Students who wish to take the following SANS course:

Security 503 – Intrusion Detection In-Depth

should note that these courses require pre-existing knowledge of basic concepts relating to the TCP/IP protocol suite.

We encourage students who consider attending any of the courses listed above to test their understanding of prerequisite material by taking the following quiz.

Read the following questions, note your answers, and check your results against the answers provided at the end. While this quiz alone cannot completely measure a student's readiness, it should be used as a guide to estimate your preparedness to help you get the most out of your SANS course. There is no minimum score prerequisite; though if you are not familiar with most of the concepts in the questions, you may find the course particularly challenging.

<u>Quiz</u>

1. How many bits in a byte?
    a. 8
    b. 16
    c. 4
    d. 2
2. The maximum decimal value that can be represented in a byte is:
    a. 256
    b. 255
    c. 128
    d. 127
3. What is a MAC address?
    a. The IP address of the host
    b. The embedded IP protocol
    c. The hardware address assigned to the network card/interface
    d. The embedded protocol port address
4. What does the Address Resolution Protocol (ARP) do?
    a. Resolves a known IP address with a MAC address
    b. Resolves a known MAC address with an IP address
    c. Resolves a known network interface name with a hardware address
    d. Resolves a known MAC address with a vendor type
5. A server port of UDP or TCP 53 is typically associated with what service?
    a. HTTP
    b. DNS
    c. FTP
    d. RPC
6. How does a host that has sent TCP data know that the data was received?
    a. A TCP acknowledgement is sent from the receiver
    b. An ICMP echo reply is sent from the receiver
    c. An incremented TCP sequence number is sent from the receiver
    d. A SYN/ACK is sent from the receiver
7. Which of the following best characterizes TCP versus UDP (in most cases)?
    a. TCP is less reliable and quicker
    b. TCP is slower, more reliable, and requires more overhead
    c. TCP is faster, more reliable, and more streamlined
    d. TCP is less reliable and connection-oriented
8. Which of the following best characterizes ICMP
    a. It is used to communicate error conditions
    b. It is used for connection-oriented communications
    c. It is used for reliable communications
    d. It is used for client/server communications

9. A TCP flag of RESET indicates:
    a. An intention to open a new TCP connection
    b. An intention to gracefully close and acknowledge the termination of both sides of the connection
    c. An intention to abort a TCP connection
    d. An intention to close the connection after all in-transit data is received
10. TCP typically begins a session with:
    a. The three-way handshake of client to server with SYN set, the server response of SYN/ACK, and the client acknowledgement of ACK
    b. The three-way handshake of server to client with SYN set, the client response of SYN/ACK, and the server acknowledgement of ACK
    c. TCP is not connection oriented so no handshake is required
    d. A handshake consisting of the client request to the server with SYN set and a server response of a SYN
11. A value of 6 in the protocol field of the IP header represents:
    a. An embedded protocol of ICMP follows the IP header
    b. An embedded protocol of UDP follows the IP header
    c. An embedded protocol of TCP follows the IP header
    d. An embedded protocol of TCP precedes the IP header
12. IP fragmentation occurs when:
    a. The receiver is not ready for all the data from the sender
    b. When there are more bytes in the IP packet than the size of the Maximum Transmission Unit of all links from sender to receiver
    c. When there are more bytes in the IP packet than the size of the receiving TCP window
    d. When there are more bytes in the payload that follows the IP header than the size of the Maximum Transmission Unit of all links from the sender to receiver
13. Some of the fields in an IPv4 packet that are used by the receiver to **reassemble** associated fragments are:
    a. The IP identification field to identify all associated fragments, the More Fragment bit to indicate whether or not more fragments follow the current one, and the fragment offset to indicate where a particular fragment falls in relation to other fragments
    b. The IP identification field to identify all associated fragments, the More Fragment bit to indicate whether or not more fragments follow the current one, and the Time to Live to expire missing fragments
    c. The IP identification field to identify all associated fragments, the More Fragment bit to indicate whether or not more fragments follow the current one, and the TCP checksum to discard corrupted fragments
    d. The IP identification field to identify all associated fragments, the More Fragment bit to indicate whether or not more fragments follow the current one, the IP options to route all fragments through the same intermediate routers
14. The Time to Live (TTL) field/value found in the IP header are used to:
    a. Make sure all associated fragments arrive with a given window of time

b. Expire TCP segments in transit when the TTL value becomes 0
c. Flush DNS records from cache when the TTL value is exceeded
d. Expire IP packets in transit when the TTL value becomes 0

