Post Lecture Test

Intrusion Detection Module
Version 1 (July 1, 2014)

(1) Which of the following is an advantage of anomaly detection?

a. Rules are easy to define.
b. Custom protocols can be easily analyzed.
c. The engine can scale as the rule set grows.
d. Malicious activity that falls within normal usage patterns is detected.

(2) A false positive 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.

(3) When discussing Intrusion Detection Systems, what is a signature?

a. An electronic signature used to authenticate the identity of a user on the network
b. Attack-definition file
c. It refers to "normal," baseline network behavior
d. None of the above

(4) Which of the following is used to provide a baseline measure for comparison of Intrusion Detection Systems?

a. crossover error rate
b. false negative rate
c. false positive rate
d. bit error rate

(5) 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.

(6) 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

(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) What is the packet round-trip time?

(9) Where is the sender's IP address in a packet?

(10) How do you know if a computer is being used as a stepping-stone host?