Free Questions for GSNA by certsinside

Shared by Moreno on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

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?

Options:

A- Setting up a honey pot

B- Vulnerability scanning

C- Setting up IDS

D- Port scanning

Answer:

B

Explanation:

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

Question 2

Question Type: **MultipleChoice**

In which of the following techniques does an attacker take network traffic coming towards a host at one port and forward it from that host to another host?

Options:

A- Snooping

B- UDP port scanning

C- Firewalking

D- Port redirection

Answer:

D

Explanation:

Port redirection is a technique by which an attacker takes network traffic coming towards a host at one port and redirects it from that host to another host. For example, tools such as Fpipe and Datapipe are port redirection tools that accept connections at any specified port and resend them to other specified ports on specified hosts. For example, the following command establishes a listener on port 25 on the test system and then redirects the connection to port 80 on the target system using the source port of 25.

```
C .\>fpipe -l 25 -s 25 -r 80 IP_address
```

Answer C 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 'TTL expired 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. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers

use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept

e-mail and other private communications. Sometimes, organizations also snoop their employees legitimately to monitor their use of

organizations' computers and track Internet usage.

Answer B 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 may be useful. Certain IDS and firewalls can detect UDP port scanning easily.

Question 3

Question Type: MultipleChoice

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?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- PsPasswd

B- WinSSLMiM

C- PsFile

D- UserInfo

Answer:

A, C, D

Explanation:

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.

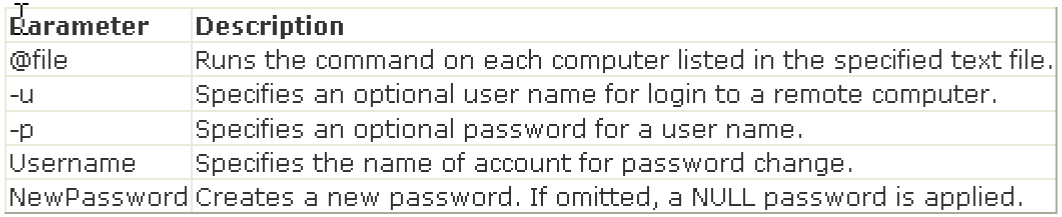
Id is the identifier of the file about which the user wants to display information.

-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]

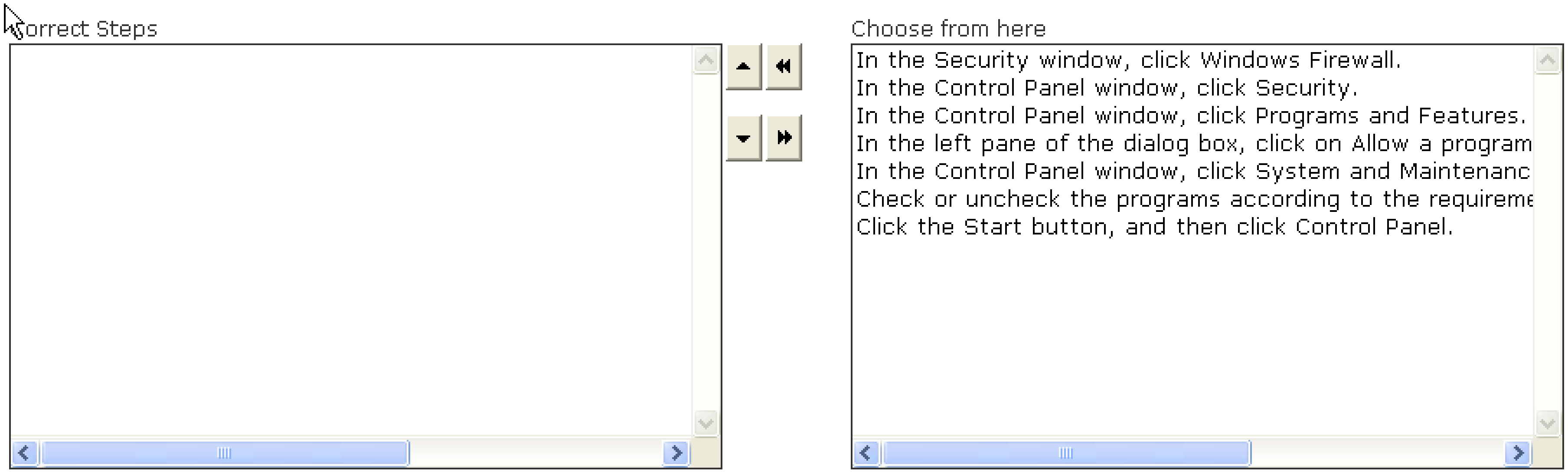


Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new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

Question 4

Question Type: OrderList

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?



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.

Answer:

[illegible]

Explanation:

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

Question Type: MultipleChoice

You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?

Options:

A- Implement WPA

B- Implement WEP

C- Don't broadcast SSID

D- Implement MAC filtering

Answer:

C

Explanation:

By not broadcasting your SSID some simple war driving tools won't detect your network. However you should be aware that there are tools

that will still detect networks that are not broadcasting their SSID.

