1. True or false? TCP window sizes are static, and do not decrease or increase after the TCP connection has been negotiated.

A. True
B. False

Correct answer: B.

Explanation: TCP window sizes do change to help facilitate a more efficient connection. The larger the window size, the fewer acknowledgements need to be sent. Basically, because TCP notices that there hasn't been significant packet loss, it know it can trust the connection and send more data with fewer acknowledgements.

2. Your firm is calculating the given risk for some of their I.T. systems. If the Single Loss Expectancy of a system is $2,000 and the Annual Rate of Occurrence is 6, what's the most money that should be spent trying to mitigate the risk in a year's time?

A. $2,000
B. $6,600
C. $12,000
D. $20,000
E. None of the above.

Correct answer: C.

Explanation: ALE = SLE * ARO. In this case, we only need to multiply the two numbers together to find the optimal threshold of resources that should be spent securing the system. Otherwise, we'll end up spending more than is necessary, which is a misappropriation of an already tight budget.

3. Put the following encryption mechanisms in order of security, starting with the weakest encryption and ending with the strongest: Blowfish, L2TP, L2TP/IPSec, SSL, and PPTP. Choose the best answer.

A. Blowfish, SSL, L2TP/IPSec, PPTP, L2TP.
B. L2TP, PPTP, L2TP/IPSec, SSL, Blowfish.
C. SSL, PPTP, L2TP/IPSec, L2TP, Blowfish.
D. L2TP, Blowfish, L2TP/IPSec, SSL, PPTP.
E. None of the above.

Correct answer: B.

Explanation: L2TP is inherently insecure because it does not offer encryption on it's own, so it starts the list off as the least secure. Next up is PPTP which is incredibly weak and easily crackable, so it shouldn't be used with exception to very special circumstances. Next is L2TP/IPSec, which does provide encryption. Then comes SSL, which most commonly uses 256-bit encryption. Last but not least is Blowfish, which is the most flexible, but can use 448-bit encryption.

4. Which of the following is true regarding TCP and UDP connections? Select all that apply.

A. TCP is much more secure than UDP because, in addition to windowing and acknowledgement features, the protocol has a built in encryption protocol.
B. UDP is much more secure than TCP because, in addition to windowing and acknowledgement features, the protocol has a built in encryption protocol.
C. Both TCP and UDP were designed with internal mechanisms that facilitate encryption, so they are equally secure.
D. TCP and UDP are equally insecure because neither protocol has its own means to encrypt data.
E. None of the above.

Correct answer: D.

Explanation: TCP and UDP are Transport protocols, and do not have their own methods of encrypting data. If you wanted to encrypt the payloads of TCP and UDP traffic, you'd need to rely on a a different protocol such as IPSec (among others).

5. What is it called when a term collects information and data, which creates an audit trail, that can be used to monitor, manage, and review network components? Choose the best answer.

A. Data mining
B. Logging
C. Capturing
D. Auditing
E. None of the above

Correct answer: B.

Explanation: This is the simplest definition of logging. The others answers are incorrect.

6. On a Linux machine, what's the quickest, easiest, and most efficent way of viewing which ports and services are active? Choose the best answer.

A. ipchains
B. ls -o ports
C. ps aux
D. netstat
E. cmd
F. None of the above

Correct answer: D.

Explanation: Netstat is the easiest way to view open ports and services, and can be run from the terminal window.

7. Which of the following protocols runs on port 990? Choose the best answer.

A. Active FTP
B. Passive FTP
C. SSH
D. FTPS
E. Telnet
F. DNS
G. None of the above

Correct answer: D.

Explanation: Secure FTP runs on port 990 by default, though it can be run on port 21 as well.

8. Which of the following are true of block ciphers and stream ciphers? Select all that apply.

A. Stream ciphers typically encrypt data in small increments, such as one byte at a time. Block ciphers, however, can deal with larger chunks of data as a single unit of encryption, such as 64-bits.
B. Block ciphers typically encrypt data in small increments, such as one byte at a time. Stream ciphers, however, can deal with larger chunks of data as a single unit of encryption, such as 64-bits.
C. Block ciphers are only used to encrypt audio data.
D. Stream ciphers are only used to encrypt audio data.
E. None of the above.

Correct answer: A.

Explanation: Interestingly enough, block ciphers can also behave like stream ciphers, in that they can encrypt data one byte at a time. However, it's more common for a block cipher to encrypt several bytes of data at a time as opposed to a byte-by-byte encryption method like a stream cipher.

9. What type of assessment would you be making if you determined that the probability of a certain security threat was “medium?” Choose the best answer.

A. Qualitative
B. Quantitative
C. SWOT
D. Baseline
E. None of the above

Correct answer: A.

Explanation: Because you weren't able to quantify the risk with a number, you would be making a qualitative risk assessment.

