IP TABLES - THE LINUX FIREWALL

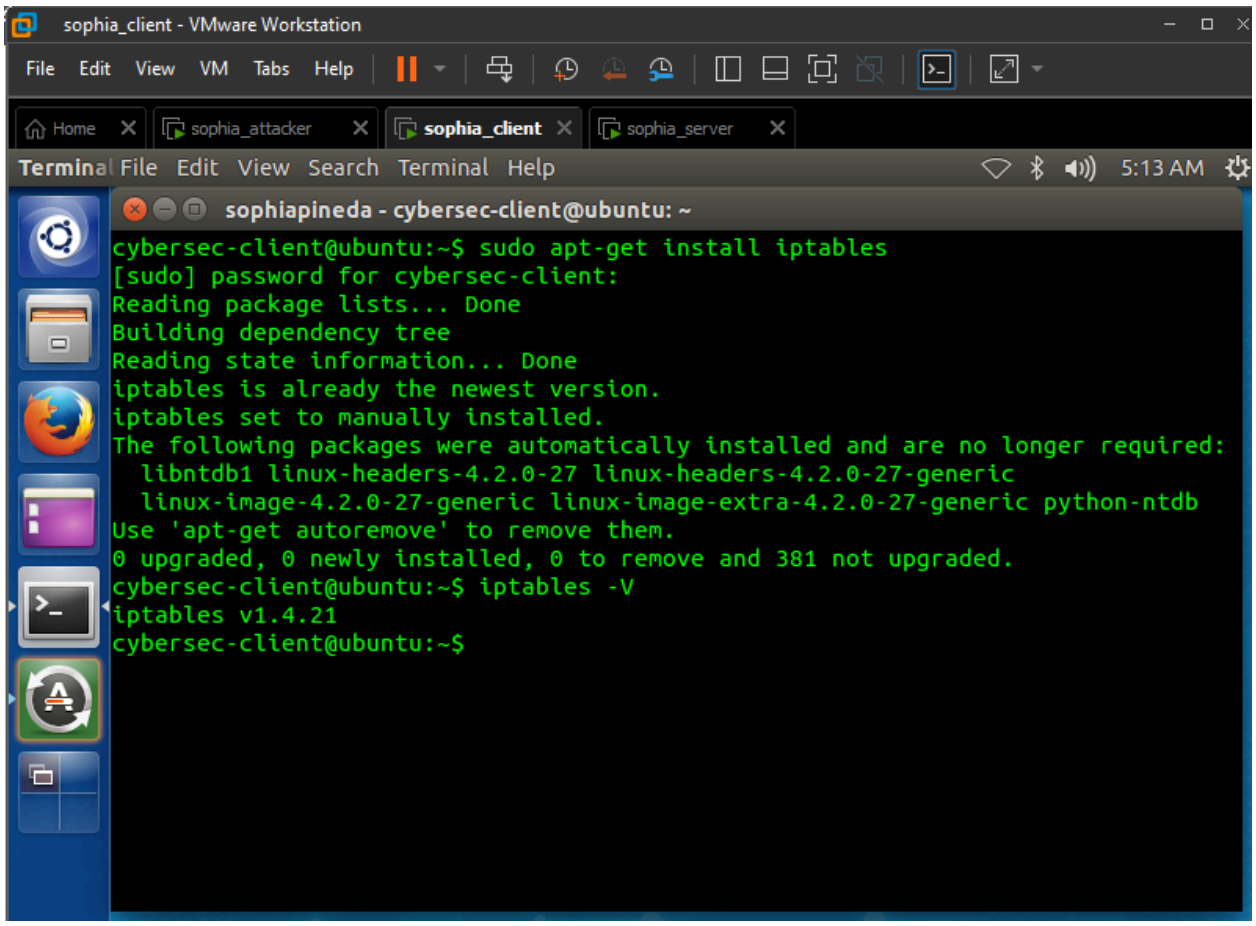
LAB

- All three VMS

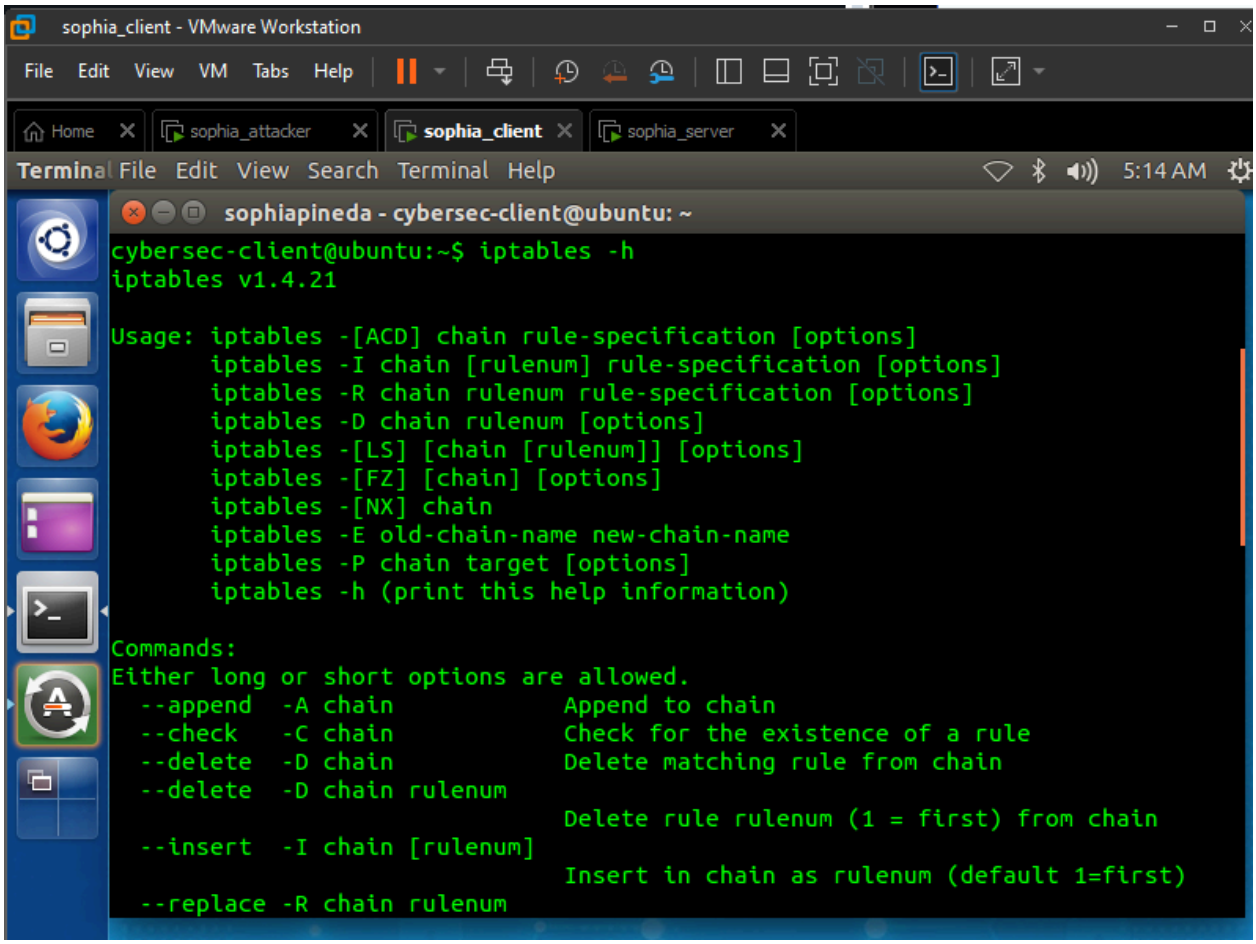
TASK: CONFIGURE IPTABLES FIREWALL RULES ON CYBER-CLIENT

