Vendor:GIAC

Exam Code:GNSA

Exam Name:GIAC Systems and Network Auditor

Version: Demo

QUESTION 1

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to perform a stealth scan to discover open ports and applications running on the We-are-secure server. For this purpose, he wants to initiate scanning with the IP address of any third party.

Which of the following scanning techniques will John use to accomplish his task?

A. UDP

B. RPC

C. IDLE

D. TCP SYN/ACK

Correct Answer: C

The IDLE scan is initiated with the IP address of a third party. Hence, it becomes a stealth scan. Since the IDLE scan uses the IP address of a third party, it becomes quite impossible to detect the hacker. Answer: B is incorrect. The RPC

(Remote Procedure Call) scan is used to find the RPC applications. After getting the RPC application port with the help of another port scanner, RPC port scanner sends a null RPC packet to all the RPC service ports, which are open into the

target system.

Answer: A is incorrect. In UDP port scanning, a UDP packet is sent to each port of the target system. If the remote port is closed, the server replies that the remote port is unreachable. If the remote Port is open, no such error is generated.

Many firewalls block the TCP port scanning, at that time the UDP port scanning maybe useful. Certain IDS and firewalls can detect UDP port scanning easily. Answer: D is incorrect. TCP SYN scanning is also known as half-open scanning

because in this a full TCP connection is never opened. The steps of TCP SYN scanning are as follows:

1.The attacker sends SYN packet to the target port.

2.

If the port is open, the attacker receives SYN/ACK message.

3.

Now the attacker breaks the connection by sending an RST packet.

4.

If the RST packet is received, it indicates that the port is closed. This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.

QUESTION 2

You have just taken over as the Network Administrator for a medium sized company. You want to check to see what services are exposed to the outside world.

What tool would you use to accomplish this?

A. Network mapper

B. Protocol analyzer

C. A port scanner

D. Packet sniffer

Correct Answer: C

A port scanner is often used on the periphery of a network by either administrators or hackers. It will tell you what ports are open. By determining what ports are open, you know what services are exposed to the outside world. For example, if

port 80 is open, then HTTP traffic is allowed, meaning there should be a Web server on the network.

Answer: A is incorrect. Network mappers give a topography of the network, letting you know what is on your network and where it is connected. Answer: B is incorrect. A protocol analyzer does detect if a given protocol is moving over a

particular network segment, thus would detect services working on that segment. However, a port scanner is a better tool for detecting all the ports that are open.

Answer: D is incorrect. Packet sniffers are used to intercept traffic and to detect the contents of that traffic.

QUESTION 3

Which of the following statements about a session are true? (Choose two)

A. The creation time can be obtained using the getSessionCreationTime() method of the HttpSession.

B. The getAttribute() method of the HttpSession interface returns a String.

C. The time for the setMaxInactiveInterval() method of the HttpSession interface is specified in seconds.

D. The isNew() method is used to identify if the session is new.

Correct Answer: CD

The setMaxInactiveInterval() method sets the maximum time in seconds before a session becomes invalid. The syntax of this method is as follows: public void setMaxInactiveInterval(int interval) Here, interval is specified in seconds. The isNew() method of the HttpSession interface returns true if the client does not yet know about the session, or if the client chooses not to join the session. This method throws an IllegalStateException if called on an invalidated session. Answer B is incorrect. The getAttribute(String name) method of the HttpSession interface returns the value of the named attribute as an object. It returns a null value if no attribute with the given name is bound to the session. This method throws an IllegalStateException if it is called on an invalidated session. Answer: A is incorrect. The creation time of a session can be obtained using the getCreationTime() method of the HttpSession.

QUESTION 4

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

A. Incontrovertible

B. Corroborating

C. Direct

D. Circumstantial

Correct Answer: D

Circumstantial evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person. Answer: B is incorrect. Corroborating evidence is evidence that tends to support a

proposition that is already supported by some evidence. Answer: A is incorrect. Incontrovertible evidence is a colloquial term for evidence introduced to prove a fact that is supposed to be so conclusive that there can be no other truth as to the

matter; evidence so strong, it overpowers contrary evidence, directing a fact-finder to a specific and certain conclusion.

Answer: C is incorrect. Direct evidence is testimony proof for any evidence, which expressly or straight-forwardly proves the existence of a fact.

QUESTION 5

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security equivalent to wired networks for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key.

Which of the following statements are true about WEP?

A. WEP uses the RC4 encryption algorithm.

B. The Initialization Vector (IV) field of WEP is only 24 bits long.

C. It provides better security than the Wi-Fi Protected Access protocol.

D. Automated tools such as AirSnort are available for discovering WEP keys.

Correct Answer: ABD

Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security equivalent to wired networks for wireless networks. WEP encrypts

data on a wireless network by using a fixed secret key. WEP uses the RC4 encryption algorithm. The main drawback of WEP is that its Initialization Vector (IV) field is only 24 bits long. Many automated tools such as AirSnort are available for

discovering WEP keys.

