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.certbus.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

Fill in the blank with the appropriate term.

When two routers are used in a firewall configuration, the internal router is known as a _____ router.

A. choke

Correct Answer: A

When two routers are used in a firewall configuration, the internal router is known as a choke router. A choke router is an interior router present in the screened host firewall architecture. It is attached to the perimeter network and protects the

internal network from the Internet and the perimeter net.

A choke router is basically employed for the job of packet filtering for the firewall. It is also used to provide access to selected services that are outbound from the internal net to the Internet. These services may include outgoing Telnet, FTP,

WAIS, Archie, Gopher, etc.

QUESTION 2

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail.

Which of the following techniques is he performing to accomplish his task?

A. Web ripping

B. Steganography

C. Email spoofing

D. Social engineering

Correct Answer: B

According to the scenario, John is performing the Steganography technique for sending malicious data. Steganography is an art and science of hiding information by embedding harmful messages within other seemingly harmless messages.

It works by replacing bits of unused data, such as graphics, sound, text, and HTML, with bits of invisible information in regular computer files. This hidden information can be in the form of plain text, cipher text, or even in the form of images.

Answer: A is incorrect. Web ripping is a technique in which the attacker copies the whole structure of a Web site to the local disk and obtains all files of the Web site. Web ripping helps an attacker to trace the loopholes of the Web site.

Answer: D is incorrect. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user\\'s

computer or network. This method involves mental ability of the people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name or password, computer name, IP address,

employee ID, or other information that can be misused.

Answer: C is incorrect. John is not performing email spoofing. In email spoofing, an attacker sends emails after writing another person\\'s mailing address in the from field of the emailed.

QUESTION 3

You are concerned about an attacker being able to get into your network. You want to make sure that you are informed of any network activity that is outside normal parameters.

What is the best way to do this?

A. Utilize protocol analyzers.

B. User performance monitors.

C. Implement signature based antivirus.

D. Implement an anomaly based IDS.

Correct Answer: D

An anomaly based Intrusion Detection System will monitor the network for any activity that is outside normal parameters (i.e. an anomaly) and inform you of it.

Answer: C is incorrect. Antivirus software, while important, won\\'t help detect the activities of intruders.

Answer: B is incorrect. Performance monitors are used to measure normal network activity and look for problems such as bottlenecks.

Answer: A is incorrect. A protocol analyzer does detect if a given protocol is moving over a particular network segment.

QUESTION 4

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 5

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 6

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He begins to perform a pre-attack test before conducting an attack on the We-are-secure server.

Which of the following will John perform in the pre-attack phase?

A. Determining network range

B. Identifying active machines

C. Enumeration

D. Finding open ports and applications

E. Information gathering

Correct Answer: ABDE

In the pre-attack phase, there are seven steps, which have been defined by the EC-Council, as follows:

1.

Information gathering

2.

Determining network range

3.

Identifying active machines

4.

Finding open ports and applications

5.

OS fingerprinting

6.

Fingerprinting services

7.Mapping the network

Answer: C is incorrect. In the enumeration phase, the attacker gathers information such as the network user and group names, routing tables, and Simple Network Management Protocol (SNMP) data.

The techniques used in this phase are as follows:

1.

Obtaining Active Directory information and identifying vulnerable user accounts

2.

Discovering NetBIOS names

3.

Employing Windows DNS queries

4.

Establishing NULL sessions and queries

QUESTION 7

Which of the following encryption modes are possible in WEP?

A. 128 bit encryption

B. No encryption

C. 256 bit encryption

D. 40 bit encryption

Correct Answer: ABD

WEP supports three encryption modes, i.e., no encryption, 40 bit encryption, and 128 bit encryption. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and

encryption. It provides security, which is equivalent to wired networks, for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the

attacks that attempt to reveal the key stream.

Answer: C is incorrect. WEP does not support 256 bit encryption.

QUESTION 8

You work as a Database Administrator for BigApple Inc. The Company uses Oracle as its database. You enabled standard database auditing. Later, you noticed that it has a huge impact on performance of the database by generating a large amount of audit data.

How will you keep control on this audit data?

