Ryan Younes

CNS Lab

LT Quarry

August 31, 2023

Lab 2

1. When would you use a Dockerfile versus a docker-compose file? What are the advantages of the latter? [1.5 points]

You would use a Dockerfile when you want to create an entirely new image through pulling updates from the internet, as seen when it calls upon external repositories with the apt-get command. A docker-compose file can utilize multiple containers to run an application, utilizing the image created by the Dockerfile.

2. If the iptables command is used without the -t option, what is the name of the table that will be changed? [1.5 points]

The name of the default table (where you omit the -t option) is **filter**, which contains the chains INPUT, OUTPUT, and FORWARD.

3. Observations from Chapter 3.3 of the SEED lab document. Answer the two questions, detail what works/doesn’t work and why, and provide screenshots that support your answers.

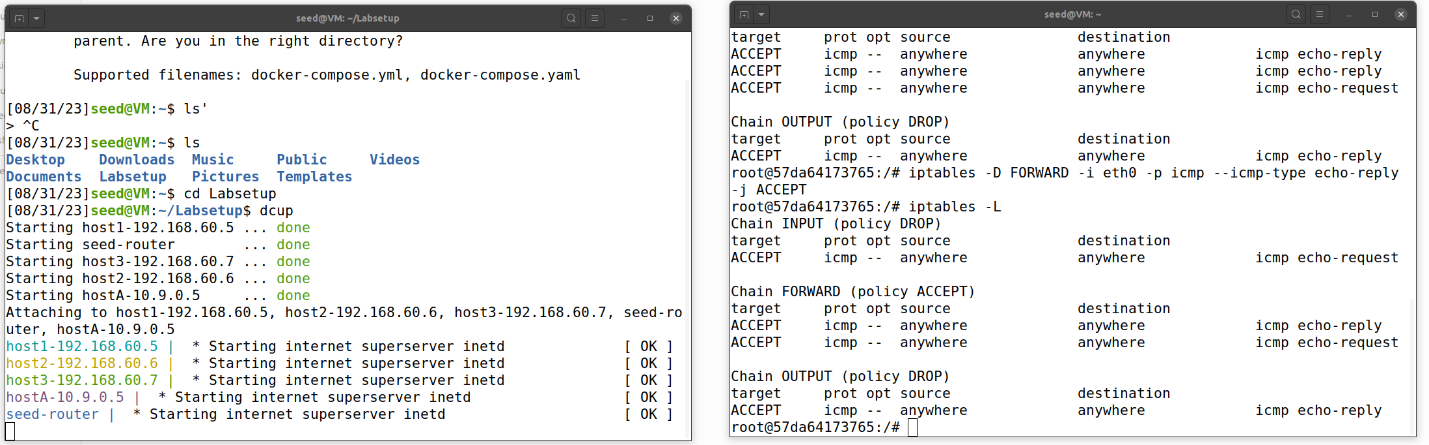
A screenshot of a computer

Description automatically generated

Attempting to ping the router from host A (10.9.0.5) results in success, as we have allowed icmp requests and replies from host A and the router as seen best in the rules under the chains INPUT and OUTPUT . Attempting to telnet into the router results in failure, as it is a separate protocol that is not permitted into the system via the rules already set up.

4. Observations from Chapter 3.4 of the SEED lab document (see the last paragraph for details) [2.5 points]

Setting up the rules for the FORWARD chain as seen below allow the four rules of the system to be followed. This will still allow other forms of traffic to make it into the internal network, however.



5. Observations from Chapter 3.5 of the SEED lab document. Provide the same level of detail as the previous question. [1.5 points]

Targeting tcp connections this time, five rules outlined in the lab document must be followed. These rules as set up allow for the internal communications but exclude outside communications for outside hosts and internal servers as well as internal servers not accessing external servers.