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?

   a) This rule applies only to established TCP connections.
   b) Any private messages going either direction from the HOME NET (on any port) to outside EXTERNAL NET Destination IP.
   c) The only outgoing traffic that is monitored will be ones that have destination ports between 6666 and 7000.

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

   Sensor - which has the role of collecting data. It's input includes network packets, log files, and system call traces.

   Analyzer - receives input from one or more sensors. It is responsible for determining if an intrusion has occured. The output of this component is an indication that an intrustion has occurred and could also include evidence supporting the conclusion.

   User Interface - enables the usre to view the output of the system or control the system behavior.

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

Base-rate fallacy is an error that occurs when the conditional probability of some hypothesis H (i.e. is this an intruder?), given some evidence E (Network data), is assessed without taking into account the prior probability of H and the total probability of evidence E. If the actual number of intrusions is low compared to the number of real users of a system, then the false alarm rate will be high unless the test is extremely discriminating.

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?

This rule will detect attempted attacks from established TCP connections. The source is any external net on any port and the direction is going from the source to destination. The destination is SQL servers and their oracle ports. This rule logs traffic that is atempting to create a database. The flow is used to match packets flowing to a server with an established TCP connection.

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

The amount of traffic logged would be significantly higher if this alert was placed outside of the firewall. If inside, there would be much less traffic logged since some invalid connection attempts are prevented by the firewall.

7. **Problem 8.6**

Answer