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.leads4pass.com/gnsa.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The SALES folder has a file named XFILE.DOC that contains critical information about your company. This folder resides on an NTFS volume. The company\\'s Senior Sales Manager asks you to provide security for that file. You make a backup of that file and keep it in a locked cupboard, and then you deny access on the file for the Sales group. John, a member of the Sales group, accidentally deletes that file. You have verified that John is not a member of any other group. Although you restore the file from backup, you are confused how John was able to delete the file despite having no access to that file. What is the most likely cause?

A. The Sales group has the Full Control permission on the SALES folder.

B. The DenyAccess permission does not restrict the deletion of files.

C. John is a member of another group having the Full Control permission on that file.

D. The Deny Access permission does not work on files.

Correct Answer: A

Although NTFS provides access controls to individual files and folders, users can perform certain actions even if permissions are set on a file or folder to prevent access. If a user has been denied access to any file and he has Full Control

rights in the folder on which it resides, he will be able to delete the file, as Full Control rights in the folder allow the user to delete the contents of the folder. Answer: C is incorrect. In the event of any permission conflict, the most restrictive one

prevails. Moreover, the question clearly states that John is not a member of any other group.

Answer: B, D are incorrect. The Deny Access permission works on files.

QUESTION 2

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 3

Which of the following types of audit constructs a risk profile for existing and new projects?

A. Technologicalposition audit

B. Technological innovation process audit

C. Innovative comparison audit

D. Client/Server, Telecommunications, Intranets, and Extranets audits

Correct Answer: B

Various authorities have created differing taxonomies to distinguish the various types of IT audits. Goodman and Lawless state that there are three specific systematic approaches to carry out an IT audit:

Technological innovation process audit: This audit constructs a risk profile for existing and new projects. The audit will assess the length and depth of the company\\'s experience in its chosen technologies, as well as its presence in relevant

markets, the organization of each project, and the structure of the portion of the industry that deals with this project or product, organization and industry structure.

Innovative comparison audit: This audit is an analysis of the innovative abilities of the company being audited in comparison to its competitors. This requires examination of company\\'s research and development facilities, as well as its track

record in actually producing new products.

Technological position audit: This audit reviews the technologies that the business currently has and that it needs to add. Technologies are characterized as being either "base", "key", "pacing", or "emerging".

Answer: D is incorrect. These are the audits to verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

QUESTION 4

Which of the following are known as safety critical software?

A. Software that is used to apply a critical decision-making process

B. Software that manages safety critical data including display of safety critical information

C. Software that intervenes when a safe condition is present or is about to happen

D. Software that is used to create safety critical functions

Correct Answer: AB

The following types of software are safety critical software: Software that is used to apply a critical decision-making process Software that is used to manage or monitor safety critical functions Software that intervenes when an unsafe condition is present or is about to happen Software that executes on the same target system as safety critical software Software that impacts the systems on which safety critical software runs Software that manages safety critical data including display of safety critical information Software that is used to validate and verify safety critical software Answer: D is incorrect. Software that is used to manage or monitor safety critical functions is known as safety critical software. Answer: C is incorrect. Software that intervenes when an unsafe condition is present or is about to happen is known as safety critical software.

QUESTION 5

You work as a Database Administrator for XYZ CORP. The company has a multi-platform network. The company requires fast processing of the data in the database of the company so that answers to queries can be generated quickly. To provide fast processing, you have a conceptual idea of representing the dimensions of data available to a user in the data cube format.

Which of the following systems can you use to implement your idea?