A. By implementing principle of least privilege.

B. By removing some potentially dangerous privileges.

C. By setting the REMOTE_LOGIN_PASSWORDFILE instance parameter to NONE.

D. By limiting the number of audit records generated to only those of interest.

Correct Answer: D

Auditing is the process of monitoring and recording the actions of selected users in a database. Auditing is of the following types: Mandatory auditing Standard auditing Fine-grained auditing

By focusing the audits as narrow as possible, you will get audit records for events that are of significance. If it is possible then try doing audit by session, not by access. When auditing a database the SYS.AUD$ table may grow many gigabytes. You may delete or truncate it periodically to control the load of audit data. minimum set of privileges that are just sufficient to accomplish their requisite roles, so that even if the users try, they cannot perform those actions that may critically endanger the safety of data in the event of any malicious attacks. It is important to mention that some damage to data may still be unavoidable. Therefore, after identifying the scope of their role, users are allocated only those minimal privileges just compatible with that role. This helps in minimizing the damage to data due to malicious attacks. Grant of more privileges than necessary may make data critically vulnerable to malicious exploitation. The principle of least privilege is also known as the principle of minimal privilege and is sometimes also referred to as POLA, an abbreviation for the principle of least authority. The principle of least privilege is implemented to enhance fault tolerance, i.e. to protect data from malicious attacks. While applying the principle of least privilege, one should ensure that the parameter 07_DICTIONARY_ACCESSIBILITY in the data dictionary is set to FALSE, and revoke those packages and roles granted to a special pseudo-user known as Public that are not necessary to perform the legitimate actions, after reviewing them. This is very important since every user of the database, without exception, is automatically allocated the Public pseudo-user role. Some of the packages that are granted to the special pseudo-user known as Public are as follows: UTL_TCP UTL_SMTP UTL_HTTP UTL_FILE REMOTE_LOGIN_PASSWORDFILE is an initialization parameter used to mention whether or not Oracle will check for a password file and by which databases a password file can be used. The various properties of this initialization parameter are as follows: Parameter type: String Syntax: REMOTE_LOGIN_PASSWORDFILE = {NONE | SHARED | EXCLUSIVE} Default value: NONE Removing some potentially dangerous privileges is a security option. All of the above discussed options are security steps and are

not involved in standard database auditing.

QUESTION 9

ACID (atomicity, consistency, isolation, and durability) is an acronym and mnemonic device for learning and remembering the four primary attributes ensured to any transaction by a transaction manager. Which of the following attributes of ACID confirms that the committed data will be saved by the system such that, even in the event of a failure or system restart, the data will be available in its correct state?

A. Durability

B. Atomicity

C. Isolation

D. Consistency

Correct Answer: A

Durability is the attribute of ACID which confirms that the committed data will be saved by the system such that, even in the event of a failure or system restart, the data will be available in its correct state. Answer: B is incorrect. Atomicity is the attribute of ACID which confirms that, in a transaction involving two or more discrete pieces of information, either all of the pieces are committed or none are. Answer: D is incorrect. Consistency is the attribute of ACID which confirms that a transaction either creates a new and valid state of data, or, if any failure occurs, returns all data to its state before the transaction was started. Answer: C is incorrect. Isolation is the attribute of ACID which confirms that a transaction in process and not yet committed must remain isolated from any other transaction.

QUESTION 10

Which of the following statements are true about locating rogue access points using WLAN discovery software such as NetStumbler, Kismet, or MacStumbler if you are using a Laptop integrated with Wi-Fi compliant MiniPCI card? (Choose two)

A. These tools can determine the rogue access point even when it is attached to a wired network.

B. These tools can determine the authorization status of an access point.

C. These tools cannot detect rogue access points if the victim is using data encryption.

D. These tools detect rogue access points if the victim is using IEEE 802.11 frequency bands.

Correct Answer: BD

WLAN discovery software such as NetStumbler, Kismet, or MacStumbler can be used to detect rogue access points if the victim is using IEEE 802 frequency bands. However, if the victim is using non-IEEE 802.11 frequency bands or unpopular modulations, these tools might not detect rogue access. NetStumbler, kismet, or MacStumbler also gives the authorization status of an access point. A Rogue access point (AP) is set up by the attackers in an Enterprise\\'s network. The attacker captures packets in the existing wireless LAN (WLAN) and finds the SSID and security keys (by cracking). Then the attacker sets up his own AP using the same SSID and security keys. The network clients unknowingly use this AP and the attacker captures their usernames and passwords. This can help the attacker to intrude the security and have access to the Enterprise data. Answer: A, C are incorrect. The WLAN software such as NetStumbler, Kismet, or MacStumbler can search rogue access points even when the victim is using data encryption. However, these tools cannot determine the rogue access point even when it is attached to a wired network.

QUESTION 11

You work as a Network Administrator for XYZ CORP. The company has a TCP/IP-based network environment. The network contains Cisco switches and a Cisco router.

You run the following command for a router interface:

show interface serial0

You get the following output:

Serial0 is administratively down, line protocol is down

What will be your conclusion after viewing this output?