STEPS

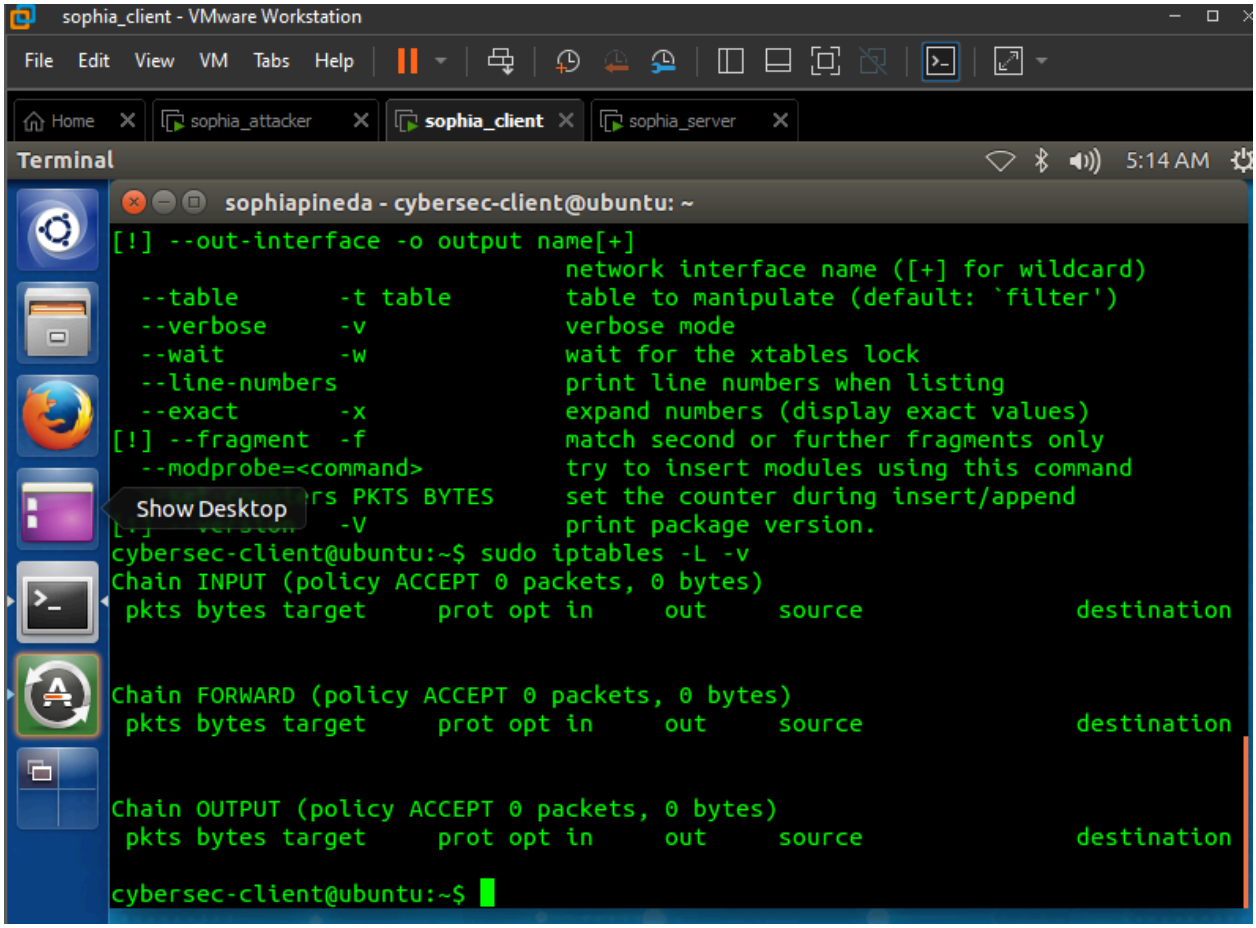
1. Enter sudo apt-get install iptables in client VM (install iptables package)
2. Enter iptables -V in client VM (Check version of iptables installed in system) SCREENSHOT



