CYBS 7357 Lab 08 Quiz

\* Answers are highlighted in yellow

1. You are configuring a VPN client on a Windows 2016 server using IPsec to create a secure tunnel to a L2TP\IPsec server. Which of the following statements is true?

a. L2TP does not perform encryption.

b. L2TP performs encryption.

c. L2TP works only for IP networks, not non-IP networks.

d. L2TP works only for non-IP networks, not non-IP networks.

2. Which of the following statements is NOT true regarding VPNs?

a. VPN tunnels are not 100% secure.

b. A client using a VPN tunnel is vulnerable to inline attacks.

c. A VPN does not mask a client's IP address.

d. The code of an inline attack can reveal a client system's IP address.

3. Which Windows feature do you use to create a VPN client?

a. Internet Options

b. Windows Firewall

c. Certificate Manager

d. Network and Sharing Center

4. When creating a VPN client in Windows, which of the following is NOT an option when selecting the type of VPN?

a. Point to Point Tunneling Protocol (PPTP)

b. Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

c. IKEv2

d. Extensible Authentication Protocol (EAP)

5. What is split tunneling?

a. Using two security protocols for a single VPN

b. Configuring clients to access a public network through a VPN while maintaining access to local resources at the same time, using the same or different network connections

c. Using two different VPN connections to access the same resources

d. Configuring clients to access public networks and local resources through two different VPNs

6. You just set up a VPN client on a Windows computer to work with a pfSense VPN server. You now want to make an IPsec connection to the server using IKEv2. What is the first step you must take?

a. Download and import a certificate file from the pfSense system.

b. Authenticate with the pfSense server.

c. Revoke a certificate from the pfSense server certificate authority (CA).

d. Add a route to the connecting IP address of the IPsec firewall.

7. In Windows, what is Trusted Root Certification Authorities?

a. A key exchange framework

b. The name of a default VPN connection

c. A certificate store

d. A folder for protocols used in secure VPN connections

8. Which of the following statements is NOT true of Secure Shell (SSH)?

a. SSH encrypts files during the file transfer process.

b. You can use SSH with FTP.

c. An attacker who gains access to SSH encryption keys can decrypt and read content.

d. An attacker who gains access to SSH encryption keys cannot decrypt and read content.

9. When configuring a VPN connection from a client to a server, what does the *route add <a.b.c.d> mask 255.255.255.0 <w.x.y.z>* command do?

a. Add a route to the client's internal firewall.

b. Add a route to the connecting IP address of the IPsec firewall.

c. Masks the IP address of the IPsec firewall.

d. Masks the source's network address.

10. What is the 255.255.255.255 address typically associated with?

a. VPN client IP address

b. VPN server IP address

c. A mobile device network adapter

d. Subnet mask

11. Which of the following statements is true of split tunnel configurations?

a. Clients do not keep local traffic on their own network.

b. Clients cannot route IPsec traffic through the VPN tunnel.

c. The configuration is optimal for performance.

d. The configuration is more secure than specifying a network address.

12. In Lab 8, you removed a split tunnel configuration from an IPsec VPN adapter. What was the result?

a. No traffic was allowed to pass through the IPsec tunnel, making the connection faster but less secure.

d. No traffic was allowed to pass through the IPsec tunnel, making the connection faster and more secure.

c. All traffic was forced through the IPsec tunnel, making the connection faster but less secure.

d. All traffic was forced through the IPsec tunnel, making the connection slower but more secure.

13. Before analyzing a network packet file in Wireshark in Lab 8, you created a filter. What did the filter do?

a. Deleted certain types of traffic from the packet file

b. Displayed only certain types of traffic in a packet file

c. Displayed all hex data for a packet file

d. Added certain types of traffic to the packet file

14. Which type of files are most appropriate to exchange via anonymous FTP?

a. Code files for a software manufacturer's application

b. A company's sales data

c. A company's marketing literature

d. Customer database files

15. Of the following, what is a packet retransmission most likely to indicate?

a. An intentional packet injection

b. A new server certificate

c. An incorrect 111user password

d. An anonymous connection

16. In Wireshark, which of the following is true of the Hex pane?

a. It displays packet `information but not file names or file paths.

b. It displays the same information as the Frame Details pane but in an easier-to-read format.

c. It can display file contents in hexadecimal only.

d. It can display file contents in hexadecimal and clear text.

17. How can FTP be made more secure?

a. Encrypt files before transferring them.

b. Decrypt files before transferring them.

c. Use a graphical user interface (GUI) rather than a command-line interface.

d. Use a command-line interface rather than a graphical user interface (GUI).

18. Secure Shell (SSH) protocol replaces which older, insecure protocol?

a. L2TP

b. Telnet

c. FTP

d. IPsec

19. If Secure Shell (SSH) is configured to use asymmetrical encryption, which of the following statements is true?

a. One key is required when sending data.

b. Two keys are required when sending data.

c. One key and a secure protocol are required to send data.

d. Two keys and Telnet are required to send data.

20. What is ISAKMP?

a. A secure certificate authority (CA)

b. A file transfer application

c. A protocol used to establish tunnels and cryptographic keys

d. A protocol used for authorization of VPN users

NAME:

Natnael kebede