**8.4 Describe the three logical components of an IDS.**

Sensors collect information from the system being protected. Analyzers determines whether intrusion has occurred based on data collected from sensors. The user interface allows users to view information about system or to adjust the behavior of the IDS.

**8.7 What is the difference between a false positive and a false negative in the context of an IDS?**

A false positive means a legitimate user is believed to be an intruder. A false negative means that an attacker is mistakenly identified as an authorized user.

**8.10 What is the difference between anomaly detection and signature or heuristic intrusion detection?**

Anomaly detection compares a particular users behavior to the more average user, and if there are significant deviations will raise alarms. On the other hand heuristic detection compares a user’s behavior to the behavior of known attackers and if they are similar will raise alarms.

**8.21 What is a honeypot?**

A honeypot is an artificial system with fake data that are intended as decoys so that attackers attack the honeypot instead of more secure systems, giving administrators time to analyze attackers and prepare their defenses.

**9.5 What is the difference between a packet filtering firewall and a stateful inspection firewall?**

A packet filtering firewall only looks at the packets passing through themselves and decides whether to let them through based on information from the packet, such as source or destination IP. A stateful inspection firewall can look inside the packets because the firewall is aware of protocols such as TCP, and thus can decide whether to allow traffic based on the contents of a message.

**Problem 9.5**

**a.** Rule A allows external users to send TCP messages to the server. Rule B allows internal users to send TCP messages to external users. Rule C allows the server to send TCP messages to external users. Rule D allows external users to send TCP messages to internal users. Rule E rejects all other traffic

**b.** All packets are accepted. Packet 1 uses rule A. Packet 2 uses rule B. Packet 3 uses rule C. Packet 3 uses rule D.

**c.** The attack will succeed. Packet 5 is allowed by rule D, and packet 6 is allowed by rule B.

**Problem 9.6**

**a.** The new rules mean that all traffic must be mediated by the server.

**b.** Packets 1-4 are permitted by the same rules as above. Packet 5 is no longer allowed by rule D and packet 6 is no longer allowed by rule B, so they are both caught by rule E.

**Problem 9.7**

**a.** Packet 7 will be allowed through by rule D, and packet 8 will be allowed by rule C.

**b.** Add to all rules that packets must have the ack bit set except for rule A