3. Enter iptables -h (checks usage of iptables) SCREENSHOT

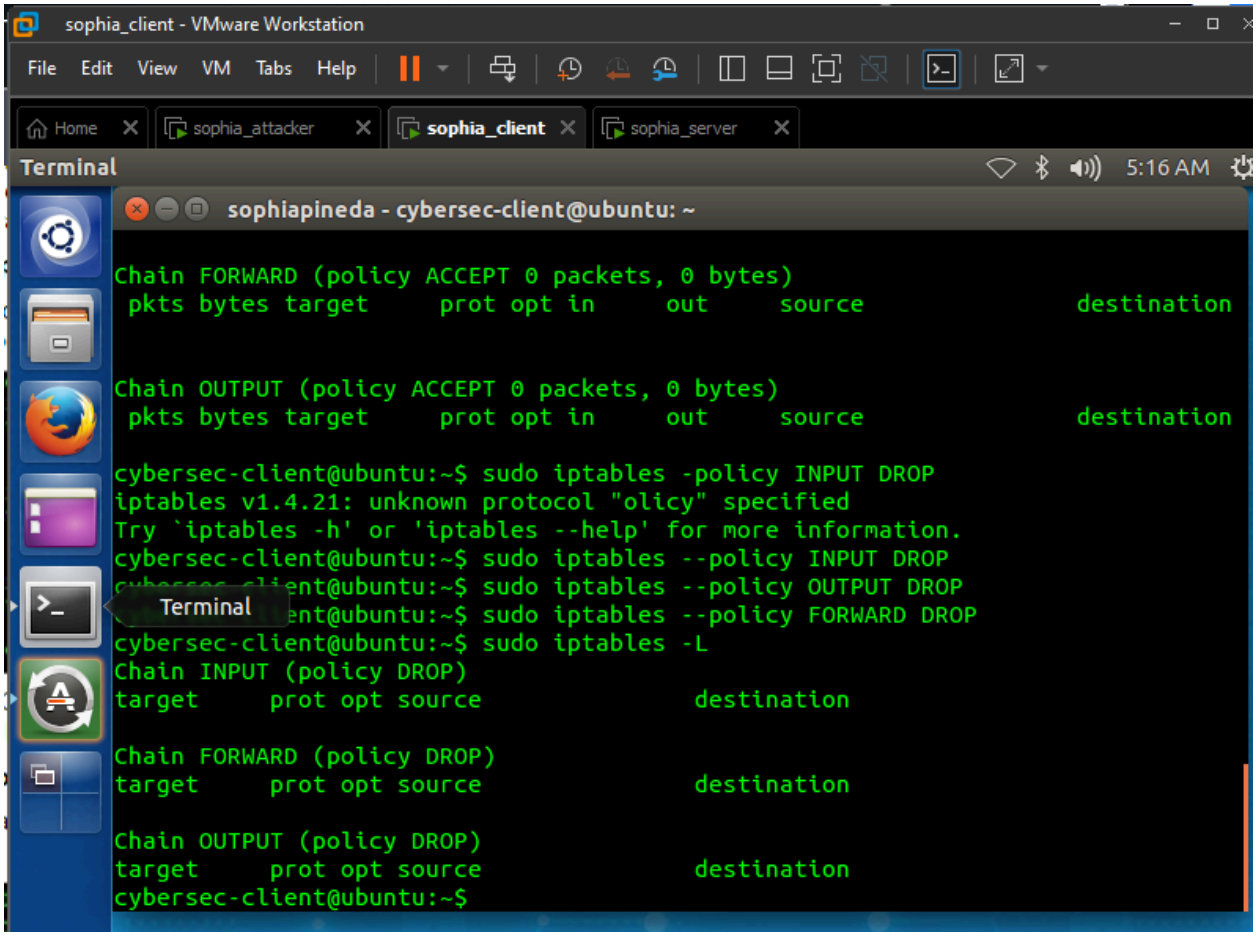


4. Enter sudo iptables -L -v (checks current iptables chains and checks number of packets accepted or denied) SCREENSHOT

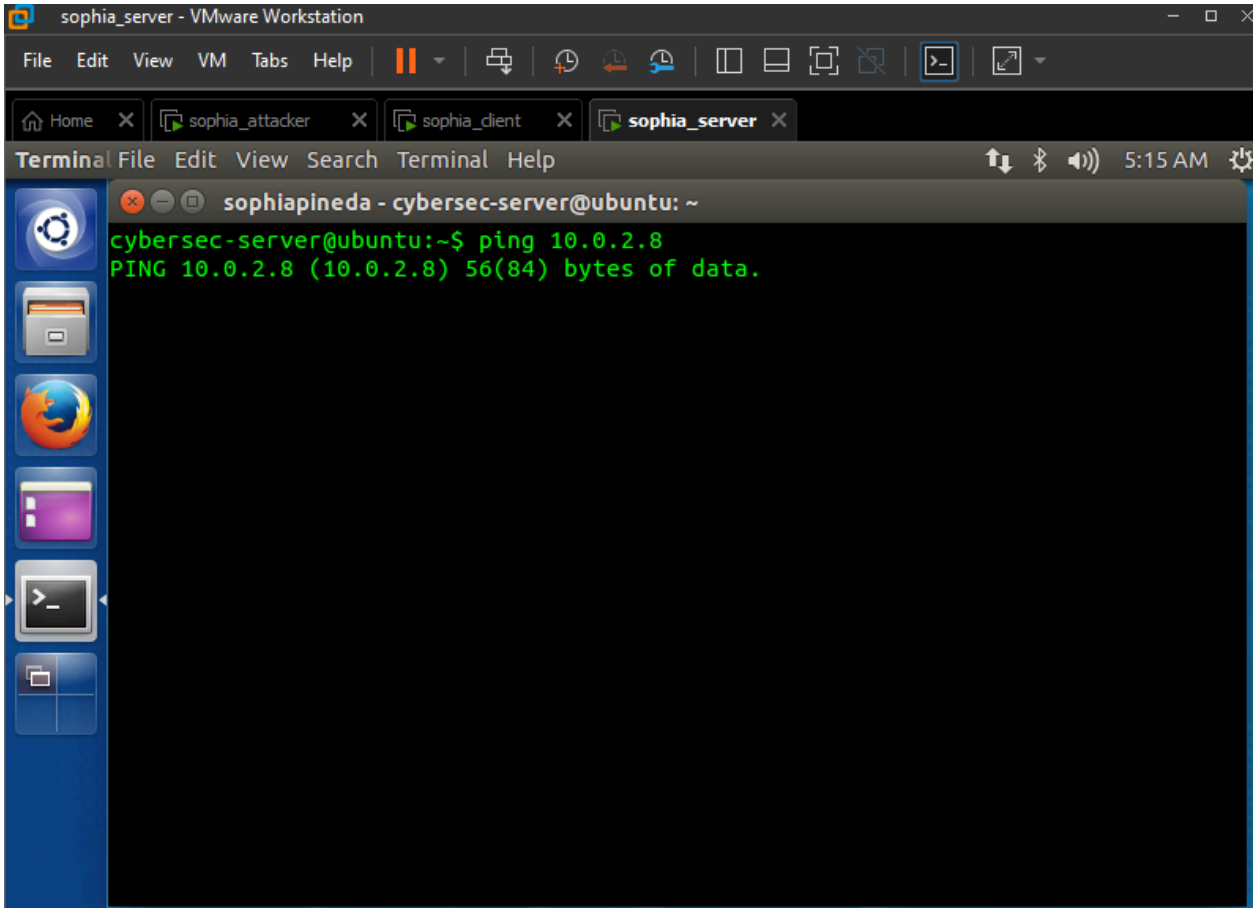


(changes behaviour of chain to drop all traffic) SCREENSHOT

5. Enter sudo iptables –policy INPUT DROP in client VM
6. Enter sudo iptables –policy OUTPUT DROP
7. Enter sudo iptables –policy FORWARD DROP

