Vendor:GIAC

Exam Code:GSNA

Exam Name:GIAC Systems and Network Auditor

Version: Demo

QUESTION 1

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 2

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

A. Single Loss Expectancy (SLE)

B. Annualized Rate of Occurrence (ARO)

C. Exposure Factor (EF)

D. Safeguard

Correct Answer: B

The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could

make that event occur.

Answer: C is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). Answer: A is incorrect. The Single Loss Expectancy (SLE) is the value in

dollars that is assigned to a single event. SLE = Asset Value ($) X Exposure Factor (EF) Answer: D is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

QUESTION 3

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 4

Which of the following commands will you use to watch a log file /var/adm/messages while the log file is updating continuously?

A. less -g /var/adm/messages

B. tail /var/adm/messages

C. cat /var/adm/messages

D. tail -f /var/adm/messages

Correct Answer: D

The tail command is used to display the last few lines of a text file or piped data. It has a special command line option -f (follow) that allows a file to be monitored. Instead of displaying the last few lines and exiting, tail displays the lines and

then monitors the file. As new lines are added to the file by another process, tail updates the display. This is particularly useful for monitoring log files. The following command will display the last 10 lines of messages and append new lines to

the display as new lines are added to messages:

tail -f /var/adm/messages

Answer: B is incorrect. The tail command will display the last 10 lines (default) of the log file. Answer: C is incorrect. The

concatenate (cat) command is used to display or print the contents of a file.

Syntax: cat filename

For example, the following command will display the contents of the /var/log/dmesg file: cat /var/log/dmesg Note: The more command is used in conjunction with the cat command to prevent scrolling of the screen while displaying the contents

of a file.

Answer: A is incorrect. The less command is used to view (but not change) the contents of a text file, one screen at a time. It is similar to the more command. However, it has the extended capability of allowing both forward and backward

navigation through the file. Unlike most Unix text editors/viewers, less does not need to read the entire file before starting; therefore, it has faster load times with large files.

The command syntax of the less command is as follows:

less [options] file_name Where,

QUESTION 5

You work as a Web Deployer for UcTech Inc. You write the element for an application in which you write the sub-element as follows: * Who will have access to the application?

A. Only the administrator

B. No user

C. All users

D. It depends on the application.

Correct Answer: C

The element is a sub-element of the element. It defines the roles that are allowed to access the Web resources specified by the sub-elements. The element

is written in the deployment descriptor as follows:

---------- Administrator Writing Administrator within the

element will allow only the administrator to have access to the resource defined within the element.

QUESTION 6

You work as a Network Administrator for XYZ CORP. 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\\'s management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks: The wireless network communication should be secured. The laptop users should be able to use smart cards for getting authenticated. In order to accomplish the tasks, you take the following steps: Configure 802.1x and WEP for the wireless connections. Configure the PEAP-MS-CHAP v2 protocol for authentication.

What will happen after you have taken these steps?

A. Both tasks will be accomplished.

B. The laptop users will be able to use smart cards for getting authenticated.

C. The wireless network communication will be secured.

D. None of the tasks will be accomplished.

Correct Answer: C

As 802.1xand WEP are configured, this step will enable the secure wireless network communication. For authentication, you have configured the PEAP-MS-CHAP v2 protocol. This protocol can be used for authentication on wireless networks, but it cannot use a public key infrastructure (PKI). No certificate can be issued without a PKI. Smart cards cannot be used for authentication without certificates. Hence, the laptop users will not be able to use smart cards for getting authenticated.

