SNORT

- Most popular open-source intrusion prevention system: does traffic analysis + packet logging on IP networks
- Defines malicious network activity
- Finds packets that match against them, generating alerts
- Three primary uses: packet sniffer, packet logger for network traffic debugging, full-blown network intrusion prevention system

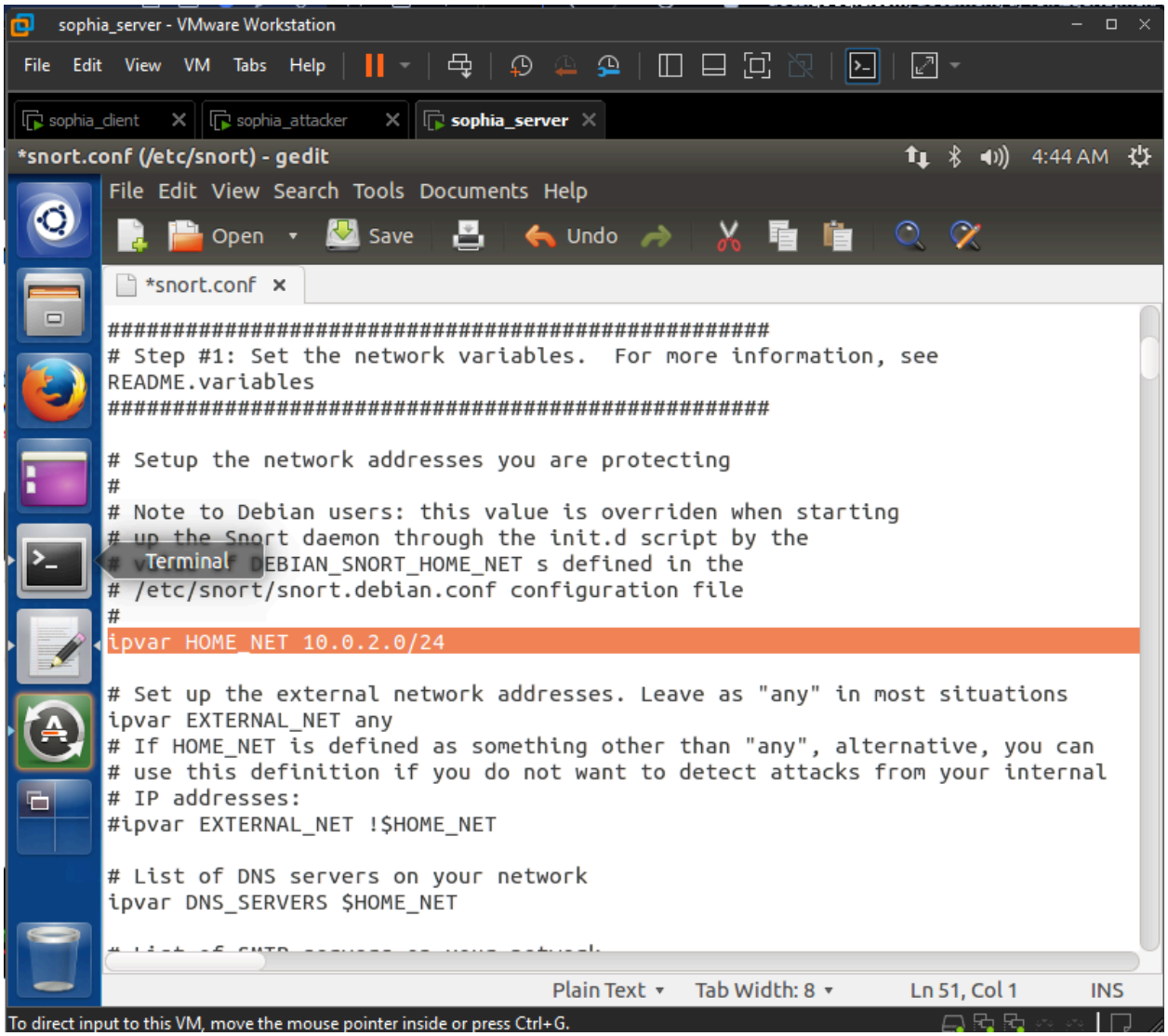
LAB ENVIRONMENT

- Server, Attacker VM
- 10.0.2.6 is server, 10.0.2.7 is attacker and 10.0.2.8 client