A. SYSDBA

B. MDDBMS

C. Federated database system

D. Hierarchical database system

Correct Answer: B

A multidimensional database management system (MDDBMS) implies the ability to rapidly process the data in the database so that answers to the queries can be generated quickly. A number of vendors provide products that use multidimensional databases. The approach behind this system is to manage that how data should be stored in the database, and depending upon that storage, how user interface should vary. Conceptually, an MDDBMS uses the idea of a data cube to represent the dimensions of data available to a user. For example, "sales" could be viewed in the dimensions of product model, geography, time, or some additional dimension. In this case, "sales" is known as the measure attribute of the data cube and the other dimensions are seen as feature attributes. Additionally, a database creator can define hierarchies and levels within a dimension (for example, state and city levels within a regional hierarchy). Answer: C is incorrect. A federated database system is a type of meta-database management system (DBMS) that transparently integrates multiple autonomous database systems into a single federated database. The constituent databases are interconnected via a computer network, and may be geographically decentralized. Since the constituent database systems remain autonomous, a federated database system is a contrastable alternative to the (sometimes daunting) task of merging together several disparate databases. A federated database (or virtual database) is the fully-integrated, logical composite of all constituent databases in a federated database system. Answer: A is incorrect. SYSDBA is a system privilege that allows a user to perform basic database administrative tasks, such as creating a database, altering a database, starting up and shutting down an Oracle instance, performing time- based recovery etc. The SYSDBA contains all system privileges with the ADMIN OPTION. It also contains the SYSOPER system privilege. Granting the SYSDBA system privilege to a user automatically adds him to the password file that is used to authenticate administrative users. Therefore, a user possessing the SYSDBA system privilege can connect to a database by using the password file authentication method. Answer: D is incorrect. A hierarchical database is a database management system that implements the hierarchical data model. A hierarchical database system organizes data in a family tree structure such that each record has only one owner and the hierarchy is in a parent and child data segment. This implies that the record can have repeated information in a child segment. The best-known hierarchical DBMS is IMS.

QUESTION 6

An executive in your company reports odd behavior on her PDA. After investigation you discover that a trusted device is actually copying data off the PDA. The executive tells you that the behavior started shortly after accepting an e-business card from an unknown person.

What type of attack is this?

A. Session Hijacking

B. Bluesnarfing

C. Privilege Escalation

D. PDA Hijacking

Correct Answer: B

Bluesnarfing is a rare attack in which an attacker takes control of a bluetooth enabled device. One way to do this is to get your PDA to accept the attacker\\'s device as a trusted device.

QUESTION 7

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You want to use multiple security countermeasures to protect the integrity of the information assets of the company. To accomplish the task,

you need to create a complex and multi-layered defense system.

Which of the following components can be used as a layer that constitutes \\'Defense in depth\\'? (Choose three)

A. Backdoor

B. Firewall

C. Antivirus software

D. Intrusion detection

Correct Answer: BCD

The components of Defense in depth include antivirus software, firewalls, anti-spyware programs, hierarchical passwords, intrusion detection, and biometric verification. In addition to electronic countermeasures, physical protection of business sites along with comprehensive and ongoing personnel training enhances the security of vital data against compromise, theft, or destruction. Answer A is incorrect. A backdoor is any program that allows a hacker to connect to a computer without going through the normal authentication process. The main advantage of this type of attack is that the network traffic moves from inside a network to the hacker\\'s computer. The traffic moving from inside a network to the outside world is typically the least restrictive, as companies are more concerned about what comes into a network, rather than what leaves it. It, therefore, becomes hard to detect backdoors.

QUESTION 8

You work as the Network Technician for XYZ CORP. The company has a Linux-based network. You are working on the Red Hat operating system. You want to view only the last 4 lines of a file named /var/log/cron.

Which of the following commands should you use to accomplish the task?

A. tail -n 4 /var/log/cron

B. tail /var/log/cron

C. cat /var/log/cron

D. head /var/log/cron

Correct Answer: A

The tail -n 4 /var/log/cron command will show the last four lines of the file /var/log/cron.

QUESTION 9

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to allow direct access to the filesystems data structure.

Which of the following Unix commands can you use to accomplish the task?

A. debugfs

B. dosfsck

C. du

D. df

Correct Answer: A

In Unix, the debugfs command is used to allowdirect access to the filesystems data structure.

Answer: D is incorrect. In Unix, the df command shows the disk free space on one or more filesystems.

Answer: B is incorrect. In Unix, the dosfsck command checks and repairs MS-Dos filesystems.

Answer: C isincorrect. In Unix, the du command shows how much disk space a directory and all its files contain.

QUESTION 10

You are the Network Administrator for a company. You have decided to conduct a user access and rights review.

Which of the following would be checked during such a review? (Choose three)

A. Access Control Lists

B. Encryption Methods

C. User Roles

D. Firewalls

E. Group Membership

Correct Answer: ACE

A user access and rights review must check all users, what groups they belong to, what roles they have, and what access they have. Furthermore, such a review should also check logs to see if users are appropriately utilizing their system rights and privileges.

