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.passapply.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

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 2

You work as a Network Auditor for XYZ CORP. The company has a Windows-based network. You use DumpSec as an auditing and reporting program for security issues.

Which of the following statements is true about DumpSec? (Choose three)

A. It obtains the DACLs for the registry.

B. It dumps user and group information.

C. It collates the DACLs for the file system.

D. It kills the running services in the Windows environment.

Correct Answer: ABC

DumpSec, a program launched by Somarsoft, is a security auditing and reporting program for Microsoft Windows. It collates and obtains the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers, and shares in

a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group, and replication information, policies, as well as services (Win32) and kernel drivers loaded on the system. It can also report

the current status of services (running or stopped) in the Windows environment.

Answer: D is incorrect. It cannot kill running services. It can only report the current status of services (running or stopped) in the Windows environment.

QUESTION 3

A Web developer with your company wants to have wireless access for contractors that come in to work on various projects. The process of getting this approved takes time. So rather than wait, he has put his own wireless router attached to one of the network ports in his department.

What security risk does this present?

A. None, adding a wireless access point is a common task and not a security risk.

B. It is likely to increase network traffic and slow down network performance.

C. This circumvents network intrusion detection.

D. An unauthorized WAP is one way for hackers to get into a network.

Correct Answer: D

Any unauthorized Wireless Access Point (WAP) is a serious security breach. Its configuration might be very unsecure. For example, it might not use encryption or MAC filtering, thus allowing anyone in range to get on the network.

QUESTION 4

Sam works as a Network Administrator for XYZ CORP. The computers in the company run Windows Vista operating system, and they are continuously connected to the Internet. This makes the network of the company susceptible to attacks from unauthorized users.

Which of the following will Sam choose to protect the network of the company from such attacks?

A. Firewall

B. Windows Defender

C. Software Explorer

D. Quarantined items

Correct Answer: A

A firewall is a set of related programs configured to protect private networks connected to the Internet from intrusion. It is used to regulate the network traffic between different computer networks. It permits or denies the transmission of a network packet to its destination based on a set of rules. A firewall is often installed on a separate computer so that an incoming packet does not get into the network directly. Answer: B is incorrect. Windows Defender is a software product designed by Microsoft to provide continuous security against malware. If it detects anything suspicious, an alert will appear on the screen. Windows Defender can also be used to scan a computer for suspicious software. It can remove or quarantine any malware or spyware it finds. Answer: C is incorrect. Software Explorer is a tool of Windows Defender. It is used to remove, enable, or disable the programs running on a computer. Answer: D is incorrect. Quarantined items is a tool of Windows Defender. It is used to remove or restore a program blocked by Windows Defender.

QUESTION 5

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 6

You work as a Network Administrator for Tech Perfect Inc. 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 has recently provided fifty laptops to its sales team members. You are required to configure an 802.11 wireless network for the laptops. The sales team members must be able to use their data placed at a server in a cabled network. The planned network should be able to handle the threat of unauthorized access and data interception by an unauthorized user. You are also required to prevent the sales team members from communicating directly to one another.

Which of the following actions will you take to accomplish the task?

A. Implement the open system authentication for the wireless network.

B. Configure the wireless network to use WEP encryption for the data transmitted over a wireless network.

C. Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only.

D. Implement the IEEE 802.1X authentication for the wireless network.

E. Using group policies, configure the network to allow the wireless computers to connect to the ad hoc networks only.

Correct Answer: BCD

In order to enable wireless networking, you have to install access points in various areas of your office building. These access points generate omni directional signals to broadcast network traffic. Unauthorized users can intercept these

packets. Hence, security is the major concern for a wireless network. The two primary threats are unauthorized access and data interception.

In order to accomplish the task, you will have to take the following steps:

Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only. This will prevent the sales team members from communicating directly to one another. Implement the IEEE 802.1X

authentication for the wireless network. This will allow only authenticated users to access the network data and resources. Configure the wireless network to use WEP encryption for data transmitted over a wireless network. This will encrypt

the network data packets transmitted over wireless connections.

