Pre Lecture Test

Intrusion Detection
Version 1 (July 1, 2014)

(1) 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

(2) 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

(3) 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

(4) TCP typically begins a session with:

a. The three-way handshake of server to client with SYN set, the client response of SYN/ACK, and the server acknowledgement of ACK
b. 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
c. The three-way handshake of client to server with SYN set, the server response of SYN/ACK, and the client acknowledgement of ACK

(5) 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

(6) 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

(7) 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

(8) A false positive (in intrusion detection) can be defined as…

a. an alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior.
b. an alert that indicates nefarious activity on a system that is not running on the network.
c. the lack of an alert for nefarious activity.
d. Both a. and b.

(9) Which of the following is true of signature-based Intrusion Detection Systems?

a. They alert administrators to deviations from "normal" traffic behavior.
b. They identify previously unknown attacks.
c. The technology is mature and reliable enough to use on production networks.
d. They scan network traffic or packets to identify matches with attack-definition files.