CSSE 341 -- Network Security

Rose-Hulman Institute of Technology

Lab 10: Introduction to Stateless Firewalls

Learning Objectives

At the end of this 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	5	
Question 7	5	
Question 8	5	
Question 9	5	
Question 10	10	
Question 11	10	
Question 12	5	
Question 13	5	
Question 14	0	
Total:	80	

1 Map the running services

The questions below refer to the first step of this lab.

Question 1. (5 points) List out the services running on the `server` container.

Question 2. (5 points) For each service running there, list a command that you can use to test if that service is running and reachable.

2 Simple `nft` firewall

The questions below refer to the second step of this concept lab.

Question 3. (5 points) What do you expect the impact of the chain we have added to be?

Question 4. (5 points) Verify your answer by running a simple command from the `client` or `server` containers.

Question 5. (10 points) How would you change the chain above to make sure that this observed behavior does not take place?

3 `nft` counters

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

Question 6. (5 points) What do you think the `counter` rule is doing?

Question 7. (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 8. (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.

4 Rules and actions

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

Question 9. (5 points) Based on your experiment, what is the main difference between the `drop` and `reject` actions?

Question 10. (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 11. (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
```

Question 12. (5 points) In your own words, please write a quick summary of what you have learned in this lab.

Question 13. (5 points) How much time did it take you to complete this lab?

Question 14. Do you have any feedback about this lab? (If you'd like to leave an anonymous feedback, feel free to detach this page and slide it under my door).