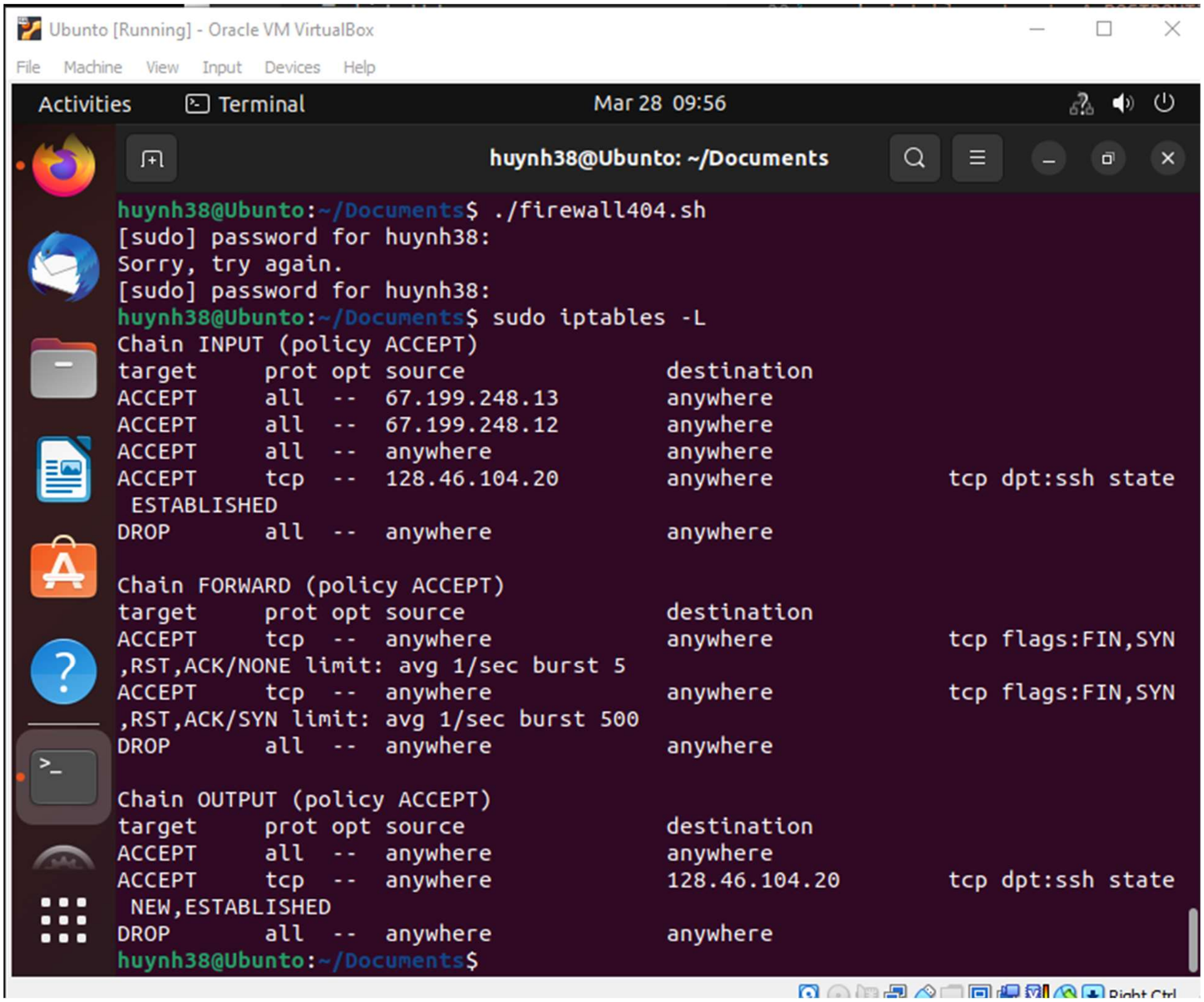
Homework Number: 9

Name: Dylan Huynh

ECN login: huynh38

Due Date: 3/28/2023

For this code, everything starts with sudo iptables because we are using the iptables command in Linux to configure settings of the firewall, and sudo is required because changing the firewall requires the permissions of a super user. In the first step, every rule is cleared and deleted from all 4 of the tables, allowing us to start fresh when creating the rules for the firewall. Next, we make a rule for the input chain of the filter table to accept packets from f1.com, using -s to denote that an address is coming next. Next, in the postrouting chain of the nat table, we use the masquerade target to change every outgoing IP to my own machine's IP. Next, I add a rule to the forward chain of the filter table, telling it for every tcp packet, that it limits the amount of syn packets it will accept to 1 per second, to stop nonstop scanning of ports. The next step defends against SYN-flooding by adding a rule to the forward chain of the filter table, telling to for tcp protocols, to limit SYN packets to one a second once the machine has reached 500 requests. The limit-burst flag places the limit where the limit flag, which denotes the amount of requests it will connect with per second, will start. I should point out that for the two rules I just mentioned, the --syn is the same as the above, looking for the SYN, ACK, FIN, and RST flags to be unset in the tcp header, except it looks for the SYN flag to be set, which is why is defends against SYN-Flooding and not scanning and vice-versa. The next two rules are for the input and output chains, which accept anything generated locally because the lo interface after the -I and -o respectively says this rule applies to locally generated packets only. The next rule is for the prerouting chain chain on the nat filter, which uses the dport flag to tell the rule that any tcp header who's destination port is 8888 will be redirected with the REDIRECT target to port 25565. To only allow ssh connections to engineering.purdue.edu, there is a filter on both the output and input chains on the filter table, using the destination port 22 because that is the port for SSH connections, and then the respective -d or -s for destination or source, respectively, to engineering.purdue.edu, whose ip address is 128.46.104.20. The added new field in the state output is because outgoing connections could also be new, and would thus also need to be accepted. The last rule is on all chains of the filter table, dropping any packets with the drop target, and must be done last as to not drop every packet.