Answer B and A are incorrect. While either encryption method is a good idea, they won't reduce the chances of a hacker stumbling

across your network.

Answer D is incorrect. While MAC filtering may help prevent a hacker from accessing your network, it won't keep him or her from finding

your network.

Question 6

Question Type: MultipleChoice

The routing algorithm uses certain variables to create a metric of a path. It is the metric that actually determines the routing path. In a metric,

which of the following variables is used to define the 'largest size' of a message that can be routed?

Options:

A- Load

B- MTU

C- Hop count

D- Bandwidth

Answer:

B

Explanation:

The routing algorithm uses certain variables to create a metric of a path. It is the metric that is actually used for path determination. Variables

that are used to create a metric of a path are as follows:

Hop count: It is the total number of routers that a data packet goes through to reach its destination.

Cost: It is determined by the administrator or calculated by the router.

Bandwidth: It is defined as the bandwidth that the link provides.

Maximum transmission unit (MTU): It is the largest message size that a link can route.

Load: It states the amount of work the CPU has to perform and the number of packets the CPU needs to analyze and make calculations on.

Question 7

Question Type: MultipleChoice

You work as a Database Administrator for Net Perfect Inc. 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?

Options:

A- SYSDBA

B- MDDBMS

C- Federated database system

D- Hierarchical database system

Answer:

B

Explanation:

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 8

Question Type: **MultipleChoice**

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?

Options:

A- UDP

B- RPC

C- IDLE

D- TCP SYN/ACK

Answer:

C

Explanation:

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 may be 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 9

Question Type: MultipleChoice

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?

Options:

A- Path MTU discovery (PMTUD)

B- AS Route Inference

C- AS PATH Inference

D- Firewalking

Answer:

C

Explanation:

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 and 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 'TTL expired 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

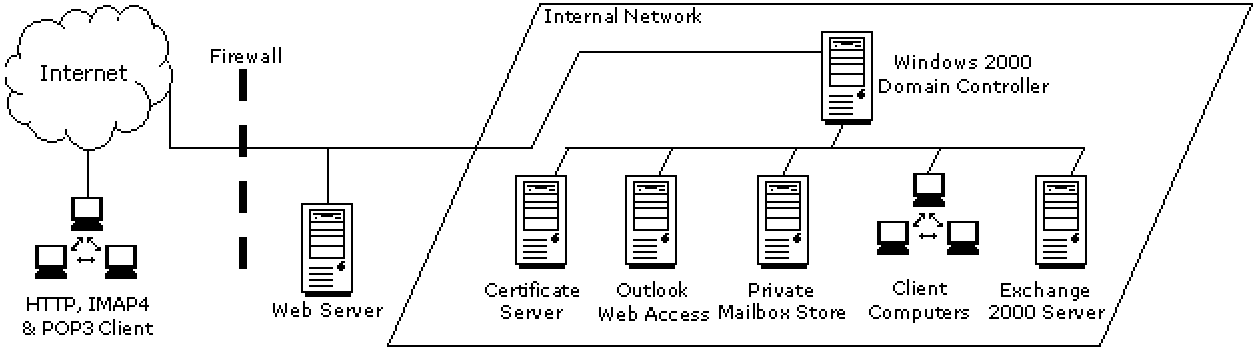
on the lower link, the OS will periodically reprobe to see if the path has changed and now allows larger packets. On Linux this timer is set by

default to ten minutes.

Question 10

Question Type: MultipleChoice

You work as an Exchange Administrator for SoftTech Inc. The network design of the company is given below:



Ensure fault tolerance amongst the servers.

Ensure the highest level of security and encryption for the Outlook Web Access clients.

What will you do to accomplish these goals?

Options:

A- Install one front-end Exchange 2000 server and continue to run Microsoft Outlook Web Access on the existing server.

Place the new server on the perimeter network.
Configure unique URLs for each server.
Configure Certificate Services.
Create a rule on the firewall to direct port 443 to the servers.

B- Install two front-end Exchange 2000 servers.
Place the new servers on the internal network and configure load balancing between them.
Configure Certificate Services.
Create a rule on the firewall to redirect port 443 to the servers.

C- Install two front-end Exchange 2000 servers.
Place the new servers on the perimeter network and configure load balancing between them.
Configure Certificate Services.
Create a rule on the firewall to redirect port 443 to the servers.

D- Install two Exchange 2000 servers.
Place the new servers on the perimeter network.
Configure unique URLs for each server.
Configure Certificate Services.
Create a rule on the firewall to direct port 443 to the servers.

Answer:

C

Explanation:

To ensure fault tolerance among the servers and to get the highest possible level of security and encryption for OWA clients, you must install two front-end Exchange 2000 servers. Place the new servers on the perimeter network and configure load balancing between them. To

enhance security, you should also configure Certificate Services and create a rule on the firewall to redirect port 443 to the servers.

The most secure firewall configuration is placing a firewall on either side of the front-end servers. This isolates the front-end servers in a

perimeter network, commonly referred to as a demilitarized zone (DMZ). It is always better to configure more than one front-end server to get

fault tolerance.