Test Yourself! – TCP/IP Knowledge Quiz

Students who wish to take any of the following SANS courses:

Security 502 – Firewalls, Perimeter Protection, and VPNs
Security 503 – Intrusion Detection In-Depth
TCP/IP for Firewalls and Intrusion Detection (Day 1 of the Security 502 and Security 503 course)

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

We encourage students who are considering attending any of the courses listed above to test their understanding of the prerequisite material using the following quiz.

Read the following questions, note your answers, and then check your results against the answer sheet provided. While this quiz alone cannot completely measure a student's readiness, it should be used as a guide to estimate your preparedness and help you get the most out of your SANS course.

Quiz (60 Questions)

1. How many bits in a byte?
a) 8
b) 16
c) 4
d) 2
Answer:_____

2. The OSI model is often used to describe communications architectures. (T/F)
Answer:_____

3. What is a MAC address?
a) the IP address of the host
b) the embedded protocol address
c) the hardware address assigned to the network card
d) the embedded protocol port address
Answer:_____

4. The maximum decimal value for a byte is 255. (T/F)
Answer:_____

5. 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 IP address with a protocol
d) resolves a known MAC address with a vendor type
Answer:_____

6. A packet that is sent on an Ethernet link is known as a frame. (T/F)
Answer:_____

7. A Class C address has:
a) 24 bits assigned for the network address, 8 bits assigned for the host address
b) 16 bits assigned for the network address, 16 bits assigned for the host address
c) 32 bits assigned for the network address, 0 bits assigned for the host address
d) 24 bits assigned for the network address, 24 bits assigned for the host address
Answer:_____

8. The MAC address is 32 bits long. (T/F)
Answer:_____

9. A server port of UDP or TCP 53 is typically associated with what service?
a) ICMP
b) IP
c) Back Orifice
d) DNS
Answer:_____

10. A Class B address has 8 bits to represent the network address and 24 bits to represent the host address. (T/F)
Answer:_____

11. How does a host that has sent TCP data know that the data has been received?
a) an acknowledgement from the receiver
b) an ICMP echo request from the receiver
c) an ICMP data received from the receiver
d) a SYN/ACK from the receiver
Answer:_____

12. The netmask tells a host what address bits identify the network and what address bits identify the host. (T/F)
Answer:_____

13. A DNS server:
a) can associate an IP address with a host name only.
b) can associate a host name with an IP address only.
c) can associate either an IP address with a host name or host name with an IP address.
d) can associate a MAC address with a host name.
Answer:_____

14. Ports can have a value of 1 through 65,535. (T/F)
Answer:_____

15. What does a router do?
a) It determines the entire route for an IP packet from source to destination.
b) It uses ARP to route all packets.
c) It attempts to get an IP packet one hop closer to the destination.
d) It uses DNS to route all packets.
Answer:_____

16. UDP is a reliable protocol. (T/F)
Answer:_____

17. Which TCP/IP protocol is associated with routing?
a) IP
b) DNS
c) UDP
d) TCP
Answer:_____

18. Hosts typically know how to route a packet using a default router. (T/F)
Answer:_____

19. Which of the following is NOT a well-known domain?
a) .us
b) .gov
c) .org
d) .host
Answer:_____

20. The gethostbyname and gethostbyaddr functions are associated with routing. (T/F)
Answer:_____

21. 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
Answer:_____

22. Some top-level DNS domains are .com, .edu, and .mil. (T/F)
Answer:_____

23. 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
Answer:_____

24. TCP is a connection-oriented protocol. (T/F)
Answer:_____

25. The UNIX /etc/services file associates:
a) port numbers and Remote Procedure Call services
b) port numbers and Internet services
c) ephemeral port numbers and localhost services
d) server ports and protocols
Answer:_____

26. The only IP protocols are ICMP, TCP, and UDP. (T/F)
Answer:_____

27. When examining the headers of packets displayed with tcpdump, counting begins with:
a) byte 0
b) byte 1
c) hexadecimal byte 10
d) hexadecimal byte 16
Answer:_____

28. Trusted or "well-known" port numbers are less than 1024. (T/F)
Answer:_____

29. The IP protocol field identifies:
a) well-known destination ports
b) well-known ephemeral ports
c) the embedded service ports
d) the embedded protocol in the packet
Answer:_____

30. The IP address 172.20.0.0 is in the Class B range of addresses. (T/F)
Answer:_____

31. tcpdump "sniffs" packets from:
a) the operating system.
b) the network.
c) the router only.
d) fragmented packets only.
Answer:_____

