Free Questions for GSEC by dumpssheet

Shared by Joseph on 20-10-2022

For More Free Questions and Preparation Resources

Question 1

You work as a Network Administrator for NetTech Inc. To ensure the security of files, you encrypt data files using Encrypting File System (EFS).

You want to make a backup copy of the files and maintain security settings. You can backup the files either to a network share or a floppy

disk. What will you do to accomplish this?

Options:

A- Copy the files to a network share on an NTFS volume.

B- Copy the files to a network share on a FAT32 volume.

C- Place the files in an encrypted folder. Then, copy the folder to a floppy disk.

D- Copy the files to a floppy disk that has been formatted using Windows 2000 Professional.

Answer:

A

Explanation:

To make a backup copy of the files with encryption information, you will have to copy the files to a network share on an NTFS volume because

only NTFS file system can preserve encryption information.

Answer option B is incorrect. Copying the files on a FAT32 volume will not help because the encryption information will be lost. FAT32 does not

support encryption.

Answer options D and C are incorrect. Copying the files on floppy disk will not help, as the encryption information will be lost. This is because a

floppy disk cannot be formatted with NTFS file system.

Question 2

Question Type: **MultipleChoice**

Which of the following statements about DMZ are true?

Each correct answer represents a complete solution. Choose two.

Options:

A- It is the boundary between the Internet and a private network.

B- It is an anti-virus software that scans the incoming traffic on an internal network.

C- It contains company resources that are available on the Internet, such as Web servers and
FTP servers.

D- It contains an access control list (ACL).

Answer:

A, C

Explanation:

Demilitarized zone (DMZ) or perimeter network is a small network that lies in between the Internet and a private network. It is the boundary

between the Internet and an internal network, usually a combination of firewalls and bastion hosts that are gateways between inside

networks and outside networks. DMZ provides a large enterprise network or corporate network the ability to use the Internet while still

maintaining its security. The DMZ contains company resources that are available on the Internet, such as Web servers and FTP servers.

Question 3

Which of the following is generally practiced by the police or any other recognized governmental authority?

Options:

A- Spoofing

B- SMB signing

C- Wiretapping

D- Phishing

Answer:

C

Explanation:

Wiretapping is an act of monitoring telephone and Internet conversations by a third party. It is only legal with prior consent. Legalized

wiretapping is generally practiced by the police or any other recognized governmental authority.

Answer option B is incorrect. Server Message Block (SMB) signing is a security feature of Windows operating systems. SMB signing ensures

that the transmission and reception of files across a network are not altered in any way. As the traditional SMB authentication is vulnerable to

man-in-the-middle (MITM) attacks, the secure transmission of SMB traffic is required. Implementing mutual authentication SMB signing protects

a network from these attacks. The SMB signing feature adds digital signatures into SMB packets to strengthen SMB authentication.

Note: Enabling SMB signing on the network reduces the performance of the network because of the increased processing and network traffic

required to digitally sign each SMB packet.

Answer option A is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the

IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his

identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the

responses to be misdirected.

Answer option D is incorrect. Phishing is a type of scam that entice a user to disclose personal information such as social security number,

bank account details, or credit card number. An example of phishing attack is a fraudulent e-mail that appears to come from a user's bank

asking to change his online banking password. When the user clicks the link available on the e-mail, it directs him to a phishing site which

replicates the original bank site. The phishing site lures the user to provide his personal information.

Question 4

Question Type: **MultipleChoice**

You are responsible for technical support at a company. One of the employees complains that his new laptop cannot connect to the company wireless network. You have verified that he is entering a valid password/passkey. What is the most likely problem?

Options:

A- A firewall is blocking him.

B- His laptop is incompatible.

C- MAC filtering is blocking him.

D- His operating system is incompatible.

Answer:

C

Explanation:

The most likely problem is that, since this is a new laptop, the laptop's MAC address is not listed with the router, and is therefore blocked by

MAC filtering.

Answer option A is incorrect. Firewalls block certain types of traffic, but would not completely block an attempt to connect.

Answer options D and B are incorrect. Wireless networking is not operating system or hardware specific. Macintosh, Linux, Windows, all can

connect to the same wireless network.

Question 5

Your customer wants to make sure that only computers he has authorized can get on his Wi-Fi. What is the most appropriate security measure you can recommend?

Options:

A- A firewall

B- WPA encryption

C- WEP encryption

D- Mac filtering

Answer:

D

Explanation:

Mac filtering only allows computers that have their MAC address listed with the router to connect.

Answer options C and B are incorrect. Any encryption will be based on password authentication, not on filtering specific computers. Only MAC

filtering will do that.

Answer option A is incorrect. A firewall will not prevent people or computers from connecting to your Wi-Fi. It will block certain, unwanted

connections.

Question 6

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. You have configured a firewall on the network. A filter has been applied to block all the ports. You want to enable sending and receiving of emails on the network. Which of the following ports will you open?

Each correct answer represents a complete solution. Choose two.

Options:

A- 80

B- 25

C- 20

D- 110

Answer:

B, D

Explanation:

In order to enable email communication, you will have to open ports 25 and 110. Port 25 is used by SMTP to send emails. Port 110 is used by

POP3 to receive emails.

Answer option C is incorrect. By default, FTP uses port 20.

Answer option A is incorrect. By default, HTTP uses port 80.

Question 7

Question Type: **MultipleChoice**

Which of the following tools is used to configure, control, and query the TCP/IP network interface parameters?

Options:

A- NSLOOKUP

B- IPCONFIG

C- ARP

D- IFCONFIG

Answer:

D

Explanation:

The IFCONFIG tool is used to configure, control, and query the TCP/IP network interface parameters.

ifconfig is a command-line tool that is used for network interface management. Following are some of the options used with the command:

up: This option is used to activate the specified interface.

down: This option is used to deactivate the specified interface.

lo: This option is used to view the loopback interface.

The ifconfig command is also used to configure an interface.

Syntax:

ifconfig interface options

For example, to configure a Linux computer's first network interface with an IP address 200.200.200.123 and subnet mask 255.255.255.0, the

following command is used:

ifconfig eth0 200.200.200.123 netmask 255.255.255.0

Answer option C is incorrect. In Unix/Linux, the ARP command is used to manipulate the kernel's ARP cache. The ARP cache contains mapping

of the IP addresses and the hardware addresses of the Ethernet devices.

Answer option A is incorrect. NSLOOKUP is a tool for diagnosing and troubleshooting Domain Name System (DNS) problems. It performs its

function by sending queries to the DNS server and obtaining detailed responses at the command prompt. This information can be useful for

diagnosing and resolving name resolution issues, verifying whether or not the resource records are added or updated correctly in a zone, and

debugging other server-related problems. This tool is installed along with the TCP/IP protocol through the Control Panel.

Answer option B is incorrect. IPCONFIG is a command-line utility that displays the current TCP/IP configuration, such as IP address, subnet

mask, default gateway etc., of a networked computer. It refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System

(DNS) settings. Users can run IPCONFIG from the command prompt whenever they need to know the status of a computer's TCP/IP

configuration.