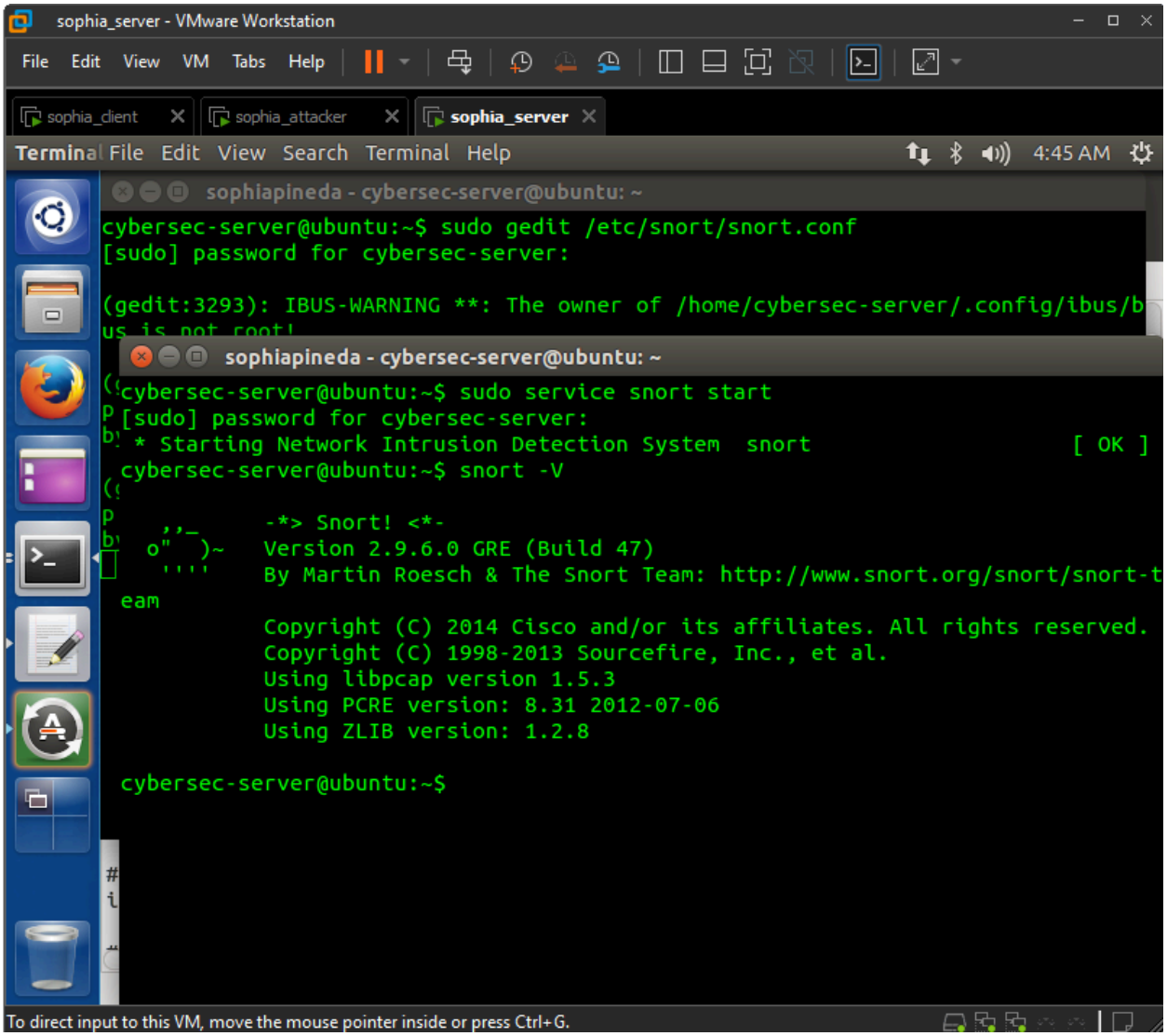
SNORT RULES

STEPS

1. Enter sudo gedit /etc/snort/snort.conf in serverVM (configuring snort rules)



