Homework Assignment 5

Cybersecurity

COSC 3371 / 2022 Spring

Please solve the following problems by answering each question using the information that is provided here as well as using what you learned in class (see Lectures 24, 25, and 26). Please submit a single file on Blackboard, containing all the numbered questions with your answers inline. You can write your answers into this file and submit it as a PDF or Word file on Blackboard.

Problem 1: Firewall Rules [5 points]

In this problem, you will evaluate the rules of a "three-legged" firewall that is supposed to protect a DMZ and an internal network. The address ranges of the DMZ and the internal network are `192.168.1.0/24` and `192.168.2.0/24`, respectively[1]. There are two servers in the DMZ, an e-mail server (`192.168.1.1`) and a web server (`192.168.1.2`). There is also a database server (`192.168.2.1`), which is located in the internal network. For this problem, we will consider only TCP packet filtering.

The rules of the firewall are as follows:

```
1. ESTAB 0.0.0.0/0       -> 0.0.0.0/0       : ANY  => ACCEPT
2. NEW   0.0.0.0/0       -> 192.168.1.1     : ANY  => ACCEPT
3. NEW   0.0.0.0/0       -> 192.168.1.2     : 80   => ACCEPT
4. NEW   192.168.1.1     -> 0.0.0.0/0       : 25   => ACCEPT
5. NEW   192.168.1.0/24  -> 192.168.2.1     : 8080 => ACCEPT
6. NEW   192.168.2.0/24  -> 0.0.0.0/0       : ANY  => ACCEPT
7. NEW   192.168.1.0/24  -> 192.168.2.0/24  : ANY  => DROP
8. NEW   192.168.1.0/24  -> 0.0.0.0/0       : ANY  => ACCEPT
9. OTHERWISE => DROP
```

The fate of each TCP packet is determined by the **first** rule that matches the packet. The last rule (Rule 9) drops all TCP packets that did not match any of the preceding rules. The syntax of the first eight rules is the following:

STATE SOURCE_IP -> DESTINATION_IP : PORT => ACTION

where

- *STATE* is either `NEW`, which matches TCP packets that are attempting to establish a new connection (i.e., matches the first message of a TCP handshake), or `ESTAB`, which

[1] In other words, addresses in the internal network range from `192.168.2.0` to `192.168.2.255`, while addresses in the DMZ range from `192.168.1.0` to `192.168.1.155`.

matches TCP packets that belong to a connection (i.e., matches anything other than the first message of a TCP handshake);[2]
- *SOURCE_IP* is either a range of source IP addresses or a specific address;
- *DESTINATION_IP* is either a range of destination IP addresses or a specific address;
- *PORT* is either a specific destination TCP port or ANY, which matches any port;
- *ACTION* is either ACCEPT, which means that the firewall should let the packet pass through, or DROP, which means that the firewall should drop (i.e., discard) the packet.

Note that the range 0.0.0.0/0 contains **all** IP addresses, and a rule matches a packet if all the fields match (i.e., state of connection, source and destination IP addresses, and destination port).

Please note that the questions below ask whether the firewall will allow or drop the packet, **not** whether the destination host will accept the connection or not.

1) Would an arbitrary host from the Internet (e.g., 198.51.100.1) be able to establish a new TCP connection to the e-mail server (192.168.1.1) on port 25? If yes, which rule accepts this packet? If no, which rule drops it?

2) Would an arbitrary host from the Internet (e.g., 198.51.100.1) be able to establish a new TCP connection to the web server (192.168.1.2) on port 25? If yes, which rule (2—9) accepts this packet? If no, which rule (2—9) drops it?

3) Would the e-mail server (192.168.1.1) be able to establish a new TCP connection to an arbitrary host on the Internet (e.g., 198.51.100.1) on port 80? If yes, which rule accepts this packet? If no, which rule drops it?

4) Would the web server (192.168.1.2) be able to establish a new TCP connection to the database server (192.168.2.1) on port 80? If yes, which rule accepts this packet? If no, which rule drops it?

5) Would the web server (192.168.1.2) be able to establish a new TCP connection to the database server (192.168.2.1) on port 8080? If yes, which rule accepts this packet? If no, which rule drops it?

6) Would the e-mail server (192.168.1.1) be able to establish a new TCP connection to the database server (192.168.2.1) on port 25? If yes, which rule accepts this packet? If no, which rule drops it?

7) Would the database server (192.168.2.1) be able to establish a new TCP connection to the web server (192.168.1.2) on port 8080? If yes, which rule accepts this packet? If no, which rule drops it?

[2] Note that the first rule (Rule 1) simply ensures that packets belonging to already established connections are allowed to pass through; the subsequent rules (Rules 2 to 9) are more interesting since they are the ones that determine what connections can be established.

8) Suppose that you have to ensure that all e-mail traffic from the internal network goes through the e-mail server by extending the firewall rules. Formally, the following requirements must be satisfied:
    a. hosts from the internal network **should be able** to establish new TCP connections to the e-mail server on port 25;
    b. hosts from the internal network **should not be able** to establish new TCP connections to any host on the Internet on port 25;
    c. other network traffic should be unaffected by your extension.

    Write a new firewall rule (or rules) **using the syntax of this problem** that satisfy the above requirements! Specify before which existing rule (1—9) should the new rule (or rules) be inserted!

Problem 2: Intrusion Detection [1 point]

For additional security, traffic going through the firewall is also monitored using the Snort network intrusion-detection system.

- Write a Snort rule that raises an alarm (with the message "`Yikes!`") when someone **not from the internal network** tries to access the page `wp-login.php` on the webserver using HTTP! Try to minimize the number of false matches.

Note that for source or destination IP addresses, you can specify a range using variable-length subnet masks (e.g., `192.168.1.0/24`). Also, note that you can specify the complement of a range or address with the negation operator (e.g., `!192.168.1.0/24` matches any IP address outside `192.168.1.0/24`).

Problem 3: Taint Analysis [1 point]

Consider the following Java code snippet:

```
Scanner scanner = new Scanner(System.in);
String var1 = scanner.next();
String var2 = "/home/student/public.txt";
String var3 = (var1 == "question") ? "true" : "false";
String var4 = var2 + var1;
String var5 = var3.trim();
String var6 = var4.toUpperCase();
String var7 = var1.substring(var2.indexOf("/"));
String var8 = var2 + var6 + var2;
```

Which of the variables `var1`, `var2`, …, `var8` should be considered tainted (e.g., for the purpose of copy-pasting it into a system command to be executed) and why?