QUESTION 7

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

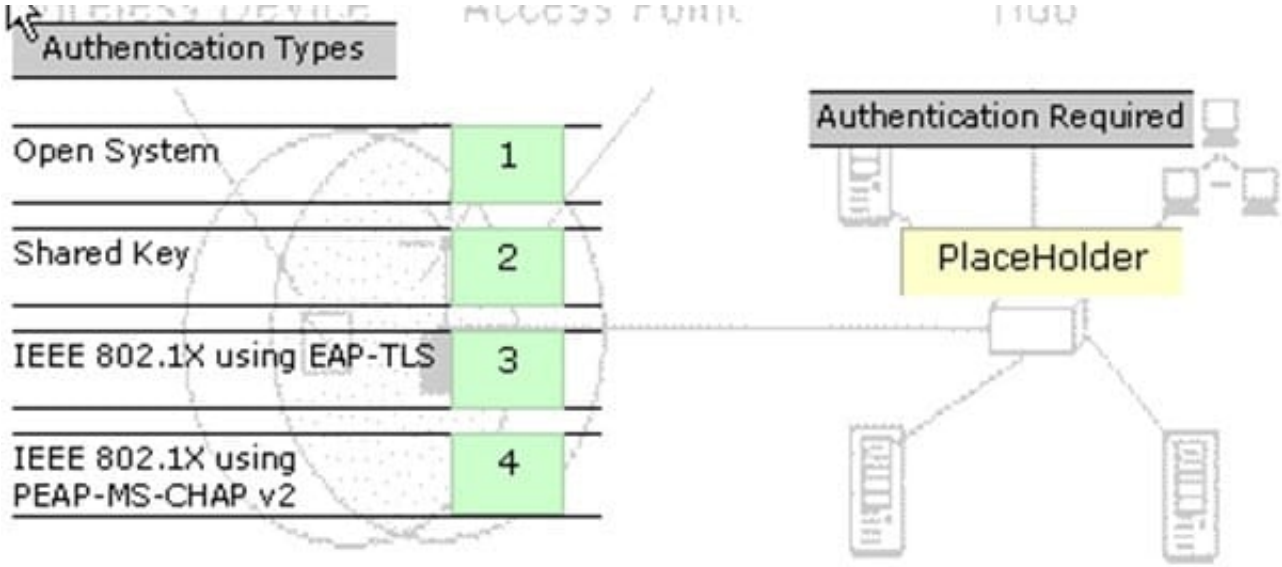
An event-based token, by its nature, has a long life span. They work on the one-time password principle and so once used, the next password is generated. Often the user has a button to press to receive this new code via either a token or via an SMS message. All CRYPTOCard\\'s tokens are event-based rather 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-the-middle 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 8