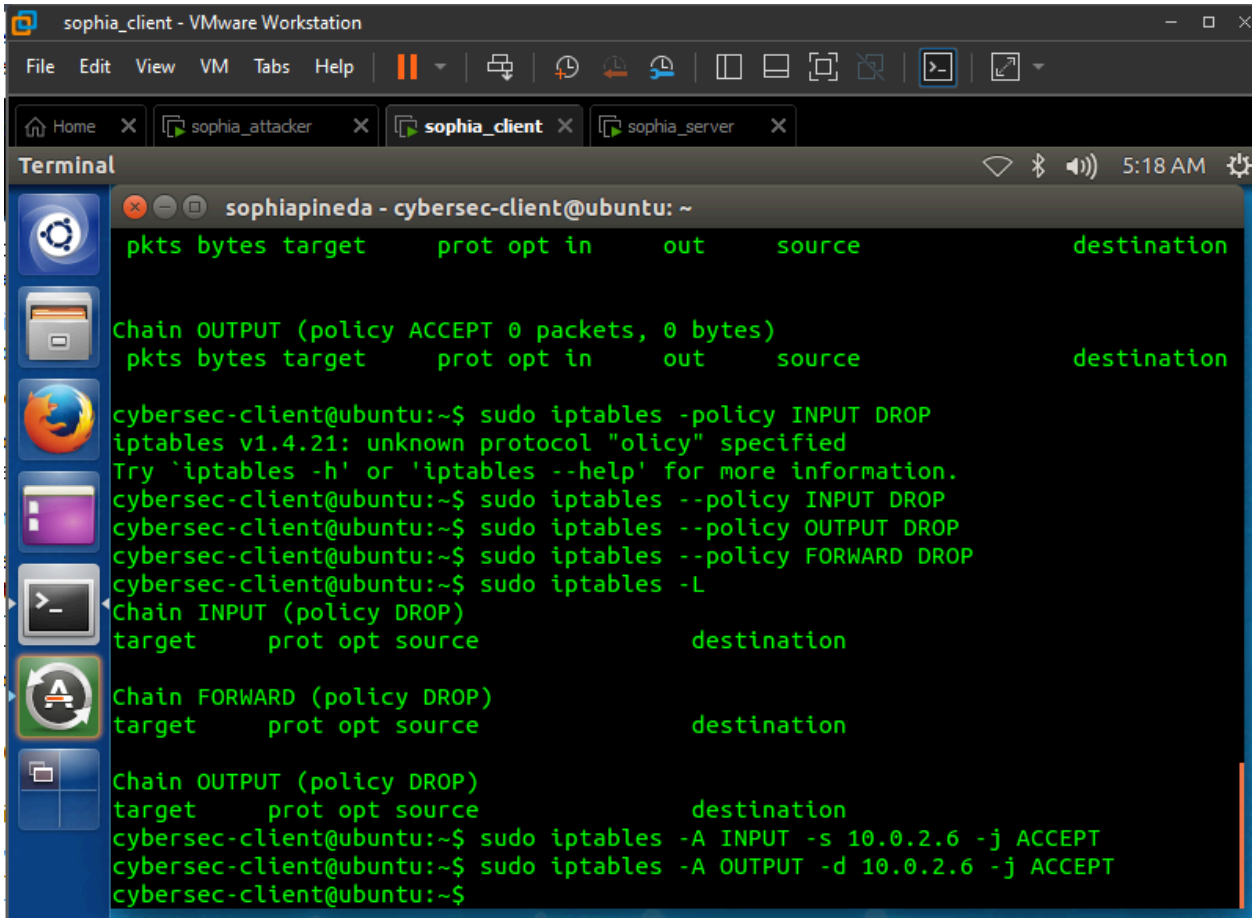


8. Enter sudo iptables -L
9. Enter ping 10.0.2.8 in server VM

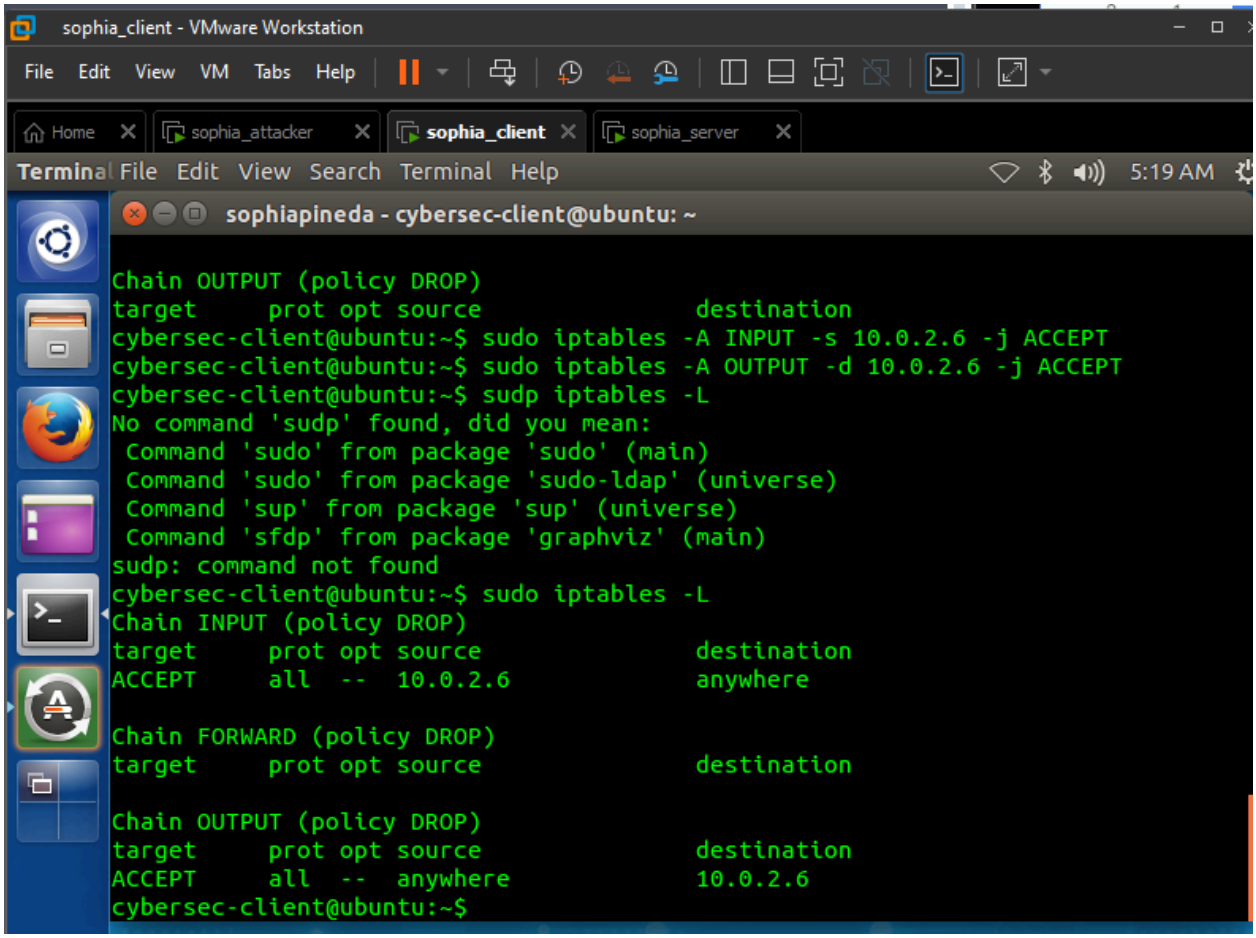


(adding rules to permit connection between server and client) SCREENSHOT

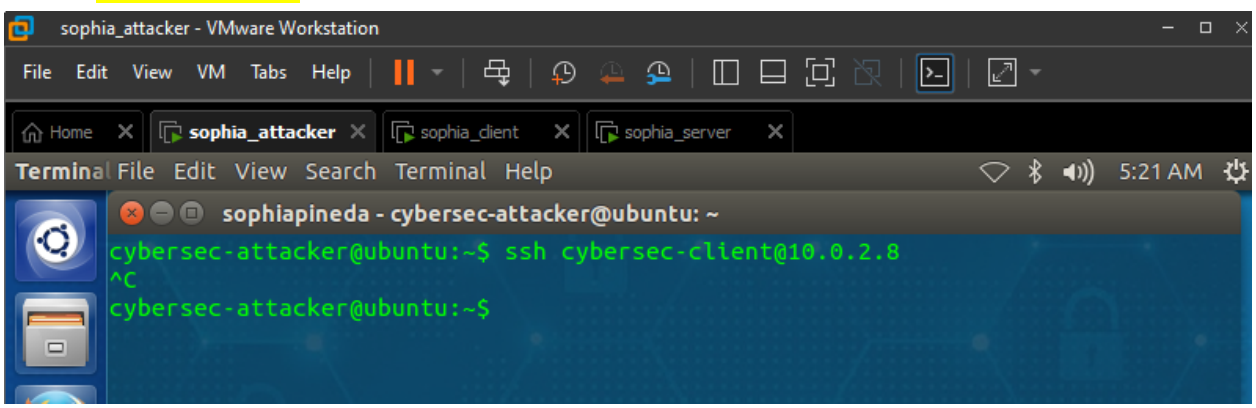
10. Enter sudo iptables -A INPUT -s 10.0.2.6 -j ACCEPT in client VM
11. Enter sudo iptables -A INPUT -d 10.0.2.6 -j ACCEPT



