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 traffic going either direction from the HOME NET (on any port) to outside EXTERNAL NET destination IP (between ports 6666:7000).

   b) Based off of the port numbers, we know that Private / IRC messages are the target traffic being monitored.

   c) An additional requirement is that only traffic on established TCP connections is being monitored.

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.

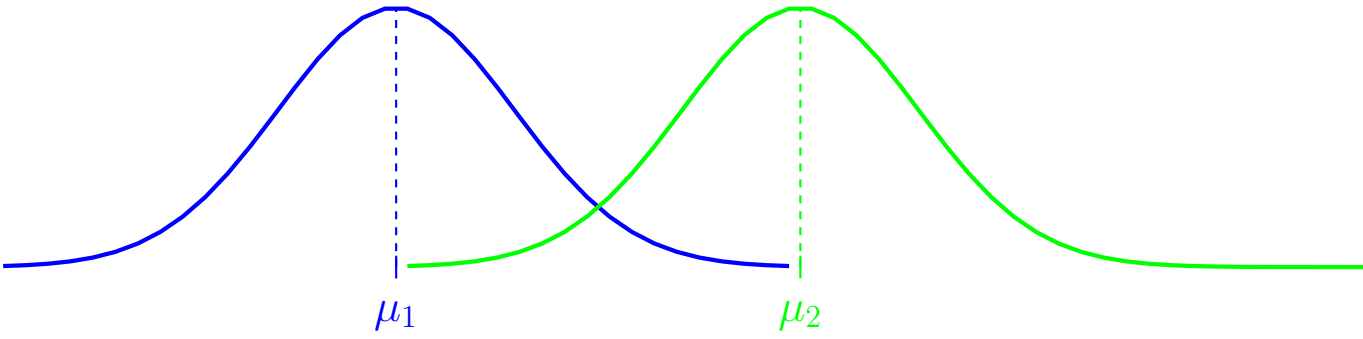
   Analyzer - receives input from one or more sensors. It is responsible for determining if an intrusion has occured. The output of this component is an indication that an intrustion has occurred and could also include evidence supporting the conclusion.

   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:



   Above we have two normal distributions. μ_1 represents average intruder behavior where μ_2 represents the average authorized user behavior. The intersection of the two bell curves represents the probabilities of when an intruder's behavior closely matches an authorized user or vice versa. The trick with False Positives and False Negatives is to use hypothesis testing to deduce the liklihoods of each case being a False Postive or a False Negative. Typically, one allows more of one option to occur to safegaurd against the other (due to their inverse relationship). In this example, we would most likely want to accept a higher False Positive rate with a lower False Negative rate since we would rather have false alarms than not catch an intruder at all.

5. **Problem 8.3** Wireless networks present different problems from wired networks for NIDS deployment because of the broadcast nature of transmission. Discuss the considerations that should come to play when deciding on locations for wireless NIDS sensors.

   An example is an organization with multiple sites with one or more LANs. To start, one could place a NID right outside of the external firewall. This allows the NID to record number and types of attacks coming from the internet and targeting the network. Another position is right inside the external firewall. This location allows the NID to find attacks coming from the outside world and that get past the firewall. NIDs at this location can also recognize outgoing traffic that results from a compromised server from inside the organization. Another location is right in front of the internal server and data resources. Here it can monitor large amounts of network traffic to find possible attacks and detect unauthorized activity by authorized users inside the organization. Lastly, if there is a separate LAN with an internal firewall for a separate deparment, a NID can be place just inside that firewall. Here, the sensor can detect attacks targeting systems and resouces.

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** An example of a host-based intrusion detection tool is the tripwire program. This is a file integrity checking tool that scans files and directories on the system on a regular basis and notifies the administrator of any changes. It uses a protected database of cryptographic checksums for each file checked and compares this value with that recomputed on each file as it is scanned. It must be configured with a list of files and directories to check and what changes, if any, are permissible to each. It can allow, for example, log files to have new entries appended, but not for existing entries to be changed. What are the advantages and disadvantages of using such a tool? Consider the problem of determining which files should only change rarely, which files may change more often and how, and which change frequently and hence cannot be checked. Consider the amount of work in both the configuration of the program and on the system administrator monitoring the responses generated.

The obvious advantage of such a tool is that it could be extremely useful for identifying changed files and directories. However, this could also be a disadvantage since a running computer can change thousands of files and directories constantly. So this tool would definitely need to be tightly configured with a list of files and directories to watch that don't change often.

Any files concerning user interaction and user data would most likely be changing constantly. Compared to system configuration files with root access should not change as often and therefore could be monitored with this

intrustion detection tool.

Lastly, there needs to be an update system in place for when files get updated or configuration changes occur. Those checksums also need to be updated when these occur.