15. What is the purpose of the IP checksum?
    a. To make sure that data in the entire packet is not corrupted in transit
    b. To make sure that data in the IP header is not corrupted in transit
    c. To make sure that data in the Ethernet frame is not corrupted in transit
    d. To make sure that data in the embedded protocol is not corrupted in transit
16. What is a common use of DNS?
    a. Resolution of a MAC address to an IP address
    b. Resolution of an IP address to a MAC address
    c. Resolution of a port number to a port service
    d. Resolution of a host name to an IP address
17. What is a typical response from a host that receives a UDP packet on a non-listening port?
    a. A UDP reset flag set to the sender
    b. A UDP FIN flag set to the sender
    c. An ICMP port unreachable message to the sender
    d. A UDP port unreachable message to the sender
18. Suppose a SYN packet is spoofed using a real IP address and then sent to a server that responds with a SYN/ACK to the actual IP address. How does the real IP address respond?
    a. With an acknowledgement since it did not send the SYN
    b. With a reset since it did not send the SYN
    c. With a duplicate SYN since it did not send the SYN
    d. With a TTL of 0 since it did not send the SYN
19. What are some differences between IPv4 and IPV6?
    a. They are the same except the IP version number in the IP header is different
    b. The IPv6 addresses are 4 times larger and some of the fields/functionality previously in the IPv4 header are now in IPv6 extension headers
    c. IPv6 allows more than 255 embedded protocols
    d. IPv6 packets are automatically encrypted while IPv4 are not
20. Suppose you had a tool that allowed you to craft an ICMP echo request over Ethernet, but you needed to tell the tool how to compose the request layer by layer in the proper order. How would you order the different layers?
    a. Ethernet header, followed by IP header, followed by ICMP header, followed by optional ICMP data
    b. IP header, followed by Ethernet header, followed by ICMP header, followed by optional ICMP data
    c. The order is unimportant – craft them in any order and the TCP/IP stack will properly assemble them before sending
    d. The Ethernet header must be first, and the order of the IP header, ICMP header, and data is unimportant since the TCP/IP stack will properly order assemble them before sending

21. What is the function of a router?
    a. It determines the entire route for an IP packet from source to destination host
    b. It uses ARP to route the packet to the next hop
    c. It uses DNS to route the packet to the next hop
    d. It attempts to move the IP packet one hop closer to the destination
22. The IP protocol field identifies:
    a. The destination port of the packet
    b. The source port of the packet
    c. The embedded service port of the packet
    d. The embedded protocol of the packet
23. A function of the TCP sequence number is:
    a. To associate a chronological number with each TCP segment, allowing the receiver to properly reorder the individual segments of data
    b. To inform the sender of the next expected chronological sequence number of the TCP segment
    c. To reassemble IP fragments
    d. To increment the hop count on all TCP segments
24. Suppose you want to ping a new known IPv4 address on your network. What must happen first?
    a. The IP address must be resolved to a host name using DNS
    b. An ICMP request must be sent to the router to locate the IP address
    c. An ARP request must be issued by your host to discover the MAC address associated with the IP address
    d. Nothing needs to occur; the hosts talk over IP simply using IP addresses
25. When an IPv4 packet traverses a router what are some of the tasks the router must perform?
    a. Decrement the Time to Live value by 1 and recompute the IP checksum
    b. Decrement the Time to Live value by 1 and recompute the IP and embedded protocol checksums
    c. Decrement the Time to Live value by 1 without changing any checksum
    d. Increment the Time to Live value by 1 and recompute the embedded protocol checksum