Question 1

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domain-based network. The company has two offices in different cities. The offices are connected through the Internet. Both offices have a Windows 2003 server named SERV1 and SERV2 respectively. Mark is required to create a secure connection between both offices. He configures a VPN connection between the offices using the two servers. He uses L2TP for VPN and also configures an IPSec tunnel. Which of the following will he achieve with this configuration?

Each correct answer represents a part of the solution. Choose two.

Options:

A) Encryption for the local files stored on the two servers

B) Highest possible encryption for traffic between the offices

C) Mutual authentication between the two servers

D) Extra bandwidth on the Internet connection

Answer:

B, C

Explanation:

Configuration of an L2TP VPN connection and an IPSec tunnel between the offices, will provide the highest possible encryption for traffic between the offices as well as mutual authentication between the two servers.

L2TP uses IPSec for data encryption. This will ensure the highest possible level of encryption for traffic between the two offices, as well as mutual authentication without any additional hardware or software.

Question 2

Question Type: MultipleChoice

What is the maximum cable segment length supported by a 10BaseT network?

Options:

A) 100 meters

B) 300 meters

C) 250 meters

D) 500 meters

E) 150 meters

Answer:

A

Explanation:

The most widely used Ethernet networks are 10BASE-T, 100BASE-TX, and 1000BASE-T (Gigabit Ethernet), running at 10 Mbit/s, 100 Mbit/s,

and 1000 Mbit/s (1 Gbit/s) respectively. These three standards all use the same connectors. Higher speed implementations nearly always

support the lower speeds as well, so that in most cases different generations of equipment can be freely mixed. They use 8 position modular

connectors, usually called RJ45 in the context of Ethernet over twisted pair. The cables usually used are four-pair or above twisted pair cable.

Each of the three standards support both full-duplex and half-duplex communication. According to the standards, they all operate over

distances of 'up to 100 meters'.

Question 3

You have a customer who wants to put wireless internet in his remote cabin. The cabin is many miles from any other building with internet connectivity or access points. What should you recommend?

Options:

A) DSL

B) FIOS connection

C) Satellite internet

D) Microwave connection

Answer:

C

Explanation:

Much like Satellite TV, Satellite internet does not require any physical connectivity and is available almost anywhere on the planet, since it uses orbiting satellites for connectivity. Speeds are not as fast as DSL, and the connectivity can be expensive.

Answer option D is incorrect. Microwave connections are very expensive and not available for residential internet use.

Answer options B and A are both incorrect. Both require local, physical connections and would not be available in a remote rural area.

Question 4

Which of the following terms refers to manual assignment of IP addresses to computers and devices?

Options:

A) Static IP addressing

B) Spoofing

C) APIPA

D) Dynamic IP addressing

Answer:

A

Explanation:

The Static IP addressing is the term used for manual assignment of IP addresses to computers and devices.

Answer option C is incorrect. Automatic Private IP Addressing (APIPA) is a Windows feature, which allows household users and small business

users to create a functional single subnet TCP/IP network without manually configuring the TCP/IP protocol or setting up a DHCP server.

Answer option D is incorrect. Dynamic IP addressing is used when IP addresses are assigned to computers and devices automatically by the

DHCP service or APIPA.

Answer option B 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.

Question 5

Which of the following statements regarding Secure Sockets Layer (SSL) are true?

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

Options:

A) SSL provides message integrity to prevent alteration to the message.

B) During SSL session, information is encrypted to prevent unauthorized disclosure.

C) SSL can process credit cards.

D) SSL can support 128-bit encryption.

Answer:

A, B, D

Explanation:

Secure Sockets Layer (SSL) is a protocol used to transmit private documents via the Internet. SSL uses a combination of public key and symmetric encryption to provide communication privacy, authentication, and message integrity. Using the SSL protocol, clients and servers can

communicate in a way that prevents eavesdropping and tampering of data on the Internet. Many Web sites use the SSL protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:. By default, SSL uses port 443 for secured communication.

Answer option C is incorrect. SSL can only secure the communication transport. Processing of credit cards cannot be done by SSL.

Question 6

Question Type: MultipleChoice

Which of the following is not an encryption technology?

Options:

A) Blowfish

B) KILL

C) 3DES

D) MD5

Answer:

B

Explanation:

KILL is a command used to terminate a specified process.

Answer options A, C, and D are incorrect. Blowfish, 3DES, and MD5 are encryption technologies used to secure the communication between computers on the network.

Question 7

Question Type: MultipleChoice

The /cat/etc/passwd file on a client computer contains the following entry:

Martha:x:::::bin/false

Which of the following is true for Martha?

Options:

A) Martha's password is x.

B) Martha has full access on the computer.

C) Martha has limited access on the computer.

D) Martha has been denied access on the computer.

Answer:

D

Explanation:

In order to deny access to a user account, an invalid shell such as /bin/false should be assigned for the user account in the /etc/passwd file. When an invalid shell is assigned to a user account, a user cannot use the computer. You can take the following steps to deny access for a user to the computer:

1.Edit the /etc/passwd file and make the appropriate changes.

2.Use the -s switch with the USERMOD command.

3.Use CHSH -s /bin/false <user name> command.

Alternatively, you can use the USERMOD -l <user name> command at the command prompt to lock the user account.

To Get Premium Files for GSEC Visit

For More Free Questions Visit