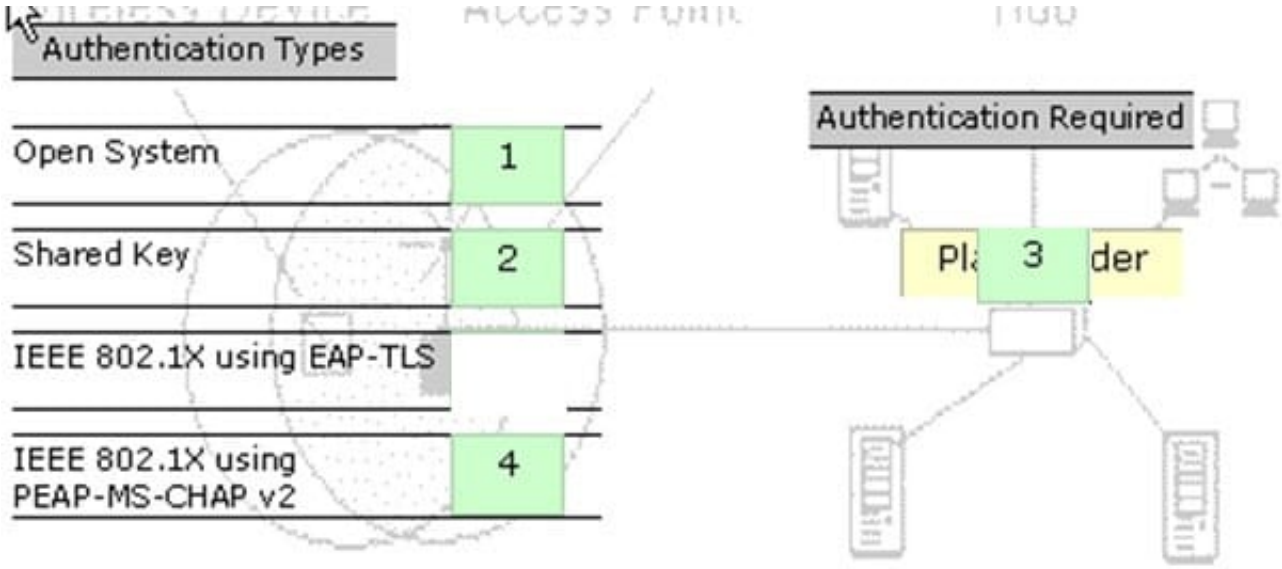
DRAG DROP

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. The company has recently provided laptops to its sales team members. You have configured access points in the network to enable a wireless network. The company\\'s security policy states that all users using laptops must use smart cards for authentication. Select and place the authentication method you are required to configure to implement the security policy of the company.

Select and Place:



Correct Answer:



In order to ensure that the laptop users use smart cards for authentication, you will have to configure IEEE 802.1X authentication using the EAP-TLS protocol on the network.

QUESTION 9

Andrew works as a Network Administrator for Infonet Inc. The company has a Windows 2003 domain- based network. The network has five Windows 2003 member servers and 150 Windows XP Professional client computers. One of the member servers works as an IIS server. The IIS server is configured to use the IP address 142.100.10.6 for Internet users and the IP address 16.5.7.1 for the local network. Andrew wants the server to allow only Web communication over the Internet. He also wants to enable the local network users to access the shared folders and other resources.

How will Andrew configure the IIS server to accomplish this? (Choose three)

A. Enable the IP packet filter.

B. Permit all the ports on the network adapter that uses the IP address142.100.10.6.

C. Permit only port 25 on the network adapter that uses the IP address 142.100.10.6.

D. Permit all the ports on the network adapter that uses the IP address 16.5.7.1.

E. Permit only port 80 on the network adapter that uses the IP address 142.100.10.6.

Correct Answer: ADE

In order to configure the IIS server to allow only Web communication over the Internet, Andrew will have to use IP packet filtering to permit only port 80 on the network adapter that uses the IP address 142.100.10.6 for connecting to the Internet. This is because Web communication uses the Hyper Text Transfer Protocol (HTTP) that uses the TCP port 80. IP packet filtering restricts the IP traffic received by the network interface by controlling the TCP or UDP port for incoming data. Furthermore, Andrew wants to allow local users to access shared folders and all other resources. Therefore, Andrew will have to enable all the ports on the network adapter that uses the IP address 16.5.7.1 for the local network.

QUESTION 10

John works as a Network Administrator for We-are-secure Inc. The We-are-secure server is based on Windows Server 2003. One day, while analyzing the network security, he receives an error message that Kernel32.exe is encountering a problem. Which of the following steps should John take as a countermeasure to this situation?

A. He should download the latest patches for Windows Server 2003 from the Microsoft site, so that he can repair the kernel.

B. He should restore his Windows settings.

C. He should observe the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new malicious process is running, he should kill that process.

D. He should upgrade his antivirus program.

Correct Answer: CD

In such a situation, when John receives an error message revealing that Kernel32.exe is encountering a problem, he needs to come to the conclusion that his antivirus program needs to be updated, because Kernel32.exe is not a Microsoft file (It is a Kernel32.DLL file.). Although such viruses normally run on stealth mode, he should examine the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new process (malicious) is running on the server, he should exterminate that process. Answer: A, B are incorrect. Since kernel.exe is not a real kernel file of Windows, there is no need to repair or download any patch for Windows Server 2003 from the Microsoft site to repair the kernel. Note: Such error messages can be received if the computer is infected with malware, such as Worm_Badtrans.b, Backdoor.G_Door, Glacier Backdoor, Win32.Badtrans.29020, etc.