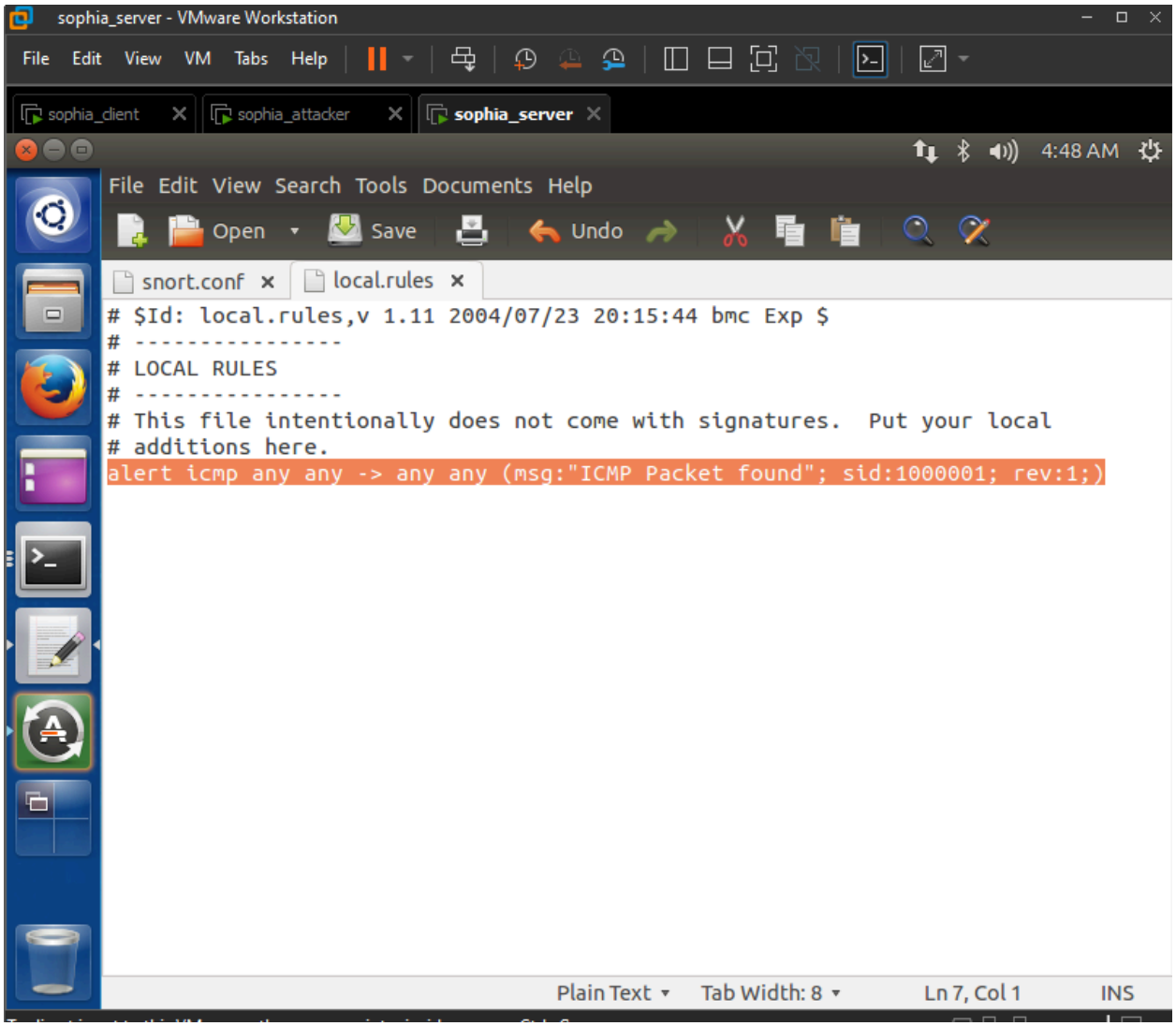
2. Enter sudo service snort start
3. Enter snort -V
4. Enter ls /ect/snort/rules (checks snort rules)



