends to start from an analysis of user needs.

Latest GNSA Dumps GNSA Study Guide GNSA Exam Questions