Answer: C is incorrect. WPA stands for Wi-Fi Protected Access. It is a wireless security standard. It provides better security than WEP (Wired Equivalent Protection). Windows Vista supports both WPA-PSK and WPA-EAP.

Each of these is described as follows:

WPA-PSK: PSK stands for Preshared key. This standard is meant for home environment. WPA-PSK requires a user to enter an 8- character to 63-character passphrase into a wireless client. The WPA converts the passphrase into a 256-bit

key.

WPA-EAP: EAP stands for Extensible Authentication Protocol. This standard relies on a back-end server that runs Remote Authentication Dial-In User Service for user authentication. Note: Windows Vista supports a user to use a smart card

to connect to a WPA-EAP protected network.

QUESTION 6

Fill in the blank with the appropriate tool name.

__________ is a wireless network cracking tool that exploits the vulnerabilities in the RC4 Algorithm, which comprises the WEP security parameters.

A. WEPcrack

Correct Answer: A

WEPcrack is a wireless network cracking tool that exploits the vulnerabilities in the RC4 algorithm, which comprises the WEP security parameters. It mainly consists of three tools:

QUESTION 7

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

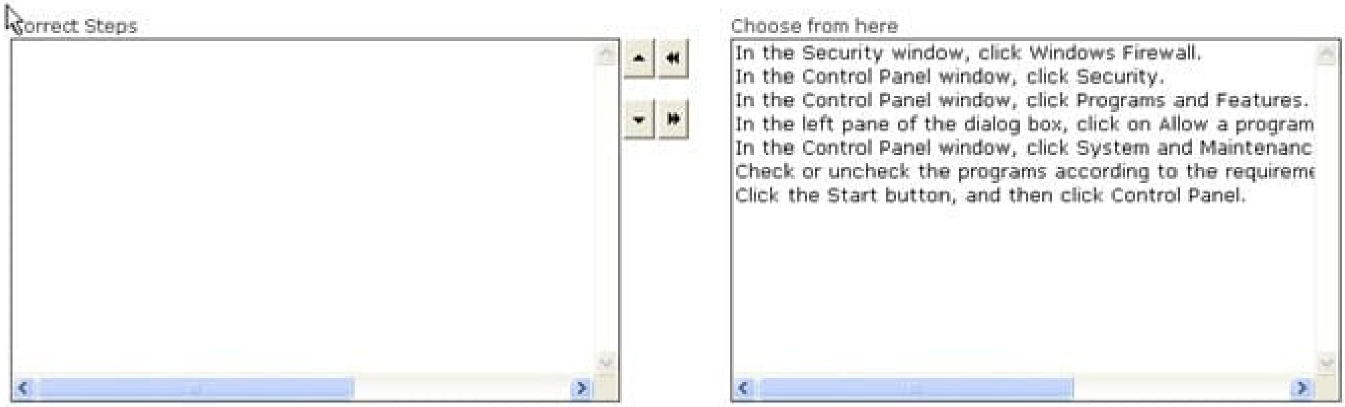
According to the question, you highest priority is to scan the Web applications for vulnerability.

QUESTION 8

DRAG DROP

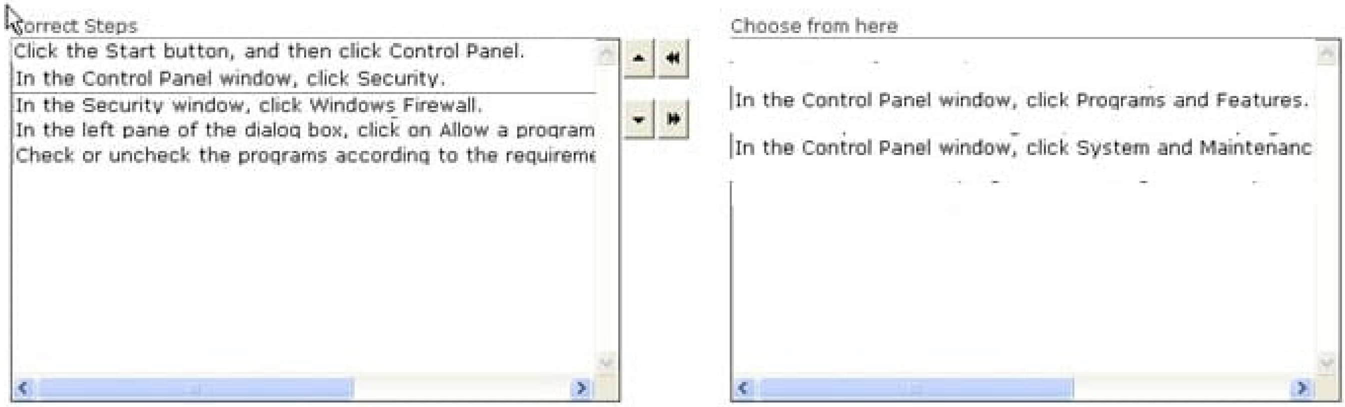
John works as a Network Administrator for Blue Well Inc. The company uses Windows Vista operating system. He wants to configure the firewall access for specific programs. What steps will he take to accomplish the task?

