CSSE 490-- NETWORK SECURITY

Rose-Hulman Institute of Technology

Mini Lab 05: Stateful Firewalls

Learning Objectives

At the end of this concept lab, you should be able to:

- Define how a firewall works in the context of a Linux box.
- Experiment with different filtering rules using 'nftables'.
- Add `nftables` rules to restrict access to your private network for certain individuals and/or applications.

Name: ____

Question	Points	Score
Question 1	5	
Question 2	5	
Question 3	5	
Question 4	5	
Question 5	10	
Question 6	10	
Total:	40	

1 `nft` counters

The questions below refer to the `nft` counter experiment.

Question 1. (5 points) What do you think the `counter` rule is doing?

Question 2. (5 points) Next, from the `client`, try to reach the server using `ping -c3 server` and then check the content of the table again. Does the table change after the client pings the server? What in the `nftables` table and chain impact this outcome?

Question 3. (5 points) If you were to change the table or chain to apply the counter rule to the client to server traffic instead, what would your script look like? Make sure to write such a script and test it before submission.

2 Rules and actions

The questions below refer to the nft rules and actions experiment.

Question 4. (5 points) Based on your experiment, what is the main difference between the drop and reject actions?

Question 5. (10 points) Consider the script presented in the lab, describe the impact of the following rule on the container:

```
add rule netsec_tbl netsec_out icmp type echo-request drop
```

Question 6. (10 points) Consider the script presented in the lab, describe the impact of the following rule on the container:

```
add rule netsec_tbl netsec_out icmp type echo-reply drop
```