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.passapply.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 Tech Perfect Inc. The company has a TCP/IP based switched network. A root bridge has been elected in the switched network. You have installed a new switch with a lower bridge ID than the existing root bridge.

What will happen?

A. The new switch starts advertising itself as the rootbridge.

B. The new switch divides the network into two broadcast domains.

C. The new switch works as DR or BDR.

D. The new switch blocks all advertisements.

Correct Answer: A

The new switch starts advertising itself as the root bridge. It acts as it is the only bridge on the network. It has a lower Bridge ID than the existing root, so it is elected as the root bridge after the BPDUs converge and when all switches know about the new switch that it is the better choice. Answer: B, C, D are incorrect. All these are not valid options, according to the given scenario.

QUESTION 2

Which of the following statements are true about data aggregation?

A. A common aggregation purpose is to get more information about particular groups based on specific variables.

B. Data aggregation cannot be user-based.

C. Data aggregation is any process in which information is gathered and expressed in a summary form.

D. Online analytic processing (OLAP) is a simple type of data aggregation.

Correct Answer: ACD

Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. A common aggregation purpose is to get more information about particular groups based on specific variables such as age, profession, or income. The information about such groups can then be used for Web site personalization to choose content and advertising likely to appeal to an individual belonging to one or more groups for which data has been collected. For example, a site that sells music CDs might advertise certain CDs based on the age of the user and the data aggregate for their age group. Online analytic processing (OLAP) is a simple type of data aggregation in which the marketer uses an online reporting mechanism to process the information. Answer: B is incorrect. Data aggregation can be user-based. Personal data aggregation services offer the user a single point for collection of their personal information from other Web sites. The customer uses a single master personal identification number (PIN) to give them access to their various accounts (such as those for financial institutions, airlines, book and music clubs, and so on). Performing this type of data aggregation is sometimes referred to as "screen scraping."

QUESTION 3

Which of the following commands can you use to search a string \\'pwd\\' in all text files without opening them? (Choose two)

A. vi

B. grep

C. sed

D. locate

Correct Answer: BC

sed and grep are the two commands that can be used to search a specified string in all text files without opening them. sed is a stream editor that is used to perform basic text transformations on an input stream (a file or input from a pipeline).

QUESTION 4

You work as a Network Administrator for Tech Perfect Inc. The company requires a secure wireless network. To provide security, you are configuring ISA Server 2006 as a firewall.

While configuring ISA Server 2006, which of the following is NOT necessary?

A. Setting up of monitoring on ISA Server

B. Defining how ISA Server would cache Web contents

C. Defining ISA Server network configuration

D. Configuration of VPN access

Correct Answer: D

Configuration of VPN access is not mandatory. It is configured on the basis of requirement. Answer: A, B, C are incorrect. All these steps are mandatory for the configuration of the ISA Server 2006 firewall.

QUESTION 5

What is the purpose of Cellpadding attribute of tag?

A. Cellpadding is used to set the width of cell border and its content.

B. Cellpadding is used to set the width of a table.

C. Cellpadding is used to set the space between the cell border and its content.

D. Cellpadding is used to set the space between two cells in a table.

Correct Answer: C

Cellpadding attribute is used to set the space, in pixels, between the cell border and its content. If you have not set the value of Cellpadding attribute for a table, the browser takes the default value as 1.

QUESTION 6

You work as a Software Developer for UcTech Inc. You build an online book shop, so that users can purchase books using their credit cards. You want to ensure that only the administrator can access the credit card information sent by users.

Which security mechanism will you use to accomplish the task?

A. Confidentiality

B. Dataintegrity

C. Authentication

D. Authorization

Correct Answer: A

Confidentiality is a mechanism that ensures that only the intended authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it.

Answer: D is incorrect. Authorization is a process that verifies whether a user has permission to access a Web resource. A Web server can restrict access to some of its resources to only those clients that log in using a recognized username

and password. To be authorized, a user must first be authenticated. Answer: C is incorrect. Authentication is the process of verifying the identity of a user. This is usually done using a user name and password. This process compares the

provided user name and password with those stored in the database of an authentication server.

Answer: B is incorrect. Data integrity is a mechanism that ensures that the data is not modified during transmission from source to destination. This means that the data received at the destination should be exactly the same as that sent from

the source.

QUESTION 7

Which of the following backup sites takes the longest recovery time?

A. Mobile backup site

B. Warm site

C. Cold site

D. Hot site

Correct Answer: C

A cold backup site takes the longest recovery time. It is the most inexpensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware contributes to the minimal startup costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the

disaster. Answer: D is incorrect. A hot site is a duplicate of the original site of the organization, with full computer systems as well as near- complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Ideally, a hot site will be up and running within a matter of hours or even less. Answer: A is incorrect. Although a mobile backup site provides rapid recovery, it does not provide full recovery in time. Hence, a hot site takes the shortest recovery time. Answer: B is incorrect. A warm site is, quite logically, a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

QUESTION 8

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 9

You work as a Network Administrator for XYZ CORP. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest network. You configure a new Windows

Server 2008 server in the network. The new server is not yet linked to Active Directory. You are required to accomplish the following tasks:

Add a new group named "Sales".