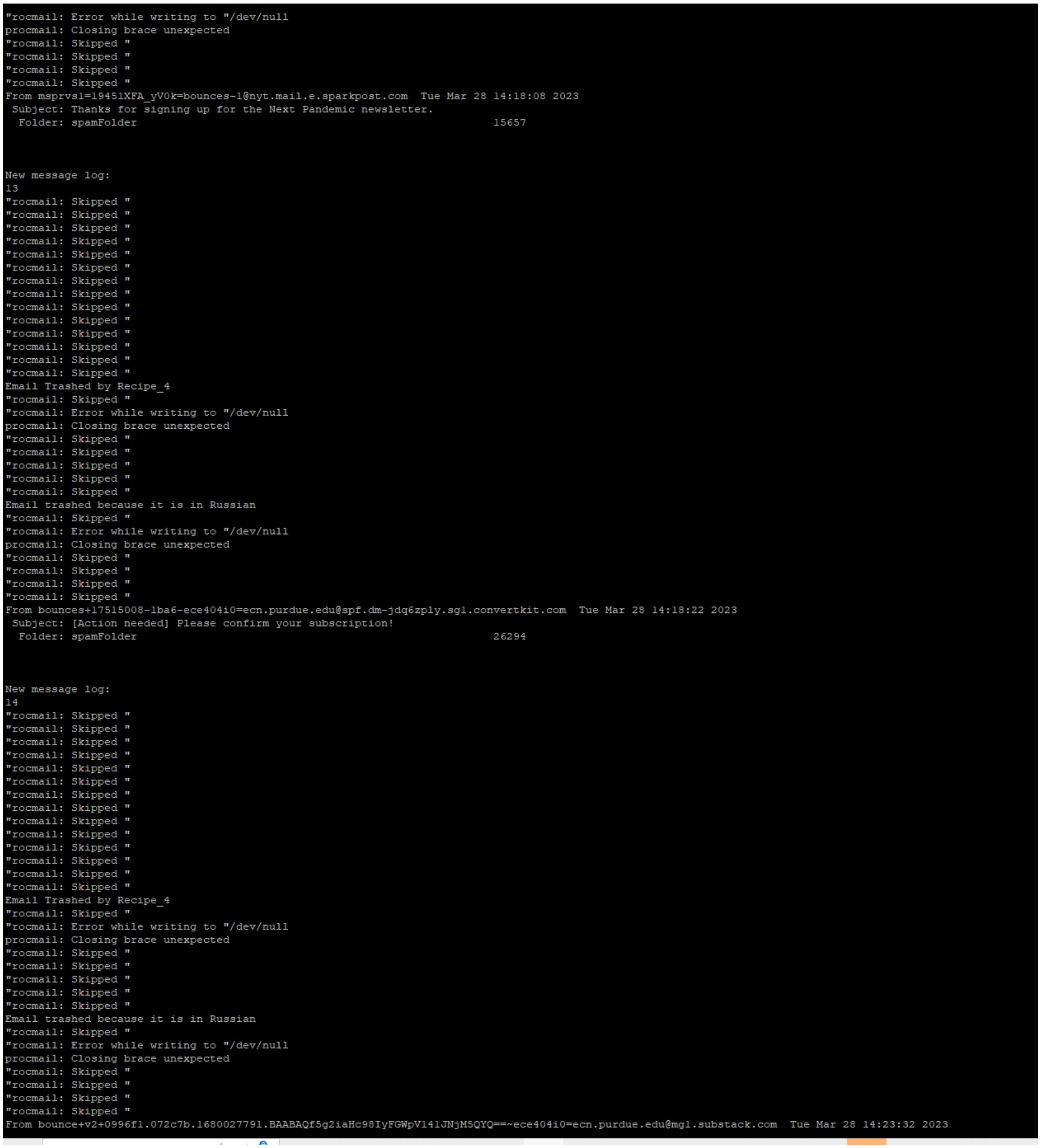


Ubunto [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mar 28 09:56
huynh38@Ubunto: ~/Documents
Right Ctrl

```
huynh38@Ubunto:~/Documents$ ./firewall404.sh
[sudo] password for huynh38:
Sorry, try again.
[sudo] password for huynh38:
huynh38@Ubunto:~/Documents$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  67.199.248.13        anywhere
ACCEPT     all  --  67.199.248.12        anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  128.46.104.20        anywhere             tcp dpt:ssh state
 ESTABLISHED
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN
,RST,ACK/NONE limit: avg 1/sec burst 5
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN
,RST,ACK/SYN limit: avg 1/sec burst 500
DROP       all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             128.46.104.20        tcp dpt:ssh state
 NEW,ESTABLISHED
DROP       all  --  anywhere             anywhere
huynh38@Ubunto:~/Documents$
```



```
"rocmail: Error while writing to "/dev/null
procmail: Closing brace unexpected
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
From msprvs1=19451XFA_yV0k=bounces-1@nyt.mail.e.sparkpost.com  Tue Mar 28 14:18:08 2023
 Subject: Thanks for signing up for the Next Pandemic newsletter.
  Folder: spamFolder                                                     15657



New message log:
13
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
Email Trashed by Recipe_4
"rocmail: Skipped "
"rocmail: Error while writing to "/dev/null
procmail: Closing brace unexpected
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
Email trashed because it is in Russian
"rocmail: Skipped "
"rocmail: Error while writing to "/dev/null
procmail: Closing brace unexpected
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
From bounces+17515008-1ba6-ece404i0=ecn.purdue.edu@spf.dm-jdq6zply.sgl.convertkit.com  Tue Mar 28 14:18:22 2023
 Subject: [Action needed] Please confirm your subscription!
  Folder: spamFolder                                                     26294



New message log:
14
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
Email Trashed by Recipe_4
"rocmail: Skipped "
"rocmail: Error while writing to "/dev/null
procmail: Closing brace unexpected
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
Email trashed because it is in Russian
"rocmail: Skipped "
"rocmail: Error while writing to "/dev/null
procmail: Closing brace unexpected
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
"rocmail: Skipped "
From bounce+v2+0996f1.072c7b.1680027791.BAABAQf5g2iaHc98IyFGWpV141JNjM5QYQ==~ece404i0=ecn.purdue.edu@mgl.substack.com  Tue Mar 28 14:23:32 2023
```