12. Enter sudo iptables -L in client VM (checks rules) SCREENSHOT

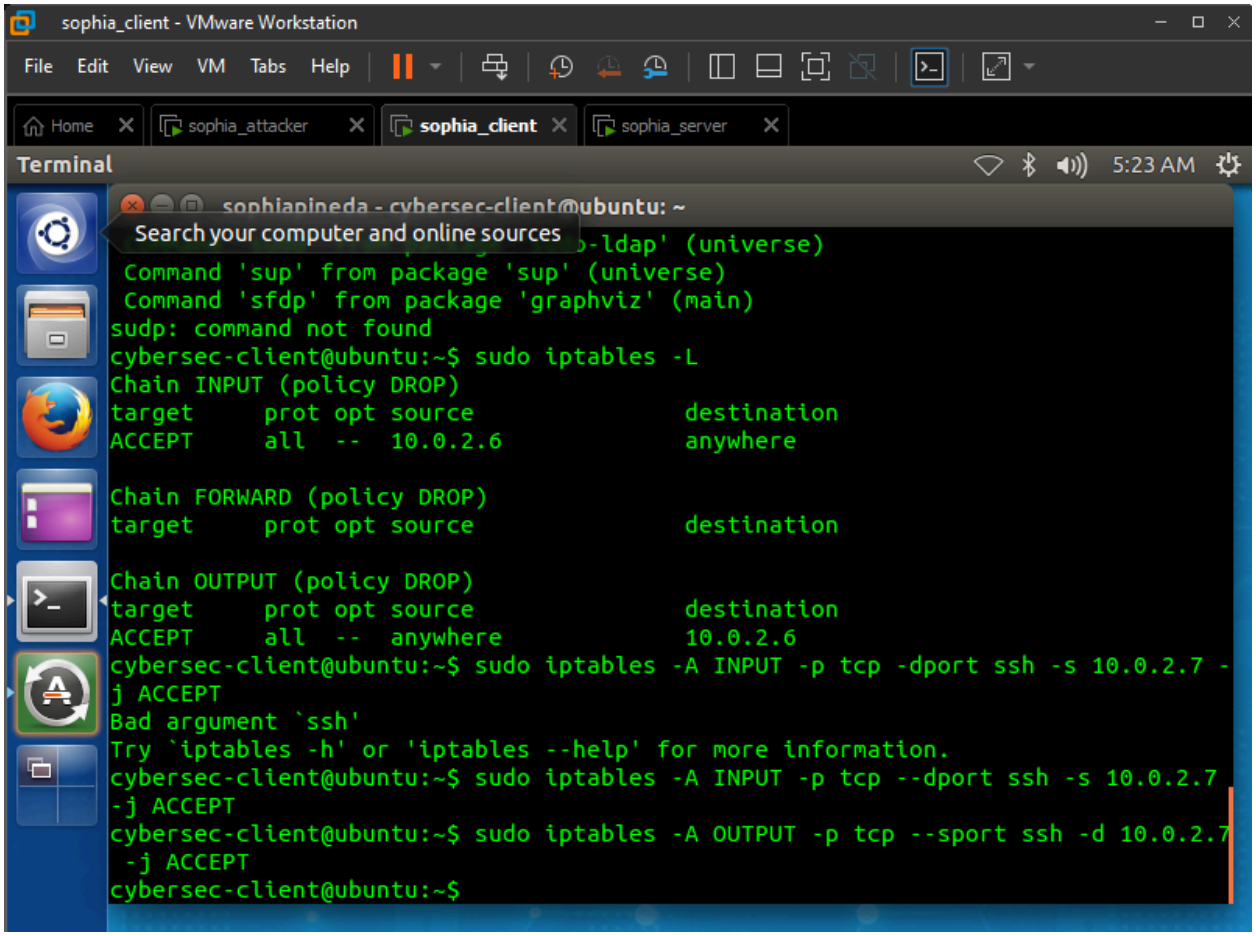


13. Enter ssh cybersec-client@10.0.2.8 in attacker VM (creates SHH connection) SCREENSHOT



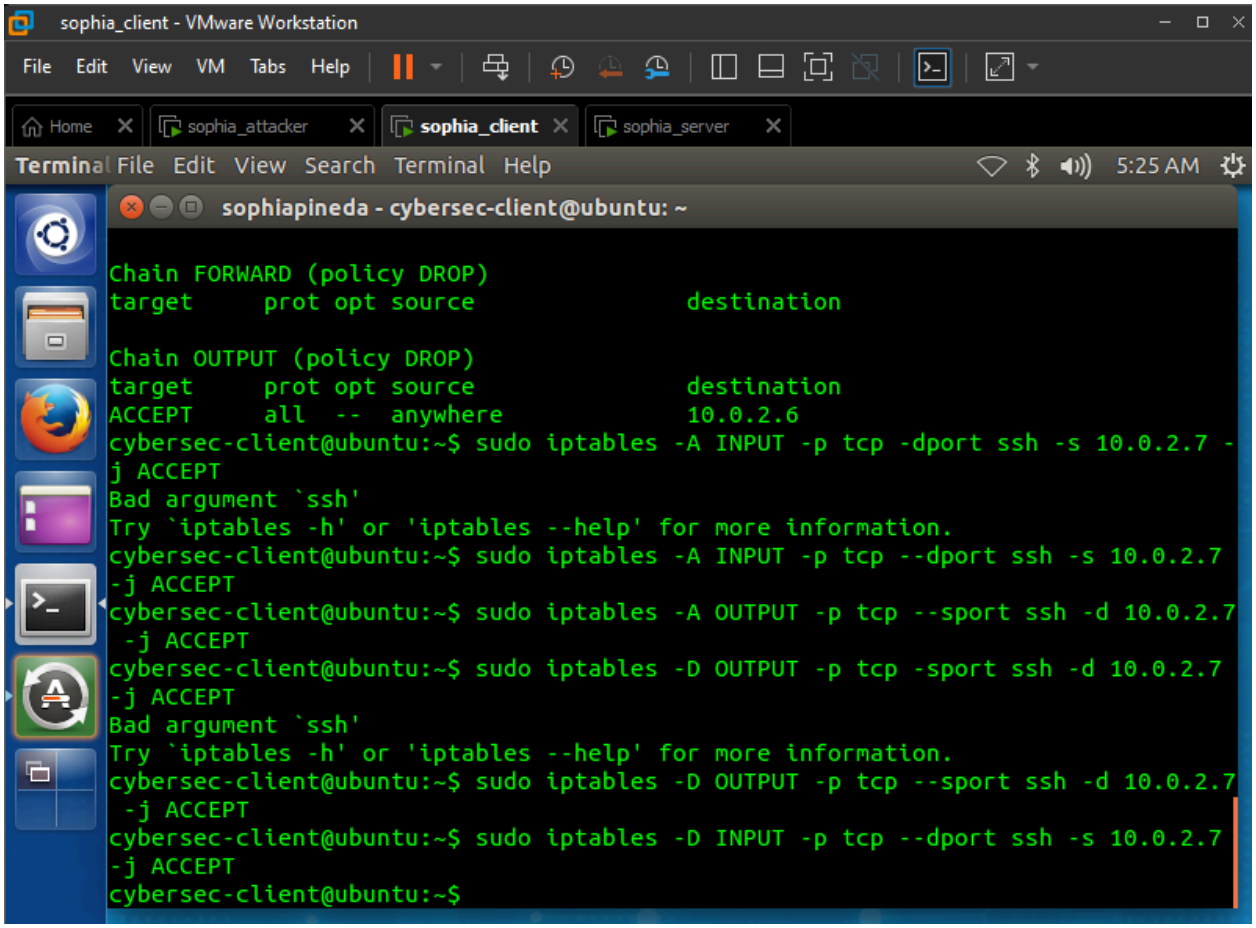
(adding rules to permit SHH connection) SCREENSHOT

14. Enter sudo iptables -A INPUT -p tcp –dport ssh -s 10.0.2.7 -j ACCEPT in client VM
15. Enter sudo iptables -A OUTPUT -p tcp –sport ssh -d 10.0.2.7 -j ACCEPT in client VM



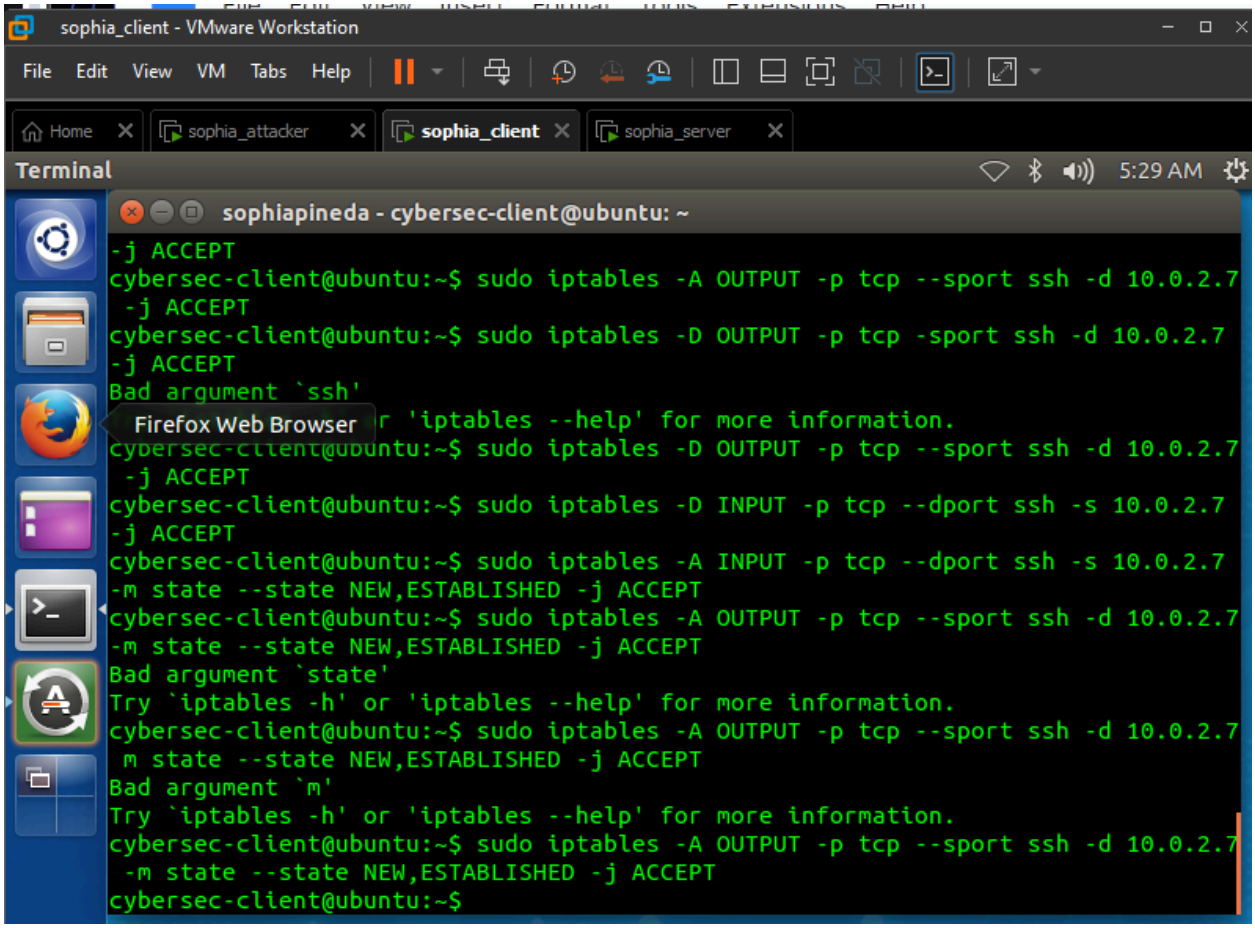
(remove rules) SCREENSHOT

16. Enter sudo iptables -D OUTPUT -p tcp –sport ssh -d 10.0.2.7 -j ACCEPT in client VM
17. Enter sudo iptables -D INPUT -p tcp –dport ssh -s 10.0.2.7 -j ACCEPT in client VM



18. Reconfigure rules -

cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport ssh -s 10.0.2.7 -m state --state NEW,ESTABLISHED -j ACCEPT cybersec-client@ubuntu:~$ sudo iptables -A OUTPUT -p tcp --sport ssh -d 10.0.2.7 m state --state NEW,ESTABLISHED -j ACCEPT