QUESTION 11

Which of the following is an Internet mapping technique that relies on various BGP collectors that collect information such as routing updates and tables and provide this information publicly?

A. Path MTU discovery (PMTUD)

B. AS Route Inference

C. AS PATH Inference

D. Firewalking

Correct Answer: C

AS PATH Inference is one of the prominent techniques used for creating Internet maps. This technique relies on various BGP collectors that collect information such as routing updates and tables and provide this information publicly. Each BGP entry contains a Path Vector attribute called the AS Path. This path represents an autonomous system forwarding path from a given origin for a given set of prefixes. These paths can be used to infer AS-level connectivity and in turn be used to build AS topology graphs. However, these paths do not necessarily reflect how data is actually forwarded. Adjacencies between AS nodes only represent a policy relationship between them. A single AS link can in reality be several router links. It is also much harder to infer peering between two AS nodes, as these peering relationships are only propagated to an ISP\\'s customer networks. Nevertheless, support for this type of mapping is increasing as more and more ISP\\'s offer to peer with public route collectors such as Route-Views and RIPE. New toolsets are emerging such as Cyclops and NetViews that take advantage of a new experimental BGP collector BGPMon. NetViews can not only build topology maps in seconds but visualize topology changes moments after occurring at the actual router. Hence, routing dynamics can be visualized in real time. Answer: B is incorrect. There is no such Internet mapping technique. Answer: D is incorrect. Firewalking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. If the firewall allows this crafted packet through, it forwards the packet to the next hop. On the next hop, the packet expires and elicits an ICMP "TTLexpired in transit" message to the attacker. If the firewall does not allow the traffic, there should be no response, or an ICMP "administratively prohibited" message should be returned to the attacker. A malicious attacker can use firewalking to determine the types of ports/ protocols that can bypass the firewall. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall. The main drawback of this technique is that if an administrator blocks ICMP packets from leaving the network, it is ineffective. Answer: A is incorrect. Path MTU discovery (PMTUD) is a technique in computer networking for determining the maximum transmission unit (MTU) size on the network path between two Internet Protocol (IP) hosts, usually with the goal of avoiding IP fragmentation. Path MTU discovery works by setting the DF (Don\\'t Fragment) option bit in the IP headers of outgoing packets. Then, any device along the path whose MTU is smaller than the packet will drop it, and send back an ICMP "Fragmentation Needed" (Type 3, Code 4) message containing its MTU, allowing the source host to reduce its path MTU appropriately. The process repeats until the MTU is small enough to traverse the entire path without fragmentation. If the path MTU changes after the connection is set up and is lower than the previously determined path MTU, the first large packet will cause an ICMP error and the new, lower path MTU will be found. Conversely, if PMTUD finds that the path allows a larger MTU than what is possible on the lower link, the OS will periodically reprobe to see if the path has changed and now allows larger packets. On Linux this timer is set by default to ten minutes.

QUESTION 12

John works as a Security Professional. He is assigned a project to test the security of www.we-are- secure.com. John wants to get the information of all network connections and listening ports in the numerical form.

Which of the following commands will he use?

A. netstat -e

B. netstat ?

C. netstat -s

D. netstat ?n

Correct Answer: D

According to the scenario, John will use the netstat -an command to accomplish the task. The netstat -an command is used to get the information of all network connections and listening ports in the numerical form. The netstat command

displays protocol-related statistics and the state of current TCP/IP connections. It is used to get information about the open connections on a computer, incoming and outgoing data, as well as the ports of remote computers to which the

computer is connected. The netstat command gets all this networking information by reading the kernel routing tables in the memory. Answer: A is incorrect. The netstat -e command displays the Ethernet information. Answer: B is incorrect.

The netstat -r command displays the routing table information. Answer: C is incorrect. The netstat -s command displays per-protocol statistics.

By default, statistics are shown for TCP, UDP and IP.