Review Questions Chapter 8

8.4) Describe the three logical components of an IDS

3 types of logical component of an IDS

1. **Sensors**
   i) Sensors are to collect data
   ii) The input for a sensor is any part of the system that contains an intrusion such as network packet, call traces, and log file
   iii) Then forward to analyzer
2. **Analyzer**
   i) Analyzer gets data from other analyzer or sensors
   ii) Is to detect intrusion is present on the data and indicate the result that an intrusion has occurred
   iii) If it has occurred, then analyzer provides the guidance about the action to take as a result of intrusion
3. **User Interface**
   i) Is used to view the result of the system, or to organize the performance of the system
   ii) User interface could be a director, manager, or console component in some system

8.8) Explain the base-rate fallacy

Ignoring statistical information in favor of using irrelevant information, that one incorrectly believes to be relevant, to make a judgment. This usually stems from the irrational belief that statistics don't apply to a situation, for one reason or another when, in fact, they do.

Example: *Only 6% of applicants make it into this school, but my son is brilliant! They are certainly going to accept him!*

Explanation: Statistically speaking, the son may still have a low chance of acceptance. The school is for brilliant kids (and everyone knows this), so the vast majority of kids who apply are brilliant. Of the whole population of brilliant kids who apply, only about 6% get accepted. So even if the son is brilliant, he still has a low chance of being accepted (about 6%).

Problems Chapter 8
8.2)

False positive of IDS (Intrusion Detection System):
(A false positive is an alarm produced by an IDS that the IDS alert to a condition)

The curve means the loose interpretation of intruder behavior catches more number of intruder, or the authorized are detected as intruders and this lead to an increased number of false positives

False negative:
(A false negative occurs when IDS fails to produce the alarm)

The curve makes an attempt to limit the false negatives by tight interpretation of intruder behavior and this leads to increase the number of false negatives, or it doesn't identify intruders as intruders.

8.4) Consider the following Snort rule:

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

a) What does this rule do?

The rule is to create a new database instance.
Line 1: is the interesting packets flowing from external IP addresses for the database servers responding on oracle ports.
Line 2: is the text alert that reports.
Line 3: 2 matching conditions
1) the packets must be intended to a server and it must be a part of established TCP connection
2) represents the case-independent string "create database" that must be a packet in the payload

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

The significance of this rule is the system admin configures a system prohibits the creation of database across the internet and this attempt is blocked by the firewall

If the NIDS (Network Intrusion Detection System) is placed externally, it simply gathers out such attacks and give an alert message
If the NIDS is place internally inside of the firewall, it cause serious deficiency in the behavior of firewall.

Problem Chapter 9

9.1)
Overcome the **tiny fragment attack** by doing approach from packet filter firewall, stateful inspection firewall, application proxy firewall, circuit level proxy firewall on types of firewall

- The fragment of IP might arrive in any order
- The first fragment of IP packet is discarding through network, so the rest of fragments can be discarded
- All the intermediate fragments of IP packet might pass via filter to filter out the traffic before discarding the first fragment of IP packet
- However, if the first fragment of IP packet is discarded, then the rest of IP packet is discarded to destination. So it's impossible to reassemble the IP packet to destination host

Thus, if the first fragment is discarded, the destination discards the entire fragment of IP packet after timeout.

9.5)
SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

a. Describe the effect of each rule

Rule A:

- Define the "remote host receiving the incoming email from external server", so rule A permits the inbound SMTP connection

Rule B:

- Define the "external server receiving the incoming email from remote host", so rule B permits the inbound SMTP connection

Rule C:

- Define the "external server transmit the outgoing email to remote host", so rule C permits outbound SMTP connection

Rule D:

- Define the "remote host transmit the outgoing email to external server", so rule D permits the outbound SMTP connection

Rule E:

- Define the direction "Any" from any source to any destination with any destination port number, so rule E is default rule to set the action is denied because it doesn't perform any action

b. Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates and SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are as shown:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP	1234	?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

Indicate which packets are permitted or denied and which rule is used in each case.

Packet1: Packet1 permits the "remote host receiving the incoming email from external host"
Packet2: Packet2 permits the "external host receiving the incoming email from remote host"
Packet3: Packet3 permits the "external host transmit the outgoing email to remote host"
Packet4: Packet4 permits the "remote host transmit the outgoing email to external host"

Thus, the final table is the following:

Packet	**Direction**	**Src Addr**	**Dest Addr**	**Protocol**	**Dest Port**	**Action**
1	In	192.168.3.4	172.16.1.1	TCP	25	Rule A
2	Out	172.16.1.1	192.168.3.4	TCP	1234	Rule B
3	Out	172.16.1.1	192.168.3.4	TCP	25	Rule C
4	In	192.168.3.4	172.16.1.1	TCP	1357	Rule C

c. Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Typical packets are as follows:

Packet	**Direction**	**Src Addr**	**Dest Addr**	**Protocol**	**Dest Port**	**Action**
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

Will the attack succeed? Explain.

Packet 5 and 6 could be successful because the original rule B and D permit all connections ends with transmission ports of above 1023

Rule B:

- Define the "external server receiving the incoming email from remote host", so rule B permits the inbound SMTP connection

Rule D:

- Define the "remote host transmit the outgoing email to external server", so rule D permits the outbound SMTP connection

So, packet 5 and 6 performs both action of receiving the incoming email and transmitting the outgoing email

Packet	**Direction**	**Src Addr**	**Dest Addr**	**Protocol**	**Dest Port**	**Action**
5	In	10.1.2.3	172.16.3.4	TCP	8080	Rule B
6	Out	172.16.3.4	10.1.2.3	TCP	5150	Rule D