CSCI 563 Assignment 3

Name: Rama Krishna Kamma
CWID: 50321021

Problem 1. Firewall Policy (60 pt.)

Suppose a home network with a network address of 128.100.5.* (i.e., 128.100.5.0/24).The home network has two servers: the Web server with IP address=128.100.5.1 and port number=TCP/80 and the DNS server with IP address=128.100.5.2 and port number=UDP/53. Configure the firewall table to implement the following ruleset.

Ruleset:

1. Allow external traffic to access the internal DNS server.
2. Allow external traffic to access the internal Web server.
3. Internal traffic is allowed to access external Web servers (TCP/80).
4. Internal traffic is allowed to access external Zoom servers (TCP/443).
5. All other TCP traffic from external to internal is disallowed
6. All other UDP traffic from external to internal is disallowed

Note: Use the notation shown in the lecture slide. Do NOT use any mnemonics, for example, ANY, HOME, EXTERNAL, etc, not used in in the slide.

Solution:

Rule	Type	Source Address	Dest. Address	Dest. Port	Action
1	**UDP**	**0.0.0.0/0**	**128.100.5.2/32**	**53**	**Allow**
2	**TCP**	**0.0.0.0/0**	**128.100.5.1/32**	**80**	**Allow**
3	**TCP**	**128.100.5.0/24**	**0.0.0.0/0**	**80**	**Allow**
4	**TCP**	**128.100.5.0/24**	**0.0.0.0/0**	**443**	**Allow**
5	**TCP**	**0.0.0.0/0**	**128.100.5.0/24**		**DisAllow**
6	**UDP**	**0.0.0.0/0**	**128.100.5.0/24**		**DisAllow**

Problem 2. Intrusion Detection (40 pt.)

Consider the following:

- Suppose an IDS is 98% accurate, having a 2% chance of false positives or false negatives.
- The intrusion detection system generates 1,000,100 log entries.
- Only 100 of the 1,000,100 entries correspond to actual malicious events.

Answer the following questions. Show your work.

a. (24 pt.) Calculate TP, TN, FP, and FN.
Solution:

The intrusion detection system creates 1000100 log entries, of which 98% are accurate IDS and the remaining 2% are false positives or false negatives, according to the provided statistics.

Only 100 of the 1000100 entries are connected to malicious events.

True Positive: A true positive is an outcome where the model correctly predicts the positive class.

True Positive (TP) = 0.98 * 100 = 98

True Negative: A true negative is an outcome where the model correctly predicts the negative class.

True Negative (TN) = 0.98 * 1000000 = 980000

False Positive: A false positive is an outcome where the model incorrectly predicts the positive class.

False Positive (FP) = 0.02 * 1000000 = 20000

False Negative: A false negative is an outcome where the model incorrectly predicts the negative class.

False Negativity (FN) = 0.02 * 100 = 2

b. (16 pt.) Calculate the number of false alarms (count) and the false alarm rate (%).
c. **Solution:**

According to the previous question (part a) we already know that the False Positive i.e., it is an outcome where the model incorrectly predicts the positive class.

False Alarms:

False Positive (FP) = 0.02 * 1000000 = 20000

False Alarm Rate:

The false positive rate gives the proportion of incorrect predictions in positive class.

False Positive Rate = (FP)/(FP + TN)

= 20000/(20000 + 980000)

=20000/1000000

= 0.02%