Copy the "Returns" group from the older server to the new one.

Rename the "Returns" group to "Revenue".

View all group members, including for multiple groups/entire domain. You use Hyena to simplify and centralize all of these tasks.

Which of the assigned tasks will you be able to accomplish?

A. Copy the "Returns" group to the new server.

B. Rename the "Returns" group to "Revenue".

C. Add the new group named "Sales".

D. View and manage all group members, including for multiplegroups/entire domain.

Correct Answer: ABC

Hyena supports the following group management functions: Full group administration such as add, modify, delete, and copy Rename groups Copy groups from one computer to another View both direct and indirect (nested) group members for one or more groups [only for Active Directory] View all group members, including for multiple groups/entire domain [only for Active Directory] Answer: D is incorrect. All group members can neither be viewed nor managed until the new server is linked to Active Directory.

QUESTION 10

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 11

Which of the following attacks allows the bypassing of access control lists on servers or routers, and helps an attacker to hide? (Choose two)

A. DNS cache poisoning

B. DDoS attack

C. IP spoofing attack

D. MAC spoofing

Correct Answer: CD

Either IP spoofing or MAC spoofing attacks can be performed to hide the identity in the network. MAC spoofing is a hacking technique of changing an assigned Media Access Control (MAC) address of a networked device to a different

one. The changing of the assigned MAC address may allow the bypassing of access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer. MAC spoofing is the activity of altering the MAC address of a network card. Answer: A is incorrect. DNS cache poisoning is a maliciously created or unintended situation that provides data to a caching name server that did not originate from authoritative Domain Name System (DNS) sources. Once a DNS server has received such non-authentic data, Caches it for future performance increase, it is considered poisoned, supplying the non-authentic data to the clients of the server. To perform a cache poisoning attack, the attacker exploits a flaw in the DNS software. If the server does not correctly validate DNS responses to ensure that they are from an authoritative source, the server will end up caching the incorrect entries locally and serve them to other users that make the same request. Answer: B is incorrect. In a distributed denial of service (DDOS) attack, an attacker uses multiple computers throughout the network that has been previously infected. Such computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. TFN, TRIN00, etc. are tools used for a DDoS attack.

QUESTION 12

Which of the following statements are true about SSIDs?

A. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict.

B. SSIDs are case insensitive text strings and have a maximum length of 64 characters.

C. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.

D. SSID is used to identify a wireless network.

Correct Answer: ACD

SSID stands for Service SetIdentifier. It is used to identify a wireless network. SSIDs are case sensitive text strings and have a maximum length of 32 characters. All wireless devices on a wireless network must have the same SSID in order to communicate with each other. The SSID on computers and the devices in WLAN can be set manually and automatically. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict. A network administrator often uses a public SSID that is set on the access point. The access point broadcasts SSID to all wireless devices within its range. Some newer wireless access points have the ability to disable the automatic SSID broadcast feature in order to improve network security.

QUESTION 13

Which of the following applications work as mass-emailing worms? (Choose two.)

A. Chernobyl virus

B. I LOVE YOU virus

C. Nimda virus

D. Melissa virus

Correct Answer: BC

The Nimda and I LOVE YOU viruses work as mass-emailing worms.

QUESTION 14

You work as a Java Programmer for JavaSkills Inc. You are working with the Linux operating system. Nowadays, when you start your computer, you notice that your OS is taking more time to boot than usual. You discuss this with your Network Administrator. He suggests that you mail him your Linux bootup report.

Which of the following commands will you use to create the Linux bootup report?

A. touch bootup_report.txt

B. dmesg > bootup_report.txt

C. dmesg | wc

D. man touch

Correct Answer: B

According to the scenario, you can use dmesg > bootup_report.txt to create the bootup file. With this command, the bootup messages will be displayed and will be redirected towards bootup_report.txt using the > command.

QUESTION 15

You work as an IT Technician for XYZ CORP. You have to take security measures for the wireless network of the company. You want to prevent other computers from accessing the company\\'s wireless network. On the basis of the hardware address, which of the following will you use as the best possible method to accomplish the task?

A. RAS

B. MAC Filtering

C. SSID

D. WEP

Correct Answer: B

MAC filtering is a security access control technique that allows specific network devices to access, or prevents them from accessing, the network. MAC filtering can also be used on a wireless network to prevent certain network devices from accessing the wireless network. MAC addresses are allocated only to hardware devices, not to persons.