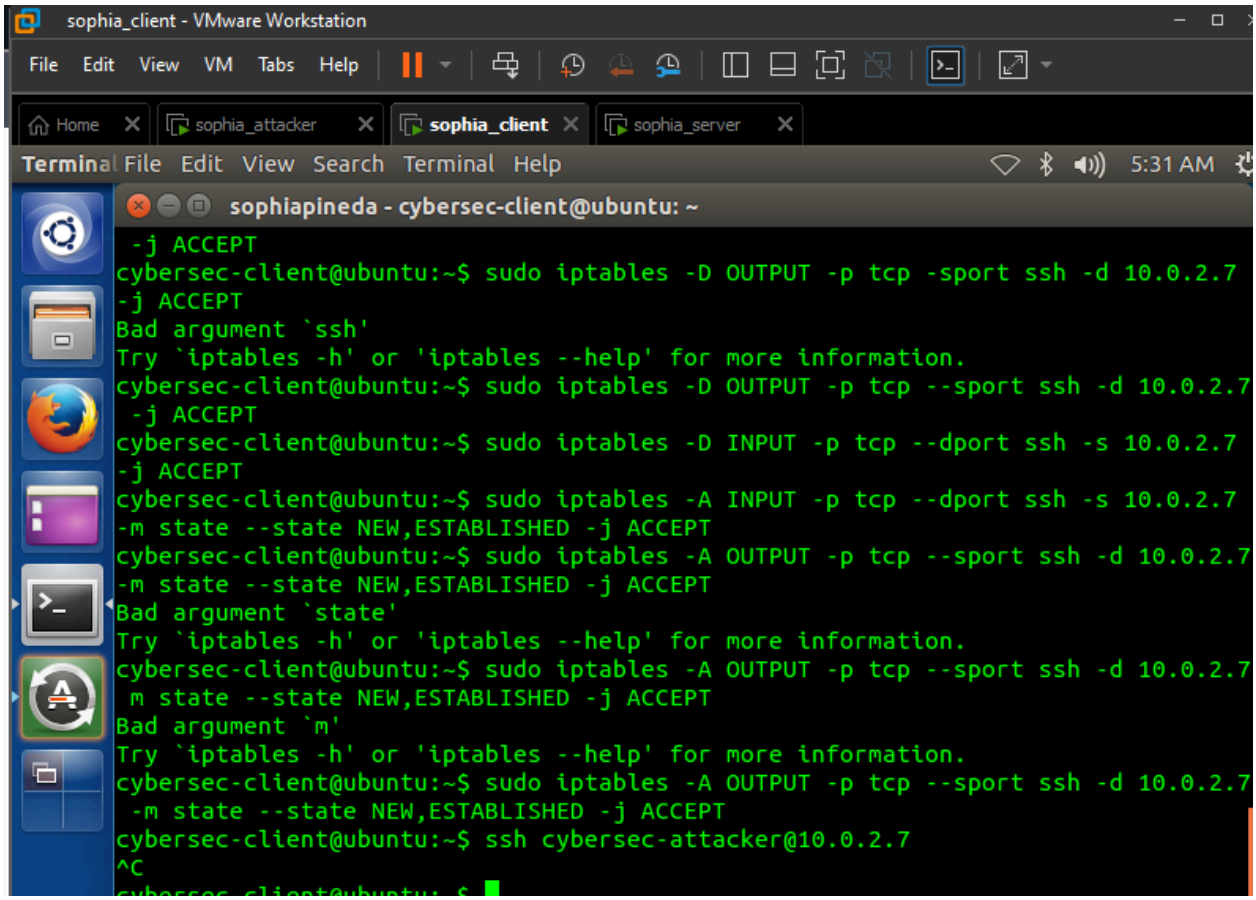


(verifies SHH connection between attacker and client) SCREENSHOT

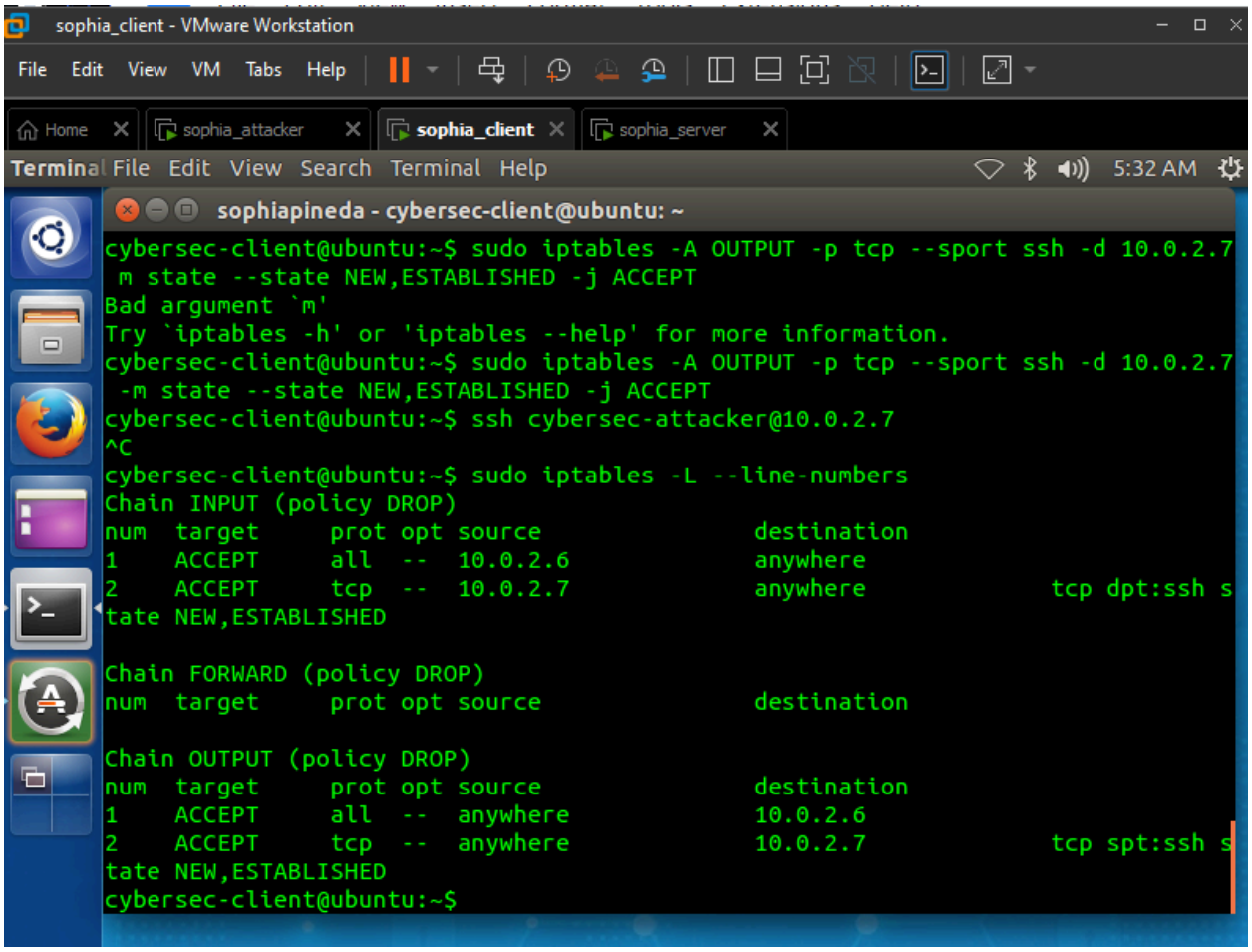
19. Enter sudo iptables -A INPUT -p tcp –dport ssh -s 10.0.2.7 -m state –state NEW,ESTABLISHED -j ACCEPT in client VM
20. Enter sudo iptables -A OUTPUT -p tcp –sport ssh -d 10.0.2.7 -m state –state NEW,ESTABLISHED -j ACCEPT in client VM

21. Enter shh cybersec-client@10.0.2.8 in attacker VM SCREENSHOT


sophia_attacker - VMware Workstation
File Edit View VM Tabs Help
Home
sophia_attacker
sophia_client
sophia_server
Terminal File Edit View Search Terminal Help
5:30 AM
sophiapineda - cybersec-client@ubuntu: ~
cybersec-attacker@ubuntu:~$ ssh cybersec-client@10.0.2.8
^C
cybersec-attacker@ubuntu:~$ ssh cybersec-client@10.0.2.8
The authenticity of host '10.0.2.8 (10.0.2.8)' can't be established.
ECDSA key fingerprint is 9a:97:a9:8f:03:2e:aa:66:fc:d0:6e:26:ed:e9:10:7b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.8' (ECDSA) to the list of known hosts.
cybersec-client@10.0.2.8's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.2.0-42-generic x86_64)
* Documentation: https://help.ubuntu.com/
381 packages can be updated.
309 updates are security updates.
Last login: Mon Sep 16 05:29:09 2024 from 10.0.2.6
cybersec-client@ubuntu:~$
Cyber Security

