

1. Which of the following is a network diagnostic tool that monitors and records network information?
 - A. Online monitor
 - B. Downtime report
 - C. Help desk report
 - D. Protocol analyzer

2. Which of the following would best ensure continuity of a wide area network (WAN) across the organization?
 - A. Built-in alternative routing
 - B. Complete full system backup daily
 - C. A repair contract with a service provider
 - D. A duplicate machine alongside each server

3. Which of the following best reduces the ability of one device to capture the packets that are meant for another device?
 - A. Hubs
 - B. Switches
 - C. Routers
 - D. Firewalls

4. When reviewing the configuration of network devices, an IS auditor should first identify:
 - A. the good practices for the types of network devices deployed.
 - B. whether components of the network are missing.
 - C. the importance of the network devices in the topology.
 - D. whether subcomponents of the network are being used appropriately.

5. Which of the following network components is primarily set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?
 - A. Firewalls
 - B. Routers
 - C. Layer 2 switches
 - D. Virtual local area networks (VLANS)

6. A company is implementing a Dynamic Host Configuration Protocol (DHCP). Given that the following conditions exist, which represents the greatest concern?
 - A. Most employees use laptops.
 - B. A packet filtering firewall is used.
 - C. The IP address space is smaller than the number of PC's.
 - D. Access to a network port is not restricted.

7. During a review of intrusion detection logs, an IS auditor notices traffic coming from the Internet, which appears to originate from the internal IP address of the company payroll server. Which of the following malicious activities would most likely cause this type of result?

- A. A denial-of-service (DoS) attack
 - B. Spoofing
 - C. Port scanning
 - D. A man-in-the middle attack
8. Why are switched infrastructures safer environments than routed networks?
- A. It is more difficult to sniff traffic since the computers have virtual private connections.
 - B. They are just as safe as nonswitched environments.
 - C. The data link encryption does not permit wiretapping.
 - D. Switches are more intelligent than bridges and implement security mechanisms.
9. Which of the following protocols is considered connection-oriented?
- A. IP
 - B. ICMP
 - C. UDP
 - D. TCP
10. Which of the following shows the layer sequence as layers 2, 5, 7, 4, and 3
- A. Data link, session, application, transport, and network
 - B. Data link, transport, application, session, and network
 - C. Network, session, application, network, and transport
 - D. Network, transport, application, session, and presentation
11. Systems that are built on the OSI framework are considered open systems. What does this mean?
- A. They do not have authentication mechanisms configured by default.
 - B. They have interoperability issues.
 - C. They are built with internationally accepted protocols and standards so they can easily communicate with other systems.
 - D. They are built with international protocols and standards so they can choose what types of systems they will communicate with.
12. Which of the following protocols work in the following layers: application, data link, network, and transport?
- A. FTP, ARP, TCP, and UDP
 - B. FTP, ICMP, IP, and UDP
 - C. TFTP, ARP, IP, and UDP
 - D. TFTP, RARP, IP, and ICMP
13. One of the primary steps in a quantitative risk analysis is to determine the annualized loss expectancy (ALE). How is the ALE calculated?
- a. Single loss expectancy / Frequency per year
 - b. Asset value X 2.8
 - c. Single loss expectancy X Frequency per year

- d. Asset value + (Single loss expectancy / Frequency per year)
14. What takes place at the data link layer?
- A. End-to-end connection
 - B. Dialog control
 - C. Framing
 - D. Data Syntax
15. What takes place at the session layer?
- A. Dialog control
 - B. Routing
 - C. Packet sequencing
 - D. Addressing
16. Which best describes the IP protocol?
- A. A connectionless protocol that deals with dialog establishment, maintenance, and destruction
 - B. A connectionless protocol that deals with the addressing and routing of packets
 - C. A connection-oriented protocol that deals with the addressing and routing of packets
 - D. A connection-oriented protocol that deals with sequencing, error detection, and flow control
17. Which control is the BEST way to ensure that the data in a file have not been changed during transmission?
- a. Reasonableness check
 - b. Parity bits
 - c. Hash values
 - d. Check digits
18. A year ago when Sam carried out a risk analysis, he determined that the company was at too much of a risk when it came to potentially losing trade secrets. The countermeasures his team implemented reduced this risk, and Sam determined that the annualized loss expectancy of the risk of a trade secret being stolen once in a hundred-year period is now \$400. What is the associated single loss expectancy value in this scenario?
- a. \$65,000
 - b. \$400,000
 - c. \$40,000
 - d. \$4,000