1. **Problem 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:

   1) What type of connections would the rule apply to?
   So we have a source address "HOME˙NET", a source port "any", a destination address "EXTERNAL˙NET", and a destination port "6666:7000 "
   This means we have connection from home, using any port, to external destination address with port that ranges 6666:7000, and is a bidirectional connection.

   2) What type of traffic is being monitored?
   IRC traffic

   3) Is there any additional requirement on the traffic?
   The connections need to be established and the messages need to be private.

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

   (a) **Sensors** - these are responsible for collecting data. The input for a sensor may be any part of a system that could contain evidence of an intrusion. Types of input to a sensor includes network packets, log files, and system call traces. Sensors collect and forwards this information to the analyzer.

   (b) **Analyzers** - These receive input from one or more sensors or from other analyzers. These are responsible for determining iff an intrusion has occurred. The output may include evidence supporting the conclusion that an intrusion occurred.

   (c) **User Interface** - The user interface to an IDS enables a user to view outputs from the system or control the behavior of the system. In some systems, the user interface may equate to a manager, director, or console component.

   (Page 256-257)

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

   The base-rate fallacy occurs when in general, if the actual numbers of intrusions is low compared to the number of legitimate uses of a system, then the false alarm rate will be high unless the test is extremely discriminating.
   (Page 259)

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 nis in effect. Using the following diagram, depict two curves that roughly indicate false positives and false negatives respectively:

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 into play when deciding on locations for wireless NIDS sensors.

   The consideration that should come into play when deciding on locations for wireless NIDS sensors are:

   (a) LOCATION AND ACCESS POINTS- It is important to pick a location where the sensor can be deployed with Wireless Local Area Network, this will allowed the sensor to monitor the Radio Frequency range of the organizations access points and stations. Depending on where you are putting these sensors, you would have to take different measurements of care. For example, if you're putting them in interiors, there is not much risk, but if you're putting them in exteriors, you have to consider physical threats and will have to add anti-tamper features to these. In addition, you have to consider the Access Points in the locations since the software is deployed with the device.

   (b) RANGE - range has to do with location, they go hand to hand. The sensors that are deployed in interiors and are tend to be more effective than the one in exteriors. However, there could be the case that if you have sensors inside and outside in the location, these may overlap.

   (c) ACCESSIBILITY - it is important to know that sensors function better with a wired network. Therefore, wherever there are wireless NIDS sensors, it is important to make sure that there are wired network connections close enough to provide access to monitoring.

   (d) COST - Wanting to have wireless NIDS sensors might be more expensive because you might need more units to have a good range, might need more maintenance, might need a more elaborated plan of deployment or design to allocate them. So comparing the cost of the wireless against the wired networks.

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 vice 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 is creating a database after checking if the packet is "to˙server" which means that is intended a server, and has to have a connection established. Also checks if the content/string "create database" is a packet in the payload.
The source address is EXTERNAL˙NET, the source port is any, the destination address is SQL˙SERVERS, and the destination port are ORAVLE˙PORTS.

b) *Comment on the significance of this rule if the Snort devices is placed inside or outside of the external firewall*
This rule is making sure that the systems blocks any possible creation of databases across the internet, in case there is one request of creating one, the attempt is blocked by the firewall.
Therefore if we have the snort devices INSIDE, it will mess up the behavior of the firewall since it will be causing trouble to legit people trying to create a database.
If is OUTSIDE then it will send the alert. It will let us know that someone tried to create the database, so IT IS BETTER to have outside of the external firewall.

7. **Problem 8.6**. Look page 287 - I will just write the answer here because the question is too long

   ADVANTAGES - The tripwire program is good at noticing the files that were not supposed to be modified and they were. For example, directories or files in the system that have changes will be detected by the tripwire.
   -Tripwire can be monitored without many problems since the changes in small list of configuration files and critical system programs can be easily detected.
   -Files generated on one platform can be read and used on other platforms.
   -The program can be run without relying on outside, potentially vulnerable programs.

   DISADVANTAGES - Files can change constantly because most of the computer system are not static.
   -Machine should be operated in a single user mode when installing the database.
   -The changes in a large file made by the attacker cannot be detected if the large area of the system is not monitor properly.
   -More attention and care is needed to identify the files that are not expected to change in the large area of the system.

-If the system already has some bugs before building Tripwire, then Tripwire will have been installed too late to report those tampering.
-Special process is needed to manage the update of monitored files
-The process must verify whether the files are correct and then updates the cryptographic checksum of the files.

In conclusion, even though the number of disadvantages is greater than the number of advantages, the program can be manageable and really good to use when one user is using it and setting the correct configuration, this will decrease the risk of many changes in configurations in a large scale and changed files can be detected more reliably.