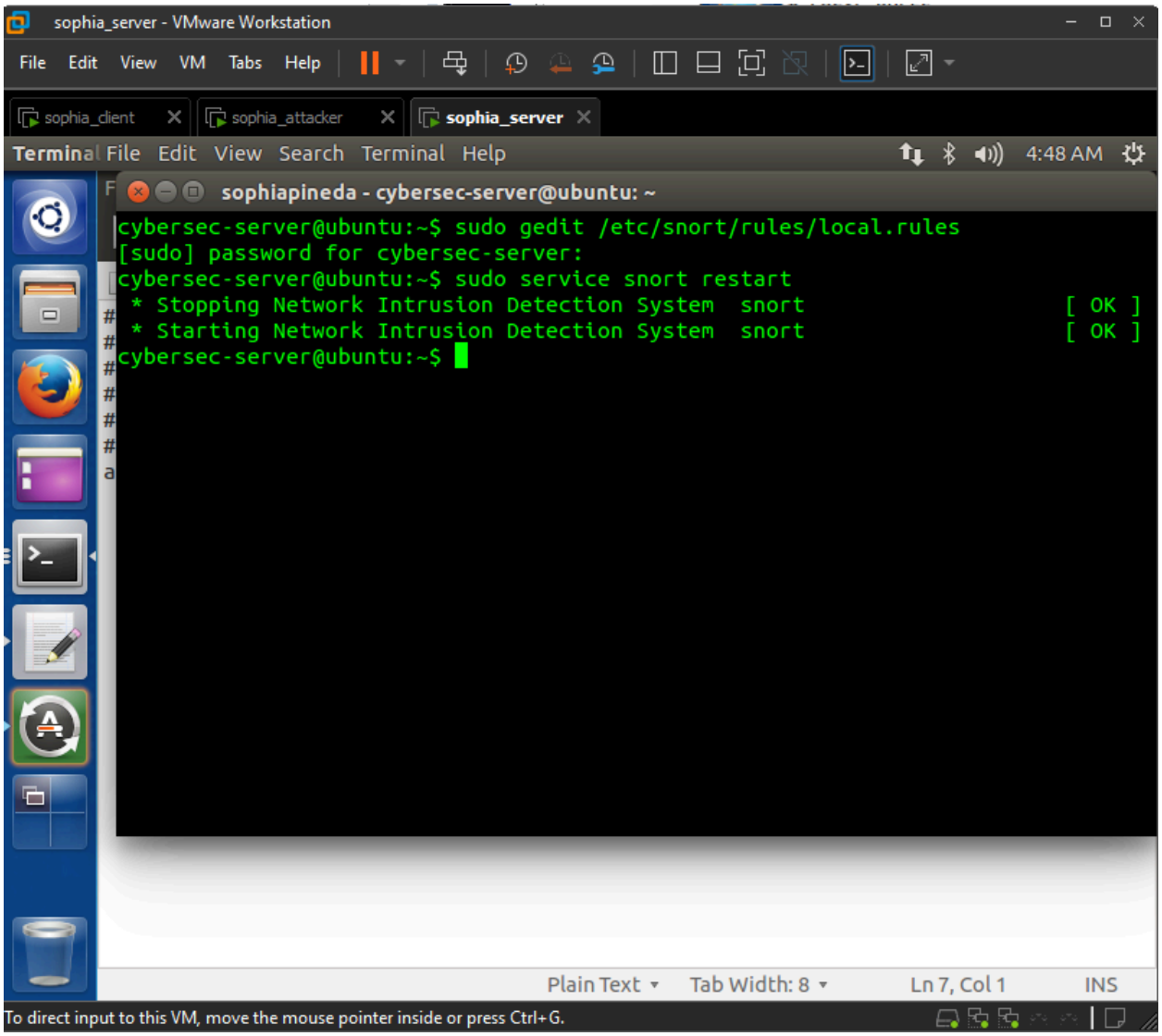
TASK 1: ADDING A RULE FOR ICMP PACKETS

STEPS

1. Enter sudo gedit /etc/snort/rules/local.rules in serverVM
2. Add “alert icmp any any -> any any (msg:"ICMP Packet found"; sid:1000001; rev:1;)” in file