Select and Place:



In the Security window, click Windows Firewall.
In the Control Panel window, click Security.
In the Control Panel window, click Programs and Features.
In the left pane of the dialog box, click on Allow a program
In the Control Panel window, click System and Maintenanc
Check or uncheck the programs according to the requireme
Click the Start button, and then click Control Panel.

Correct Answer:



Click the Start button, and then click Control Panel.
In the Control Panel window, click Security.
In the Security window, click Windows Firewall.
In the left pane of the dialog box, click on Allow a program
Check or uncheck the programs according to the requireme

In the Control Panel window, click Programs and Features.
In the Control Panel window, click System and Maintenanc

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.

QUESTION 9

You have to move the whole directory /foo to /bar. Which of the following commands will you use to accomplish the task?

A. mv /bar /foo

B. mv -R /foo /bar

C. mv /foo /bar

D. mv -r /bar /foo

Correct Answer: C

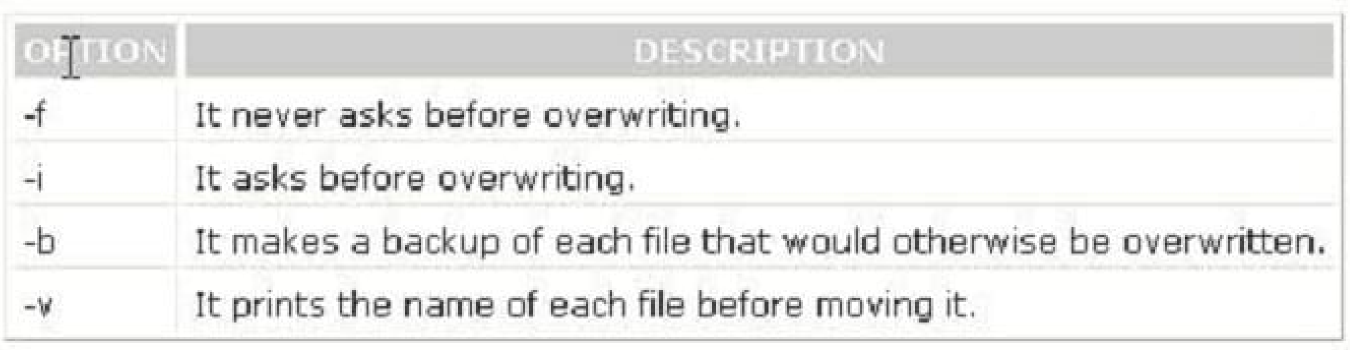
You will use the mv /foo /bar command to move the whole directory /foo to /bar. The mv command moves files and directories from one directory to another or renames a file or directory. mv must always be given at least two arguments.

The first argument is given as a source file.

The second argument is interpreted as the destination.

If destination is an existing directory, the source file is moved to that directory with the same name as the source. If the destination is any other directory, the source file is moved and/or renamed to that destination name.

Syntax : mv [options] source destination Some important options used with mv command are as follows:



OPTION	DESCRIPTION
-f	It never asks before overwriting.
-i	It asks before overwriting.
-b	It makes a backup of each file that would otherwise be overwritten.
-v	It prints the name of each file before moving it.

Answer: A is incorrect. The mv /bar /foo command will move the whole /bar directory to the /foo directory. Answer: B, D are incorrect. These are not valid Linux commands.

QUESTION 10

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 11

John works as a Network Auditor for XYZ CORP. The company has a Windows-based network. John wants to conduct risk analysis for the company.

Which of the following can be the purpose of this analysis? (Choose three)

A. To ensure absolute safety during the audit

B. To analyze exposure to risk in order to support better decision-making and proper management of those risks

C. To try to quantify the possible impact or loss of a threat

D. To assist the auditor in identifying the risks and threats

Correct Answer: BCD

There are many purposes of conducting risk analysis, which are as follows: To try to quantify the possible impact or loss of a threat To analyze exposure to risk in order to support better decision-making and proper management of those risks To support risk-based audit decisions To assist the auditor in determining the audit objectives To assist the auditor in identifying the risks and threats Answer: A is incorrect. The analysis of risk does not ensure absolute safety. The main purpose of using a risk-based audit strategy is to ensure that the audit adds value with meaningful information.

QUESTION 12

You work as the Network Administrator for XYZ CORP. The company has a Linux-based network. You are a root user on the Red Hat operating system. You want to see first five lines of the file /etc/passwd.

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

A. head -n 5 /etc/passwd

B. head 5 -n /etc/passwd

C. tail -n 5 /etc/passwd

D. head /etc/passwd

Correct Answer: A

The head -n 5 /etc/passwd command will show the first 5 lines of the file /etc/passwd.