1/c Charles Norman

Computer and Network Security

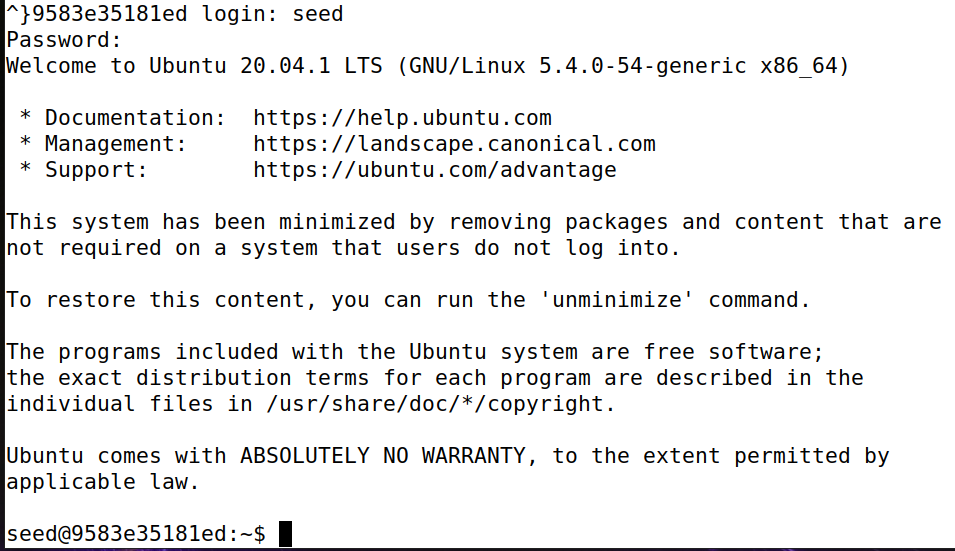
LT Quarry

Lab 2

31AUG23

1. When would you use a Dockerfile versus a docker-compose file? What are the advantages of the latter?
   1. If I only wanted to build a Docker image, not configure and control multiple Docker containers, I would use a Dockerfile. One of the main advantages of the docker-compose file is that I can use one file to configure multiple containers then start/stop all of them with one command. This makes it more straightforward to create consistent containers or even network them.
2. If the iptables command is used without the -t option, what is the name of the table that will be changed?
   1. The default table is the filter table, so if iptables is issued without the -t option it will change the filter table.
3. Observations from Chapter 3.3 of the SEED lab document.
   1. Before issuing the iptables commands:A screenshot of a computer program

      Description automatically generated



* 1. After issuing the commands:

A screenshot of a computer error

Description automatically generatedA close up of words

Description automatically generated

I waited for approximately 2 minutes before using Ctrl+C to disrupt the command.

* 1. My first thought completing this portion was that I wished there was a way to write these commands into a txt file and have the shell execute them each in sequence from the file. The meaning of the commands: since each does not utilize the -t command, the rules are being added to the filter table. INPUT/OUTPUT means that the command applies to packets coming in or coming out (respectively). -A means the rule is being appended to the end of the table. -p allows specification of the protocol, in this case icmp. -j specifies what to do with the packet if it matches the rule given earlier, whether ACCEPT, DROP, QUEUE, or RETURN. For the second two command, the -P flag specifies a policy to apply, in this case dropping packets in and out.

1. Observations from Chapter 3.4 of the SEED lab document.
   1. My initial thought was to write a command that blocked any ping coming in from the 10.9.0.0/24 ip range, then specifically allow the router’s ip to be pinged from any host. Although my first thought was that all pings should be already allowed from internal to external hosts, but a rule could be written that expressly allows pings to the 10.9.0.0/24 range. To fulfill the final rule, I would want a rule that only allows icmp traffic (or negated, i.e. drop everything that isn’t a ping).
2. Observations from Chapter 3.5 of the SEED lab document.
   1. For the first rule, I would have to write a rule that drops all traffic on port 23 that is destined for any ip other than 192.168.60.5. Following that, I would have to allow all traffic coming from the 192.168.60.0/24 ip range, allowing the hosts to telnet to each other. To restrict the internal hosts from accessing external hosts, I would block all traffic outbound from the 192.168.60.0/24 ip range.