32. The client sends a RESET to the server to indicate its desire to reopen a half closed session. (T/F)
Answer:_____

33. TCP begins a connection with:
a) the three-way handshake.
b) the two-way termination.
c) fragmenting packets.
d) tcpdump.
Answer:_____

34. Because TCP is full duplex both the client and server have to initiate a FIN to close their connection
gracefully. (T/F)
Answer:_____

35. The SYN bit signals the client's intention to:
a) connect to the server.
b) fragment a packet.
c) terminate a session.
d) push data to the server.
Answer:_____

36. When tcpdump is displayed in hexadecimal you see the entire datagram captured by tcpdump if the
snapshot length (snaplen) parameter is larger than the datagram size. (T/F)
Answer:_____

37. In the tcpdump output shown below, what does 09:32:43:9100000 represent?

```
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
```

a) Timestamp when the record was captured
b) Timestamp when the record was sent
c) TCP sequence number
d) TCP acknowledgement number
Answer:_____

38. The client port, also known as an ephemeral port, is used for the current session and freed afterward for re-use. (T/F)
Answer:_____

39. In the tcpdump output shown below, what does 1173 represent?

```
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
```

a) source sequence number
b) source port
c) source identifier
d) source process ID
Answer:_____

40. A value of 6 in the byte 9 of the IP header means that the embedded protocol is TCP. (T/F)
Answer:_____

41. In the tcpdump output shown below, what does dns.net represent?

```
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
```

a) the destination host name
b) the destination router
c) the destination DNS server
d) the destination host IP address
Answer:_____

42. The tcpdump -x option dumps the record in hexadecimal. (T/F)
Answer:_____

43. In the tcpdump output shown below, what does the "S" indicate?

```
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
```

a) dns.net wants to start a connection with nmap.edu
b) nmap.edu wants to start a connection with dns.net
c) nmap.edu wants to send 21 bytes of data to dns.net
d) nmap.edu wants to terminate a session with dns.net
Answer:_____

44. The tcpdump -s option can change the number of bytes collected. (T/F)
Answer:_____

45. In the tcpdump output shown below, what does 62697789 represent?

```
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
```

a) the acknowledgement number for dns.net
b) the acknowledgement number for nmap.edu
c) the initial sequence number for dns.net
d) the initial sequence number for nmap.edu
Answer:_____

46. If a tcpdump record is UDP, tcpdump will always display "UDP" in the output. (T/F)
Answer:_____

47. In the tcpdump output shown below, what does the (0) indicate?
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
a) 0 sequence numbers consumed on the SYN connection
b) 0 window size for the SYN connection
c) 0 acknowledged bytes on the SYN connection
d) 0 data bytes sent on the SYN connection
Answer:_____

48. The three-way handshake requires the following sequence of flags in the first three exchanges:
record 1: SYN/ACK record 2: SYN record 3: ACK (T/F)
Answer:_____

49. What embedded protocol is used in the tcpdump record shown below?
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
a) ICMP
b) TCP
c) UDP
d) DNS
Answer:_____

50. Servers use ephemeral ports. (T/F)
Answer:_____

51. The three parts of a TCP connection are typically:
a) name resolution, echo request, session termination
b) session establishment, data transfer, and session termination
c) name resolution, port lookup, session termination
d) session establishment, session negotiation, session abort
Answer:_____

52. Two ways to terminate a TCP session are ICMP echo request and ICMP echo reply. (T/F)
Answer:_____

53. The PUSH flag says to:
a) terminate the session
b) establish the session
c) send the data in this TCP segment
d) abort the session immediately
Answer:_____

54. The tcpdump output shown below is in hexadecimal. (T/F)
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
Answer:_____

55. The field that is 9 bytes offset into the IP header is:
a) the embedded IP protocol
b) the destination IP address
c) the source IP address
d) the destination port
Answer:_____

56. The server port in the tcpdump output shown below is 1173. (T/F)
```
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
```
Answer:_____

57. Server port numbers are typically:
a) greater than 1023
b) in the range of 1-1023 and often change
c) well-known port numbers that do not change
d) different on every host depending on operating system and the number of Internet services that run on the host
Answer:_____

58. The client port in the tcpdump output shown below is 1173. (T/F)
```
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
```
Answer:_____

59. A server response with the RESET and ACK flags set to an attempted client connection means:
a) the server host is not alive
b) the attempted TCP port connection to the server is listening
c) the attempted TCP port connection to the server is not listening
d) the attempted UDP port connection to the server is not listening
Answer:_____

60. The window size for dns.net in the tcpdump output shown below is 512. (T/F)
```
09:32:43.910000 nmap.edu.1173 > dns.net.21: S 62697789:62697789(0) win 512
```
Answer:_____