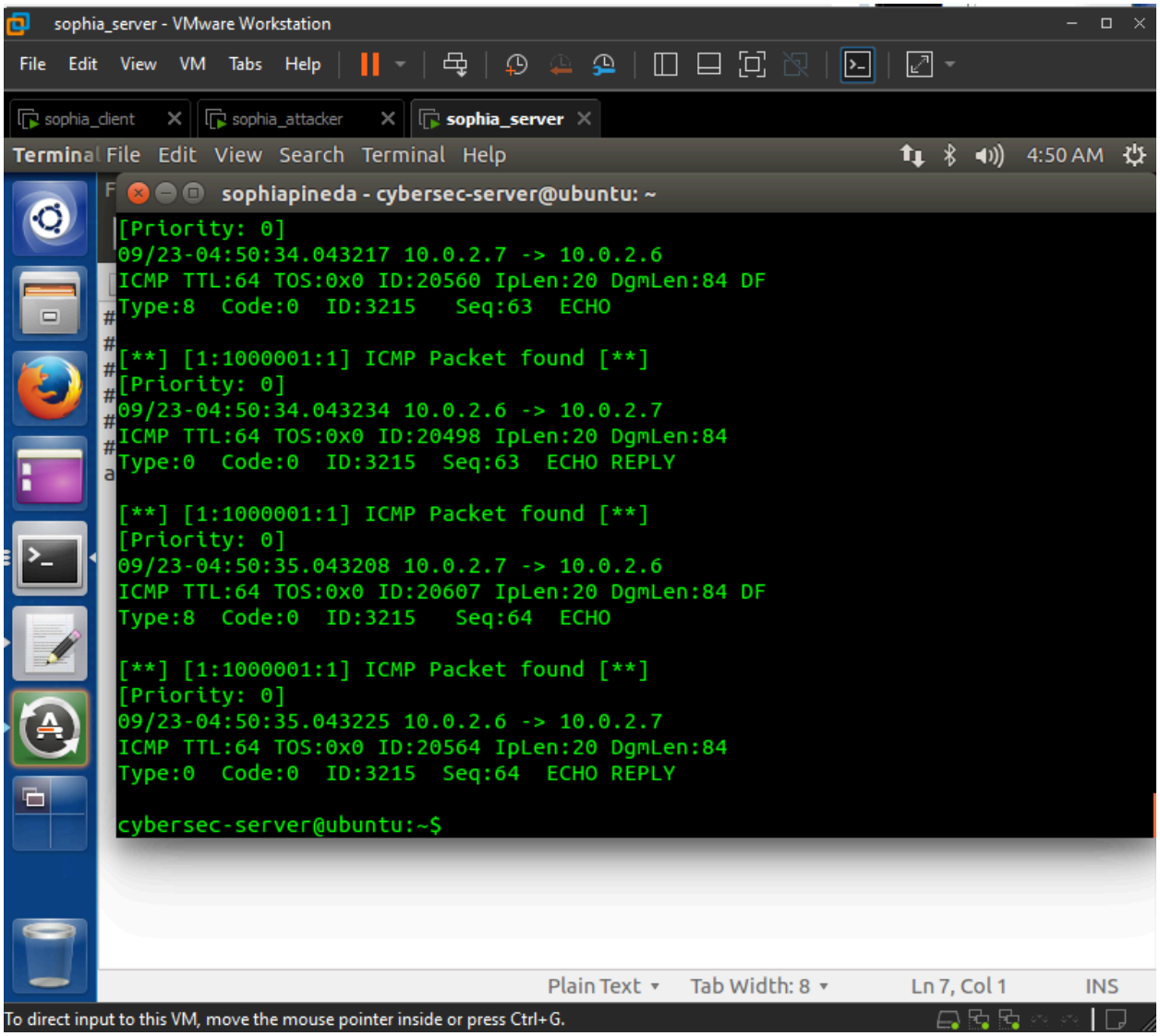


3. Enter sudo service snort restart



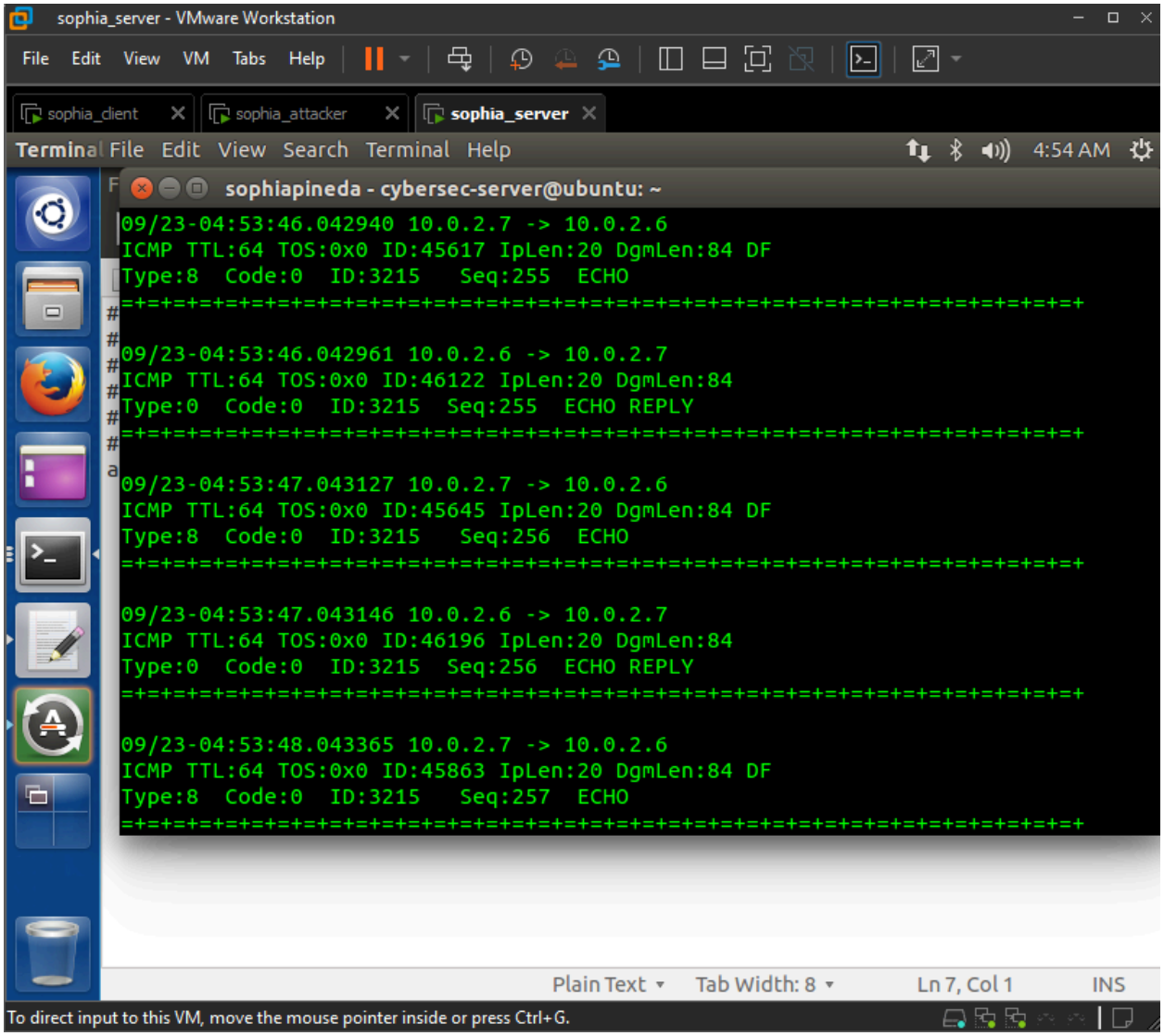
4. Enter ping 10.0.2.6 in attackerVM

5. Enter cat /var/log/snort/alert in serverVM



QUESTION 1. Have you received alert messages for ICMP Packets? Please provide screenshot to support your answer

- Ls /var/log/snort/ in serverVM
- Enter sudo snort -r /var/log/snort/snort.log.1663555616" in server VM

