GSNA Q&As

GIAC Systems and Network Auditor

Pass GIAC GSNA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/gsna.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Network mapping provides a security testing team with a blueprint of the organization.

Which of the following steps is NOT a part of manual network mapping?

A. Gathering private and public IP addresses

B. Collecting employees information

C. Performing Neotracerouting

D. Banner grabbing

Correct Answer: C

Using automated tools, such as NeoTraceroute, for mapping a network is a part of automated network mapping. part of manual network mapping. Network mapping is the process of providing a blueprint of the organization to a security testing

team. There are two ways of performing network mapping:

Manual Mapping: In manual mapping, a hacker gathers information to create a matrix that contains the domain name information, IP addresses of the network, DNS servers, employee information, company location, phone numbers, yearly

earnings, recently acquired organizations, email addresses, publicly available IP address ranges, open ports, wireless access points, modem lines, and banner grabbing details.

Automated Mapping: In automated mapping, a hacker uses any automated tool to gather information about the network. There are many tools for this purpose, such as NeoTrace, Visual traceroute, Cheops, Cheops-ng, etc. The only

advantage of automated mapping is that it is very fast and hence it may generate erroneous results.

QUESTION 2

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He is configuring the Apache Web server settings. He does not want the commands being used in the settings to be stored in the history.

Which of the following commands can he use to disable history?

A. history !!

B. set +o history

C. history !N

D. set -o history

Correct Answer: B

According to the scenario, John can use the set +o history command to disable history. Answer: D is incorrect. John

cannot use the set -o history command to accomplish his task. This command is used to enable disabled history.

Answer: A is incorrect. John cannot use the history !! command to accomplish his task. This command is used to see the most recently typed command.

Answer: C is incorrect. John cannot use the history !N command to accomplish his task. This command is used to display the Nth history command.

QUESTION 3

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.

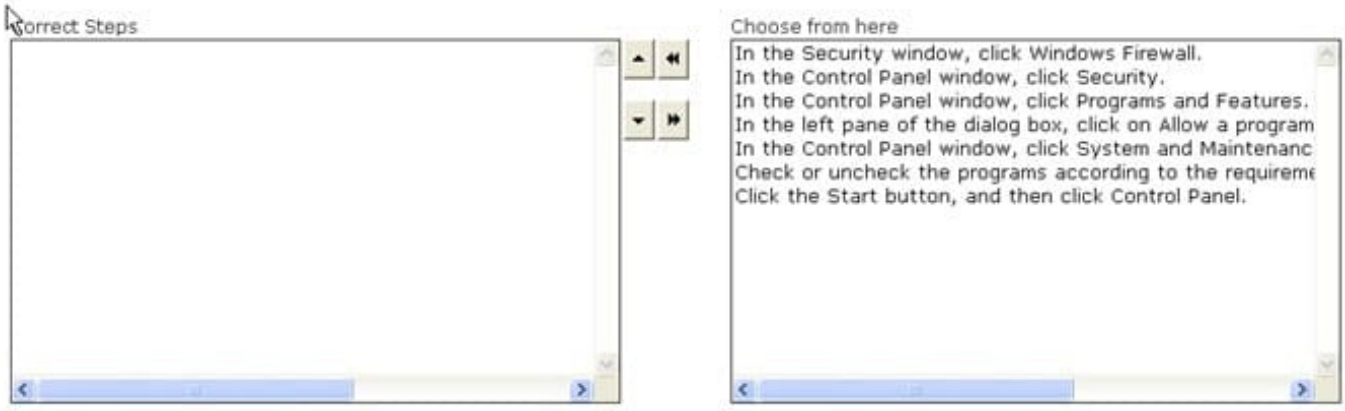
If the RST packet is received, it indicates that the port is closed. This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.

QUESTION 4

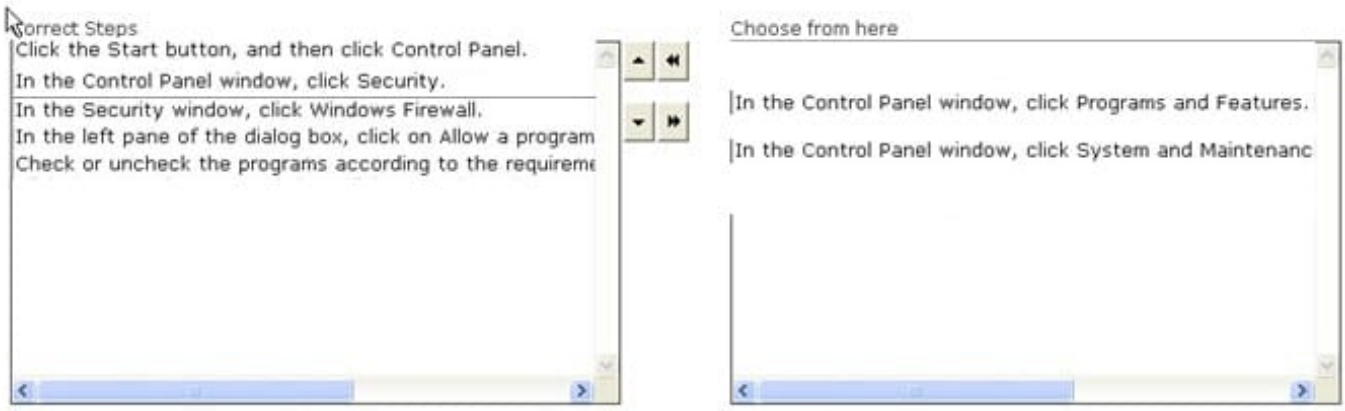
DRAG DROP

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:



Correct Answer:



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 5

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.