10. True or false? In crytographic functions, such as those used in AES-256, there are multiple combinations of bits that can act as valid keys for encryption and decryption, though never more than 2^4 valid combinations.

A. True
B. False

Correct answer: B.

Explanation: Cryptographic functions are built on very advanced and complex mathematical formulas that only allow for a single key to encrypt the data. Otherwise, there could be multiple keys with the ability to decrypt data, which would defeat the purpose of the encryption algorithm.

11. Which of the following options will help preserve the availability of data? Choose the two best answers.

A. Firewalls
B. Physical access control
C. User and group policies
D. Anti-static carpet
E. None of the above

Correct answer: B, D.

Explanation: Firewalls, as well as user and group policies, while both essential to a network, will not preserve data over time.

12. Your firm lacks the budget to implement physical security systems such as magnetic keycards. What type of attacks are your systems most susceptible to? Choose the best answer.

A. Virus-based attacks
B. Scripting-based attacks
C. Social engineering
D. Password attacks
E. None of the above

Correct answer: C.

Explanation: Because the systems aren't physically secured, it would be possible for an attacker to leverage social engineering to gain access to the hardware, and potentially steal data or harm the device.

13. On a Linux system, how would you go about finding the default gateway's IP address, as well as any other layer 3 configurations concerning where data is sent? Select all that apply.

A. Use the traceroute command from the terminal to see what path data takes through a network.
B. Open the Network and Sharing Center.
C. Issue the **ipchains** command.
D. Open a terminal and issue the **route** command to view the contents of the routing table.
E. None of the above.

Correct answer: A, D.

Explanation: Though D is the best answer, the instructions asked to select all that apply. Traceroute will show you where ICMP traffic is destined to, and on most networks, this will travel through the default gateway. However, in some instances, there may be special routes for certain types of traffic that meet various criteria, so remember to use the **route** command.

14. After performing a packet capture on a router's network interface, you notice an unusually large amount of traffic on ports 160 and 161. What does this indicate? Choose the best answer.

A. There is a Brute Force password attack making login attempts on ports 160 and 161.
B. There is a DDoS attack on ports 160 and 161.
C. The LDAP server is simply downloading and installing the latest patches and updates.
D. This is normal, because ports 160 and 161 are used for SNMP.
E. None of the above.

Correct answer: D.

Explanation: SNMP runs on ports 160 and 161.

15. True or false? Email is inherently secure by default.

A. True
B. False

Correct answer: B.

Explanation: Email is insecure by default, and needs to be secured with encryption technologies.

16. Which of the following correctly describes the port number used by the Cisco-based routing protocol EIGRP?

A. 179
B. 220
C. 1004
D. 54
E. None of the above

Correct answer: E.

Explanation: EIGRP doesn't operate over TCP or UDP connections, and instead runs directly over IP. As such, it doesn't have a port number. Instead, it use IP protocol number 88.

17. Your I.T. department needs a way to securely monitor and manage hundreds of networking devices and servers. Which protocol should you use? Select all that apply.

A. SSH
B. SNMPv3
C. SNMPv2
D. SNMPv1
E. SNMPv4
F. BGP
G. SMTP
H. SMTPv2
I. EIGRP
J. None of the above

Correct answer: B.

Explanation: The key here is that the firm needs a *secure* way to manage devices. SNMPv3 (Simple Network Management Protocol) adds both authentication *and* encryption to the existing SNMP framework.

18. If you wanted to download a configuration file to update the operating system code on a router, switch, or other network device, which protocol would you use? Choose the best answer.

A. TFTP
B. FTPS
C. FTP
D. SSH
E. None of the above

Correct answer: A.

Explanation: It's pretty standard practice to use TFTP to download system configuration files and router code to upgrade a system. Even though it doesn't provide encryption, the server is typically on the same LAN.

19. Which of the following accurately describes the difference between PPP and PPTP? Choose the best answer.

A. PPTP is often used on point-to-point WAN links.
B. PPP offers strong encryption, though PPTP only offers weak encryption.
C. PPP offers weak encryption, though PPTP offers strong encryption.
D. PPP offers no encryption, though PPTP only offers weak encryption.
E. None of the above.

Correct answer: D.

Explanation: PPP is frequently used on WAN links to setup a connection between to remote interfaces. Typically, it's common to find that PPP is implemented on network subnets with a /30 subnet mask – but it doesn't provide encryption. PPTP is a security protocol developed by a Microsoft consortium that only offers weak encryption.

20. Which of the following accurately describe vulnerabilities found in email systems? Select all that apply.

A. Unencrypted emails can easily be captured with sniffing software in plain text.
B. Emails are stored in an unencrypted format by default on most mail servers.
C. Emails can easily be tricked into being sent to the wrong server with DNS-based attacks.
D. Emails are one of the most common mediums for spreading viruses and malware.
E. None of the above.

Correct answer: A, B, C, D.

Explanation: All of the answers list some of the largest security problems regarding emails.