QUESTION 11

You are concerned about rootkits on your network communicating with attackers outside your network.

Without using an IDS how can you detect this sort of activity?

A. By setting up a DMZ.

B. You cannot, you need an IDS.

C. By examining your domain controller server logs.

D. By examining your firewall logs.

Correct Answer: D

Firewall logs will show all incoming and outgoing traffic. By examining those logs you can detect anomalous traffic, which can indicate the presence of malicious code such as rootkits.

Answer: B is incorrect. While an IDS might be the most obvious solution in this scenario, it is not the only one.

Answer: C is incorrect. It is very unlikely that anything in your domain controller logs will show the presence of a rootkit, unless that rootkit is on the domain controller itself.

Answer A is incorrect. A DMZ is an excellent firewall configuration but will not aid in detecting rootkits.

QUESTION 12

The tool works under Windows 9x/2000. Which of the following tools can be used to automate the MITM attack?

A. Airjack

B. Kismet

C. Hotspotter

D. IKECrack

Correct Answer: A

Airjack is a collection of wireless card drivers and related programs. It uses a program called monkey_jack that is used to automate the MITM attack. Wlan_jack is a DoS tool in the set of airjack tools, which accepts a target source and BSSID to send continuous deauthenticate frames to a single client or an entire network. Another tool, essid_jack is used

to send a disassociate frame to a target client in order to force the client to reassociate with the network and giving up the network SSID. Answer: C is incorrect. Hotspotter is a wireless hacking tool that is used to detect rogue access point. It fools users to connect, and authenticate with the hacker\\'s tool. It sends the deauthenticate frame to the victim\\'s computer that causes the victim\\'s wireless connection to be switched to a non-preferred connection. Answer: D is incorrect. IKECrack is an IKE/IPSec authentication crack tool, which uses brute force for searching password and key combinations of Pre-Shared-Key authentication networks. The IKECrack tool undermines the latest Wi-Fi security protocol with repetitive attempts at authentication with random passphrases or keys. Answer: B is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets To detect standard named networks To detect masked networks To collect the presence of non-beaconing networks via data traffic

QUESTION 13

What will be the output of the following command? echo $(date %M) > date.txt

A. The current time (Month) will be written in the date.txt file.

B. It will create a variable $(date %M).

C. It will print a string "date %M".

D. The current time (Minutes) will be written in the date.txt file.

Correct Answer: D

The date command with the %M specifier prints the current time (Minutes). Since the output is redirected towards the date.txt file, the current time (Minutes) will be printed in the date.txt file.

QUESTION 14

You are the Security Consultant and have been hired to check security for a client\\'s network. Your client has stated that he has many concerns but the most critical is the security of Web applications on their Web server.

What should be your highest priority then in checking his network?

A. Setting up a honey pot

B. Vulnerability scanning

C. Setting up IDS

D. Port scanning

Correct Answer: B

According to the question, you highest priority is to scan the Web applications for vulnerability.

QUESTION 15

Which of the following functions are performed by methods of the HttpSessionActivationListener interface?

A. Notifying an attribute that a session has just migrated from one JVM to another.

B. Notifying the object when it is unbound from a session.

C. Notifying the object when it is bound to a session.

D. Notifying an attribute that a session is about to migrate from one JVM to another.

Correct Answer: AD

The HttpSessionActivationListener interface notifies an attribute that the session is about to be activated or passivated. Methods of this interface are as follows:

public voidsessionDidActivate(HttpSessionEvent session): It notifies the attribute that the session has just been moved to a different JVM. public void sessionWillPassivate(HttpSessionEvent se): It notifies the attribute that the session is about

to move to a different JVM. Answer: B, C are incorrect. These functions are performed by the HttpSessionBindingListener interface. The HttpSessionBindingListener interface causes an object of the implementing class to be notified when it is

added to or removed from a session. The HttpSessionBindingListener interface has the following methods:

public void valueBound(event): This method takes an object of type HttpSessionBindingEvent as an argument. It notifies the object when it is bound to a session.

public void valueUnbound(HttpSessionBindingEvent event): This method takes an object of type HttpSessionBindingEvent as an argument. It notifies the object when it is unbound from a session.