Although WEP encryption does not prevent intruders from capturing the packets, it prevents them from reading the data inside.

QUESTION 7

Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration. The tool uses raw IP packets to determine the

following:

What ports are open on our network systems.

What hosts are available on the network.

Identify unauthorized wireless access points.

What services (application name and version) those hosts are offering.

What operating systems (and OS versions) they are running.

What type of packet filters/firewalls are in use.

Which of the following tools is Victor using?

A. Nessus

B. Sniffer

C. Nmap

D. Kismet

Correct Answer: C

Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is

capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version

number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows etc.

Answer: D 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

Answer: A is incorrect. Nessus is proprietary comprehensive vulnerability scanning software. It is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on the tested systems. It is capable

of checking various types of vulnerabilities, some of which are as follows:

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.

Answer: B is incorrect. A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the

network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host. This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal, Snort, Windump,

EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc.

QUESTION 8

You work as a Network Administrator for Infosec Inc. Nowadays, you are facing an unauthorized access in your Wi-Fi network. Therefore, you analyze a log that has been recorded by your favorite sniffer, Ethereal. You are able to discover

the cause of the unauthorized access after noticing the following string in the log file:

(Wlan.fc.type_subtype eq 32 and llc.oui eq 0x00601d and llc.pid eq 0x0001)

When you find All your 802.11b are belong to us as the payload string, you are convinced about which tool is being used for the unauthorized access.

Which of the following tools have you ascertained?

A. AiroPeek

B. AirSnort

C. Kismet

D. NetStumbler

Correct Answer: D

NetStumbler, a war driving tool, uses an organizationally unique identifier (OID) of 0x00601A, D protocol identifier (PID) of 0x0001. Each version has a typical payload string. For example, NetStumbler 3.2.3 has a payload string: \\'All your 802.11b are belong to us\\'. Therefore, when you see the OID and PID values, you discover that the attacker is using

NetStumbler, and when you see the payload string, you are able to ascertain that the attacker is using NetStumbler 3.2.3.

QUESTION 9

George works as an office assistant in Soft Well Inc. The company uses the Windows Vista operating system. He wants to disable a program running on a computer.

Which of the following Windows Defender tools will he use to accomplish the task?

A. Allowed items

B. Quarantined items

C. Options

D. Software Explorer

Correct Answer: D

Software Explorer is used to remove, enable, or disable a program running on a computer. Answer: A is incorrect. Allowed items contains a list of all the programs that a user has chosen not to monitor with Windows Defender.

Answer: C is incorrect. Options is used to choose how Windows Defender should monitor all the programs running on a computer.

Answer: B is incorrect. Quarantined items are used to remove or restore a program blocked by Windows Defender.

QUESTION 10

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following pre-attack phases while testing the security of the server:

Footprinting Scanning

Now he wants to conduct the enumeration phase.

Which of the following tools can John use to conduct it?

A. PsPasswd

B. WinSSLMiM

C. PsFile

D. UserInfo

Correct Answer: ACD

John can use the UserInfo, PsFile, and PsPasswd tools in the enumeration phase. UserInfo is a utility that retrieves all available information about any known user from any Windows 2000/NT operating system (accessible by TCP port 139).

UserInfo returns mainly the following information: SID and Primary group Logon restrictions and smart card requirements Special group Password expiration Note: UserInfo works as a NULL user even if the RestrictedAnonymous value in the

LSA key is set to 1 to specifically deny anonymous enumeration. PsFile is a command-line utility that shows a list of files on a system that are opened remotely. It also allows a user to close opened files either by name or by a file identifier.

The command syntax for PsFile is as follows:

psfile [\\RemoteComputer [-u Username [-p Password]]] [Id | path] [-c]

-u specifies the optional user name for logging in to a remote computer.

-p specifies a password for a user name.

If this is omitted, the user is prompted to enter the password without it being echoed to the screen.

Id is the identifier of the file about which the user wants to display information.

-c closes the files identifed by the ID or path.

PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system.

The command syntax of PsPasswd is as follows: pspasswd [\\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]

Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new password. If omitted, a NULL password is applied.

