

## Management 414: SANS CISSP® 10 Domains +5 QUIZ - Domain 2

1. Which of the following topologies is most widely used today because of its scalability and fault tolerance?
  - a) Ring Topology
  - b) Loop Topology
  - c) Star topology
  - d) Bus Topology
2. When examining an IP packet header, at which byte would find the Protocol field?
  - a) Byte 11.
  - b) Byte 9
  - c) Byte 8
  - d) Byte 10
3. Which of the following statements is FALSE?
  - a) 802.11b supports up to 2.4 Mbps at 11 GHz
  - b) 802.11a supports up to 54 Mbps at 5 GHz
  - c) 802.11g supports up to 54 Mbps at 2.4 GHz
  - d) 802.11b supports up to 11 Mbps at 2.4 GHz
4. Which of the following is NOT a WAN communication technology?
  - a) Token Ring
  - b) Frame relay
  - c) Voice over IP
  - d) Dedicated lines
5. If I were implementing a 16 Mbps network to the exact specifications provided to me, which cable category would be most appropriate to use?
  - a) Category 4
  - b) Category 5
  - c) Category 3
  - d) Category 2
6. Which network component should be used when you are concerned with internal network sniffing?
  - a) A network hub
  - b) A network bridge
  - c) A network hop
  - d) A network switch

## Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 2

7. Which of the following is the correct binary representation of the decimal number 252?
  - a) 1111 1110
  - b) 1111 1100
  - c) 11101110
  - d) 0111 1111
8. Which of the following network layer protocols provides authentication and confidentiality services by encapsulating standard IP communication, independent of the application generating the traffic?
  - a) SET
  - b) PEM
  - c) IPSec
  - d) S/MIME
9. Which of the following is the fundamental protocol of the internet?
  - a) TCP
  - b) UDP
  - c) HTTP
  - d) IP
10. Which of the following binary, decimal, protocol combinations is correct?
  - a) 0000 0000, 0, ICMP
  - b) 0010 0001, 17, UDP
  - c) 0000 0011, 6, TCP
  - d) 0000 0110, 6, TCP
  - e) 1111 0001, 1, ICMP
11. Which of the following allows you to uniquely identify a complete connection among all other connections on the internet?
  - a) A socket
  - b) A source and destination IP address
  - c) A source and destination port number
  - d) A hostname
12. When you encounter two NICs with the same embedded MAC address, what should you do?
  - a) Select a different MAC address from those available.
  - b) Increment one of the duplicate MAC addresses by 2.
  - c) You will not encounter this situation, MAC addresses are unique.
  - d) Reset both NICs in order to resolve the MAC address conflict.
13. Which of the following layers of the Open Systems Interconnect (OSI) model interacts with your information and prepares it to be transmitted across the network?

## Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 2

- a) Network Layer
  - b) Transport Layer
  - c) Presentation Layer
  - d) Application Layer
14. What is the current, widespread implemented solution to network address congestion and conservation?
- a) IPv4
  - b) CIDR
  - c) IPv5
  - d) IPv7
15. Which of the following is a helpful network path troubleshooting tool that shows each of the nodes from a local machine to a destination?
- a) Ping
  - b) TCP
  - c) Tripwire
  - d) Traceroute
16. Which of the following is NOT a security implication of using VPNs?
- a) VPN communications bypass firewalls, IDS, virus scanners and web filters because of encryption.
  - b) VPN communications require a certain level of trust that home client computers are adequately protected.
  - c) VPN communications are slower because data must be encrypted and decrypted and the endpoints.
17. During which team's creation would one develop escalation, resolution, post-incident follow-up and reporting procedures?
- a) Pattern Matching Team (PMPT)
  - b) Profile Team (PT)
  - c) Protocol Behavior Team (PBT)
  - d) Computer Incident Response Team (CIRT)
18. What is it called when data is encrypted into ciphertext, transmitted over the Internet and then decrypted at the destination into the original cleartext?
- a) Transmission Control Protocol (TCP)
  - b) File Transfer Protocol (FTP)
  - c) Data obfuscation
  - d) Virtual Private Network (VPN)

## Management 414: SANS CISSP® 10 Domains +5 QUIZ -- Domain 2

19. Which of the following is NOT one of the primary principles associated with securing enterprise and telecommuting remote connectivity?
- a) Securing external connections
  - b) Remote access authentication systems
  - c) Ensuring high connection speeds
  - d) Remote node authentication protocols
20. Which of the following is an example of the Telecommunications and Network Security domain that directly affects the Information Security tenet of availability?
- a) VPN
  - b) IPSEC
  - c) OOP
  - d) RAID
21. Which RAID Level stripes data across all disks but provides NO redundancy?
- a) RAID Level 0
  - b) RAID Level 1
  - c) RAID Level 2
  - d) RAID Level 5
22. Which RAID Level mirrors each drive to an equal drive partner, which is continually being updated with current data?
- a) RAID Level 3
  - b) RAID Level 5
  - c) RAID Level 1
  - d) RAID Level 7
23. Which RAID Level consists of bit-interleaved data on multiple disks?
- a) RAID Level 2
  - b) RAID Level 1
  - c) RAID Level 5
  - d) RAID Level 7
24. Which RAID Level writes parity info to the next available drive rather than a dedicated drive using an interleave parity?
- a) RAID Level 0
  - b) RAID Level 5
  - c) RAID Level 3
  - d) RAID Level 2
25. Which RAID Level Allows the drive array to continue to operate if any disk or any path to any disk fails?
- a) RAID Level 6
  - b) RAID Level 4

**Management 414: SANS CISSP® 10 Domains +S QUIZ -- Domain 2**

- c) RAID Level 5
  - d) RAID Level 7
26. What is it called when you take the concept of RAID 1 (mirroring) and applies it to a pair of servers?
- a) Binding Server Implementation
  - b) Redundant Server Implementation
  - c) Daisy Chain Server Implementation
  - d) Duplicate systems
27. Which type of backup makes a complete backup of every file on the server every time it is run?
- a) Partial Backup
  - b) Full Backup
  - c) Incremental Backup
  - d) Differential Backup
28. Which type of backup copies only files that have recently been added or changed since the last full or incremental backup and ignores any other backup set?
- a) Partial Backup
  - b) Incremental Backup
  - c) Full Backup
  - d) Differential Backup
29. Which type of backup copies only files that have changed since a full backup was last performed?
- a) Partial Backup
  - b) Full Backup
  - c) Incremental Backup
  - d) Differential Backup
30. Of the following choices, which best describes when the IDS sets off an alert for normal traffic
- a) True negative
  - b) False positive
  - c) False negative
  - d) True positive

**Management 414: SANS CISSP® 10 Domains +S QUIZ -- Domain 2**

31. Which step during Incident Handling involves updating the disaster recovery plan, providing checklists and procedures, and providing training?
- a) Lessons Learned
  - b) Recovery
  - c) Preparation
  - d) Eradication
32. Which of the following choices is NOT one of the six Incident Handling steps?
- a) Infiltrate
  - b) Lessons Learned
  - c) Recovery
  - d) Eradication
33. Which of the following network devices blocks broadcast traffic?
- a) Hub
  - b) Switch
  - c) Router
  - d) Bridge
34. Which of the following layers of the Open Systems Interconnect (OSI) model connects the physical part of the network with the abstract part?
- a) Data Link Layer
  - b) Network Layer
  - c) Presentation Layer
  - d) Application Layer
35. Which of the following layers of the Open Systems Interconnect (OSI) model handles the establishment and maintenance of connections between systems?
- a) Network Layer
  - b) Presentation Layer
  - c) Session Layer
  - d) Transport Layer