Question 1: A Dockerfile is just a text file with instructions to create one container where a Docker Compose is used to set up multiple containers and set how they interact with each other. One reason you might use a Docker Compose rather than just a Dockerfile is if you are trying to set up a model network like what was done with this lab. If Dockerfiles where used it would be tedious to set up the environment for this lab where Docker Compose allowed us to quickly create a model network and we were able to test and if need be easily create another network of containers.

Question 2: If using iptables and the -t flag is not used, the table that is changed is the filter table. The filter table is allows to make rules traffic that is inputted, outputted, or forwarded through the host. This is the table that we utilized during this lab.

Question 3: I was able to ping the router from the attacker as the filters set in the iptables allowed for ICMP echo request on the input and reply on the output. Because of this the attacker machine was able to ping the router. Since all other packets are blocked on the input and output the attacker was not able to connect by telnet to the router. Below is the specific iptables commands that where inputted to allow outside hosts only to ping the router and have all other traffic blocked.

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

iptables -P OUTPUT DROP

A screenshot of a computer code

Description automatically generatediptables -P INPUT DROP

Above is the configuration on the router

A screenshot of a computer

Description automatically generated

Above shows how a host outside the network is able to ping the router but not able to telnet into the router

Question 4:

For question we had to create a network that 1. allows outside hosts to ping the router 2. Internal host can ping external hosts 3. Outside hosts cannot ping internal hosts 4. Any other traffic between external and internal hosts is blocked. Using the same commands as part 3 to block any traffic from external hosts to the router except pings from an external host to the router. In order to allow internal host ping external host we had to allow ping requests to be allowed to go from internal hosts to external hosts through the router and to allow reply’s to from external network to internal network. In order to accomplish this these commands below must be inputted

iptables -A FORWARD -i eth1 -o eth0 -p icmp –icmp-type echo-request -j ACCEPT

iptables -A FORWARD -o eth1 -i eth0 -p icmp –icmp-type echo-reply -j ACCEPT

A screenshot of a computer

Description automatically generated

Above is an example of an external host trying but being unsuccessful at pinging an internal host

A screenshot of a computer

Description automatically generated

A computer code with text

Description automatically generatedAbove is an example of an internal host successfully pinging an external host.

Above is the router configuration to meet the objectives laid out in Question 4