A. There is a physical problem either with the interface or the cable attached to it.

B. The router has no power.

C. There is a problem related to encapsulation.

D. The interface is shut down.

Correct Answer: D

According to the question, the output displays that the interface is administratively down. Administratively down means that the interface is shut down. In order to up the interface, you will have to open the interface with the no shutdown command.

Answer: A is incorrect. Had there been a physical problem with the interface, the output would not have displayed "administratively down". Instead, the output would be as follows: serial0 is down, line protocol is down Answer: B is incorrect.

You cannot run this command on a router that is powered off.

Answer: C is incorrect. Encapsulation has nothing to do with the output displayed in the question.

QUESTION 12

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows: C.\whisker.pl -h target_IP_address -- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - = = Host: target_IP_address = Server: Apache/1.3.12 (Win32) ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22 + 200 OK: HEAD /cgi-bin/printenv John recognizes /cgi-bin/printenv vulnerability (\\'Printenv\\' vulnerability) in the We_are_secure server.

Which of the following statements about \\'Printenv\\' vulnerability are true?

A. With the help of \\'printenv\\' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

B. \\'Printenv\\' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.

C. The countermeasure to \\'printenv\\' vulnerability is to remove the CGI script.

D. This vulnerability helps in a cross site scripting attack.

Correct Answer: ACD

\\'Printenv\\' vulnerability allows an attacker to input specially crafted links and/or other malicious scripts. For example, http://www/cgi-bin/printenv/alert (An attacker can misuse it!) Since \\'printenv\\' is just an example CGI script (It

comes with various versions of the Apache Web server.) that has no real use and has its own problems, there is no problem in removing it.

Answer: B is incorrect. \\'Printenv\\' does not maintain any log file of user activities.

QUESTION 13

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You have been assigned the task to design the authentication system for the remote users of the company. For security purposes, you want to issue security tokens to the remote users. The token should work on the one-time password principle and so once used, the next password gets generated.

Which of the following security tokens should you issue to accomplish the task?

A. Virtual tokens

B. Event-based tokens

C. Bluetooth tokens

D. Single sign-on software tokens

Correct Answer: B

An event-based token, by its nature, has a long life span. They work on the one-time password principle and so once used, the next password is generated. Often the user has a button to press to receive this new code via either a token or via an SMS message. All CRYPTOCard\\'s tokens are event-based rather than time-based. Answer: C is incorrect. Bluetooth tokens are often combined with a USB token, and hence work in both a connected and disconnected state. Bluetooth authentication works when closer than 32 feet (10 meters). If the Bluetooth is not available, the token must be inserted into a USB input device to function. Answer: A is incorrect. Virtual tokens are a new concept in multi-factor authentication first introduced in 2005 by security company Sestus. Virtual tokens work by sharing the token generation process between the Internet website and the user\\'s computer and have the advantage of not requiring the distribution of additional hardware or software. In addition, since the user\\'s device is communicating directly with the authenticating website, the solution is resistant to man-in-themiddle attacks and similar forms of online fraud. Answer: D is incorrect. Single sign-on software tokens are used by the multiple, related, but independent software systems. Some types of single sign-on (SSO) solutions, like enterprise single sign-on, use this token to store software that allows for seamless authentication and password filling. As the passwords are stored on the token, users need not remember their passwords and therefore can select more secure passwords, or have more secure passwords assigned.

QUESTION 14

You work as a Network Administrator for XYZ CORP. The company\\'s Windows 2000 network is configured with Internet Security and Acceleration (ISA) Server 2000. ISA Server is configured as follows: The server uses the default site and content rule and default IP packet filters. Packet filtering is enabled. The server has two protocol rules:

Name of the Rule	Scope	Action	Protocol	Applies To	Schedule
Web-Secure	Array	Allow	HTTPS	Any request	Always
Web	Array	Allow	HTTPS	Any request	Always

Users in the network complain that they are unable to access secure Web sites. However, they are able to connect to Web sites in which secure transmission is not required.

What is the most likely cause?

A. A protocol rule that allows the use of HTTP has not been created.

B. An IP packet filter that allows the use of network traffic on port 80 has not been created.

C. An IP packet filter that allows the use of network traffic on port 443 has not been created.

D. A protocol rule that allows the use of HTTPS has not been created.

Correct Answer: C

The default IP packet filter allows HTTP protocol (for non-secure communication) at port 80 to access the Internet. However, to allow users to access secure Web sites, you will have to create an additional packet filter to allow communication on port 443.

QUESTION 15

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.