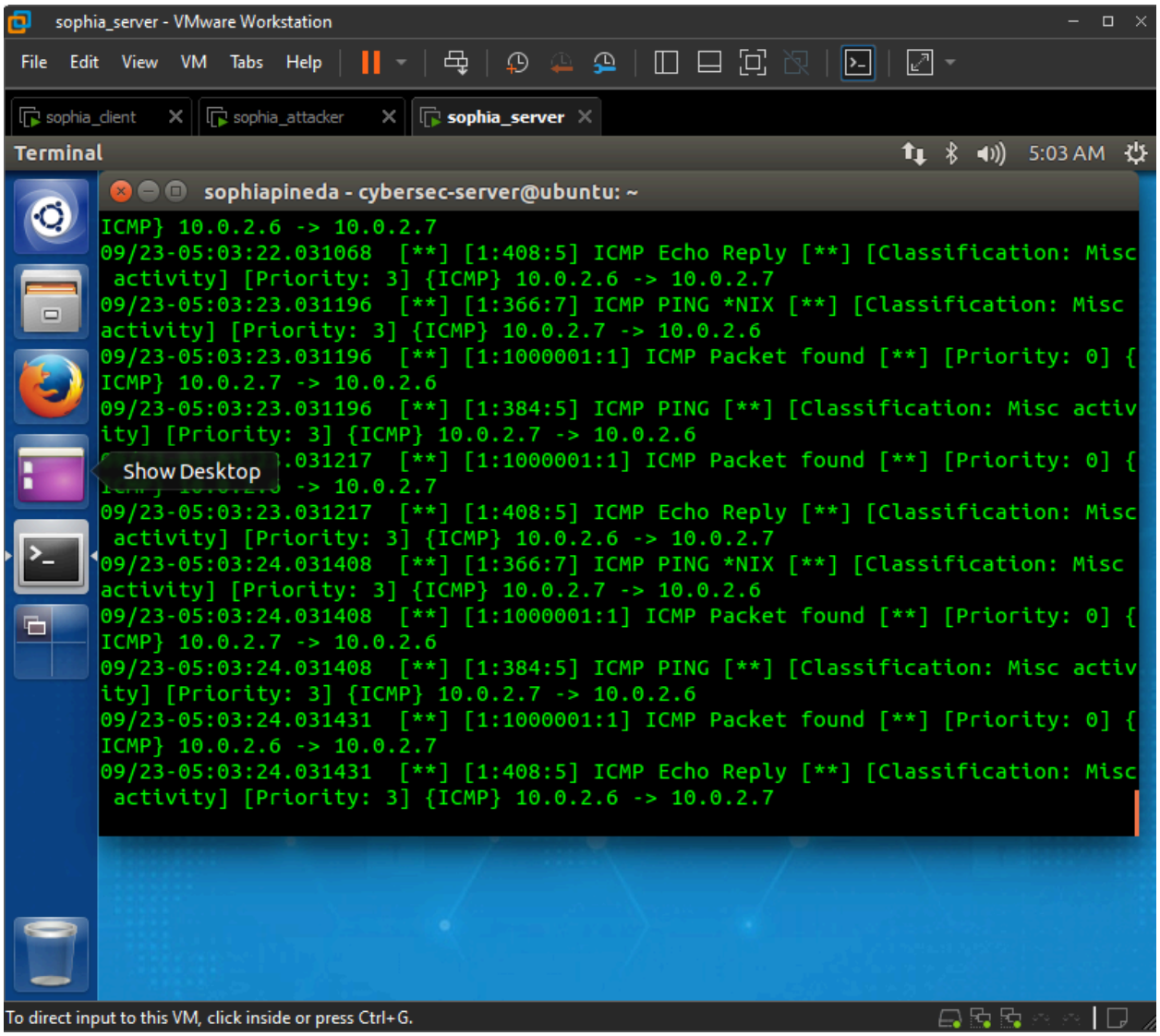


TASK 2: SNORT IN IDS MODE AND DISPLAYING ALERTS TO CONSOLE

STEPS

1. Enter sudo snort -A console -q -c /etc/snort/snort.conf -i eth0 in severVM
2. Enter ping 10.0.2.6 in attackerVM