QUESTION 11

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to run a command that forces all the unwritten blocks in the buffer cache to be written to the disk.

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

A. swapon

B. tune2fs

C. swapoff

D. sync

Correct Answer: D

The sync command is used to flush filesystem buffers. It ensures that all disk writes have been completed before the processor is halted or rebooted. Generally, it is preferable to use reboot or halt to shut down a system, as they may

perform

additional actions such as resynchronizing the hardware clock and flushing internal caches before performing a final sync.

Answer: B is incorrect. In Unix, the tune2fs command is used to adjust tunable filesystem parameters on the second extended filesystems.

Answer: A is incorrect. In Unix, the swapon command is used to activate a swap partition.

Answer: C is incorrect. In Unix, the swapoff command is used to de-activate a swap partition.

QUESTION 12

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 13

What does CSS stand for?

A. Cascading Style Sheet

B. Coded System Sheet

C. Cyclic Style Sheet

D. Cascading Style System

Correct Answer: A

A Cascading Style Sheet (CSS) is a separate text file that keeps track of design and formatting information, such as colors, fonts, font sizes, and margins, used in Web pages. CSS is used to provide Web site authors greater control on the appearance and presentation of their Web pages. It has codes that are interpreted and applied by the browser on to the Web pages and their elements. CSS files have .css extension. There are three types of Cascading Style Sheets: External Style Sheet Embedded Style Sheet Inline Style Sheet

QUESTION 14

A sequence number is a 32-bit number ranging from 1 to 4,294,967,295. When data is sent over the network, it is broken into fragments (packets) at the source and reassembled at the destination system. Each packet contains a sequence number that is used by the destination system to reassemble the data packets in the correct order. The Initial Sequence Number of your computer is 24171311 at login time. You connect your computer to a computer having the IP address

210.213.23.21. This whole process takes three seconds.

What will the value of the Initial Sequence Number be at this moment?

A. 24171811

B. 24619311

C. 24171111

D. 24171311

Correct Answer: B

You took 3 seconds to establish a connection. During this time, the value of the Initial Sequence Number would become [24171311 + (1 * 64000) + (3 * 128000)], i.e., 24619311.

QUESTION 15

You want to monitor the network infrastructure of a software-based company. The network infrastructure of the company consists of the following:

Windows TCP/IP services

Web and mail servers

URLs Applications (MS Exchange, SQL etc.)

Which of the following network monitoring solutions can you use to accomplish the task?

A. Axence nVision

B. CommandCenter NOC

C. Netmon

D. Cymphonix Network Composer

Correct Answer: A

Axence nVision is an advanced solution for a comprehensive network management. It is used to monitor network infrastructure such as Windows, TCP/IP services, web and mail servers, URLs, and applications (MS Exchange, SQL, etc.). It is also used to monitor routers and switches such as network traffic, interface status, and connected computers. It collects the network inventory and audit license usage. It also gives alerts in case of a program installation or any configuration change on a remote node. With the agent, an administrator can easily monitor user activities and can access computers remotely. Answer: B is incorrect. CommandCenter NOC is a simple and effective tool that performs network monitoring with a powerful polling engine. It provides polling, Windows and UNIX/Linux server management, intrusion detection, vulnerability scanning, and traffic analysis in an integrated appliance. Answer: D is incorrect. Cymphonix Network Composer is a precise Web gateway appliance. It is used to monitorInternet traffic by user, application, and threat. It consists of controls to shape access to Internet resources by user, group, and/or time of day. It also supports anonymous proxy blocking, policy management, and real time monitoring. Answer: C is incorrect. Network Monitor (Netmon) is a protocol analyzer. It is used to analyze the network traffic. It is installed by default during the installation of the operating system. It can be installed by using Windows Components Wizard in the Add or Remove Programs tool in Control Panel. Network Monitor is used to perform the following tasks:

1.

Capture frames directly from the network.

2.

Display and filter captured frames immediately after capture or a later time.

3.

Edit captured frames and transmit them on the network.

4.

Capture frames from a remote computer.

Latest GNSA Dumps GNSA PDF Dumps GNSA Braindumps