CSCI 3403 **Brennon Lee**
Homework 11 **Fall 2018, CU-Boulder**

1. **Question Not in the Book:**Consider the SNORT rule:

   ```
   alert tcp $HOME_NET any <> $EXTERNAL_NET 6666:7000
   (msg:"CHAT IRC message"; flow:established;
   content:"PRIVMSG "; nocase; classtype:policy-violation;
   sid:1463; rev:6;)
   ```

   Explain what the snort rule does by answering:

   (a) What type of connections would the rule apply to?
   (b) What type of traffic is being monitored?
   (c) Is there any additional requirement on the traffic?

   Answer

2. **Review Question 8.4** Describe the three logical components of an IDS.

   Answer

3. **Review Question 8.8** Explain the base-rate fallacy.

   Answer

4. **Problem 8.2** In the context of an IDS, we define a false positive to be an alarm generated by an IDS in which the IDS alerts to a condition that is actually benign. A false negative occurs when an IDS fails to generate an alarm when an alert-worthy condition is in effect. Using the following diagram, depict two curves that roughly indicate false positives and false negatives, respectively:

   Answer

5. **Problem 8.3**

   Answer

6. **Problem 8.4** One of the non-payload options in Snort is flow. This option distinguishes between clients and servers. This option can be used to specify a match only for packets flowing in one direction (client to server or visa-versa) and can specify a match only on established TCP connections. Consider the following Snort rule:

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS\
(msg: ‘‘ORACLE create database attempt:;\
flow: to_server, established; content: ‘‘create database";
nocase;\
classtype: protocol-command-decode;)
```

   (a) What does this rule do?

   Answer

   (b) Comment on the significance of this rule if the Snort devices is placed inside or outside of the external firewall.

   Answer

7. **Problem 8.6**

   Answer