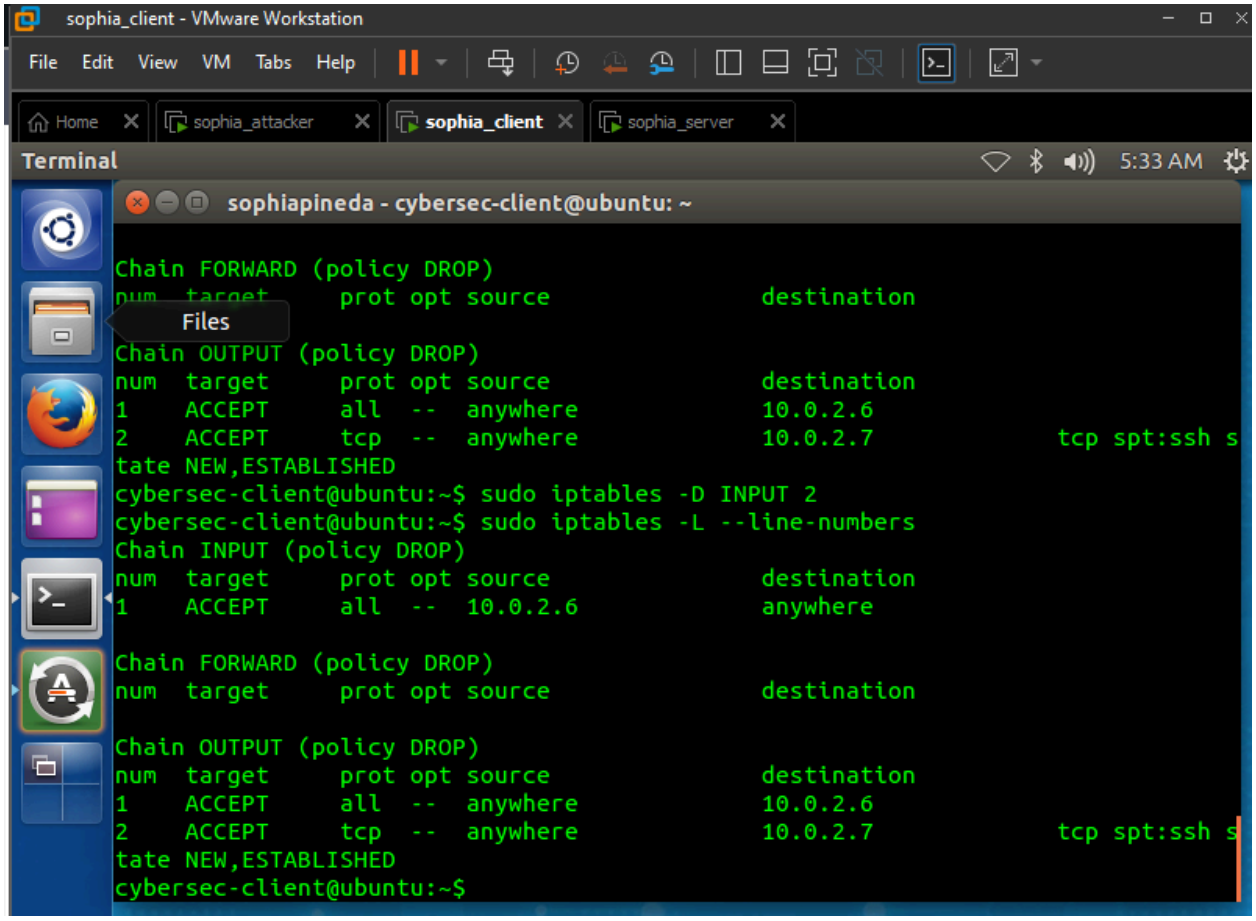


22. Enter sudo iptables -L –line-numbers in client VM SCREENSHOT

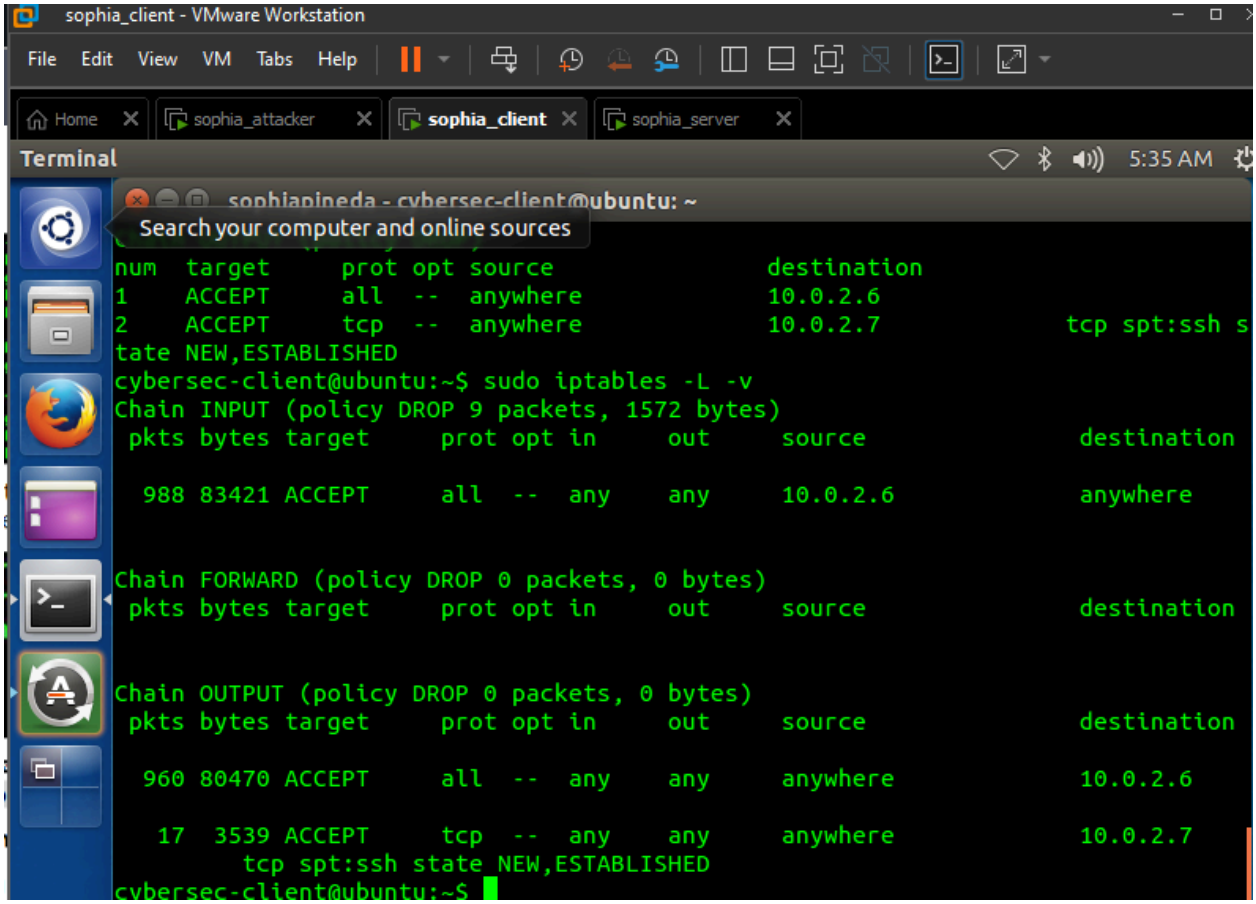


SCREENSHOT

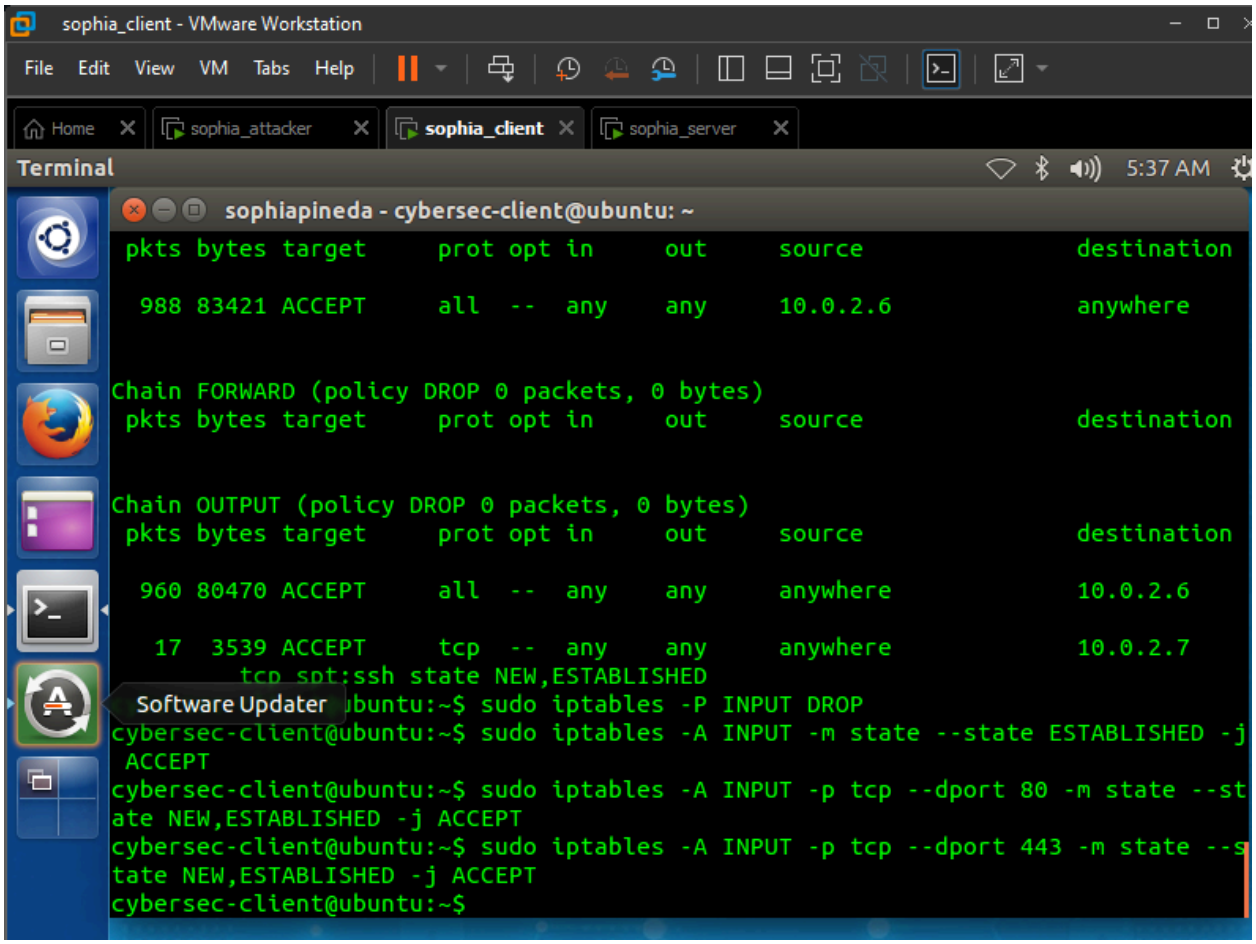
23. Enter sudo iptables -D INPUT 2
24. Enter sudo iptables -L –line-numbers



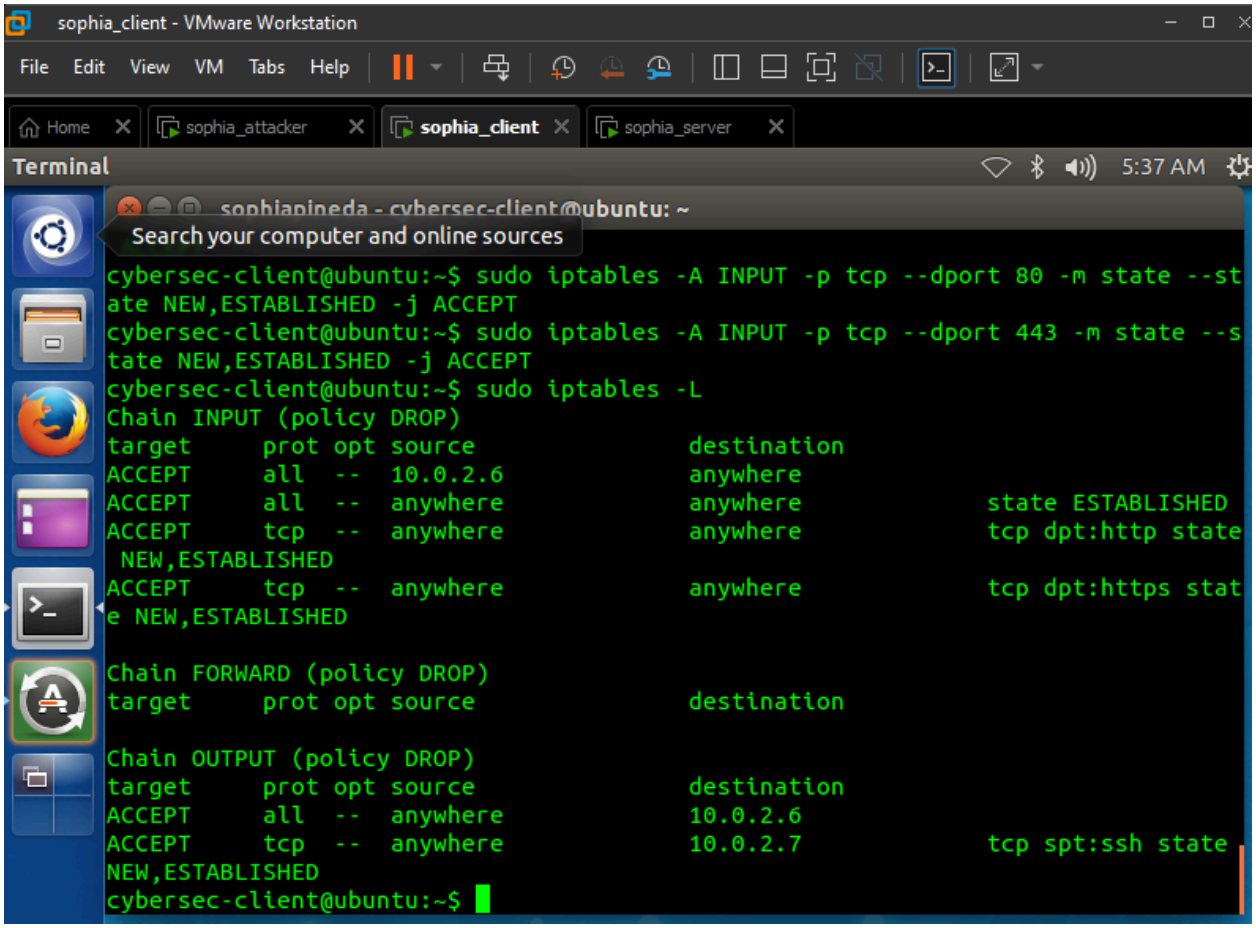
CHALLENGE
Screenshot Required:



1. Commands used to configure Iptables on Cybersec-Server to permit HTTP, HTTPS and drop other traffic.



2. Iptables chain after adding the rules. (sudo iptables -L)


sophia_client - VMware Workstation
File Edit View VM Tabs Help
Home
sophia_attacker
sophia_client
sophia_server
Terminal
5:37 AM
sophiapineda - cybersec-client@ubuntu: ~
Search your computer and online sources
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 80 -m state --st
ate NEW,ESTABLISHED -j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 443 -m state --s
tate NEW,ESTABLISHED -j ACCEPT
cybersec-client@ubuntu:~$ sudo iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- 10.0.2.6 anywhere
ACCEPT all -- anywhere anywhere state ESTABLISHED
ACCEPT tcp -- anywhere anywhere tcp dpt:http state
NEW,ESTABLISHED
ACCEPT tcp -- anywhere anywhere tcp dpt:https stat
e NEW,ESTABLISHED
Chain FORWARD (policy DROP)
target prot opt source destination
Chain OUTPUT (policy DROP)
target prot opt source destination
ACCEPT all -- anywhere 10.0.2.6
ACCEPT tcp -- anywhere 10.0.2.7 tcp spt:ssh state
NEW,ESTABLISHED
cybersec-client@ubuntu:~$