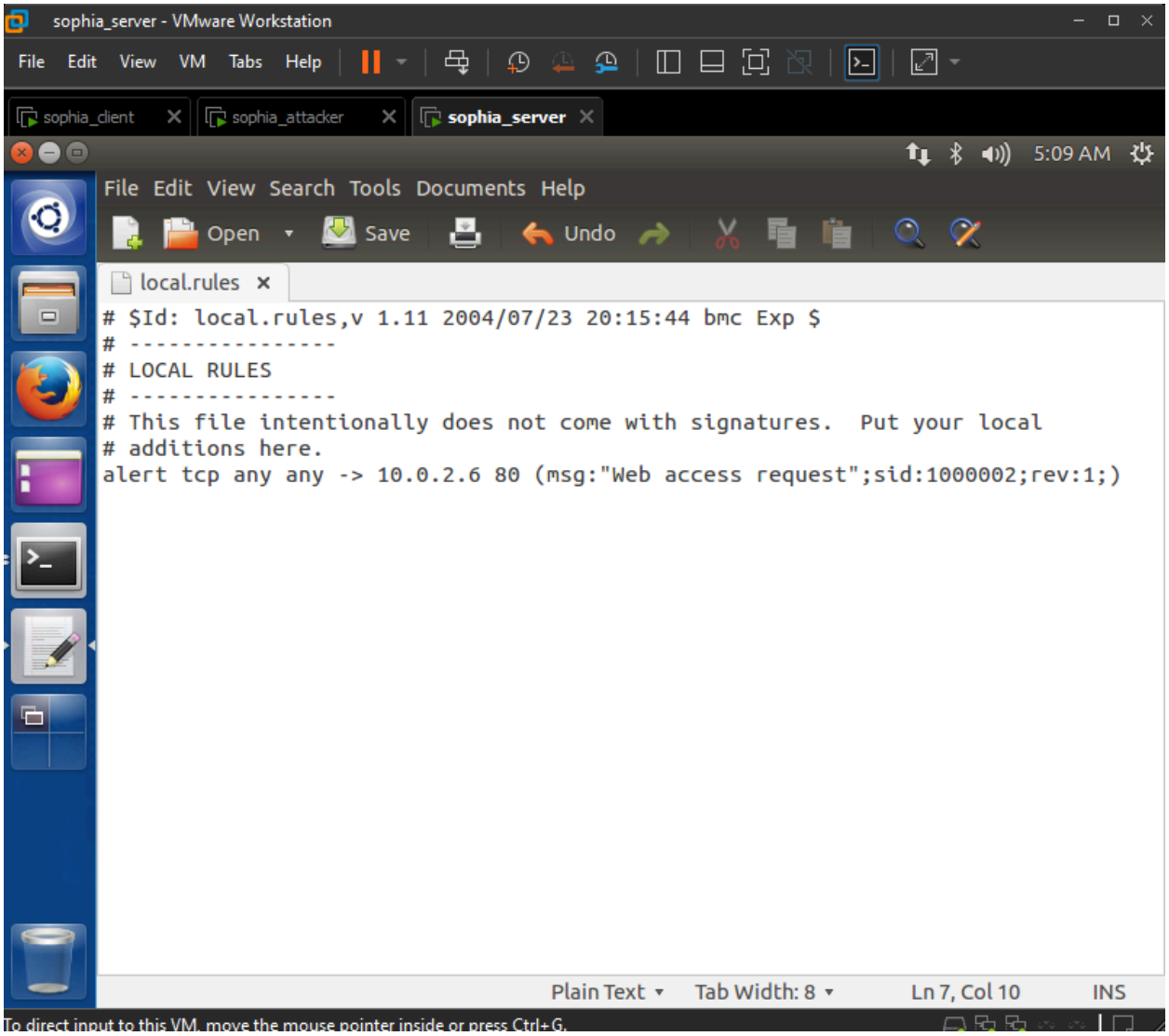
QUESTION 2. Have you received alert messages for ICMP Packets in IDS Mode? Please provide a screenshot to support your answer.



TASK 3: GENERATING ALERTS FOR WEB SERVICE

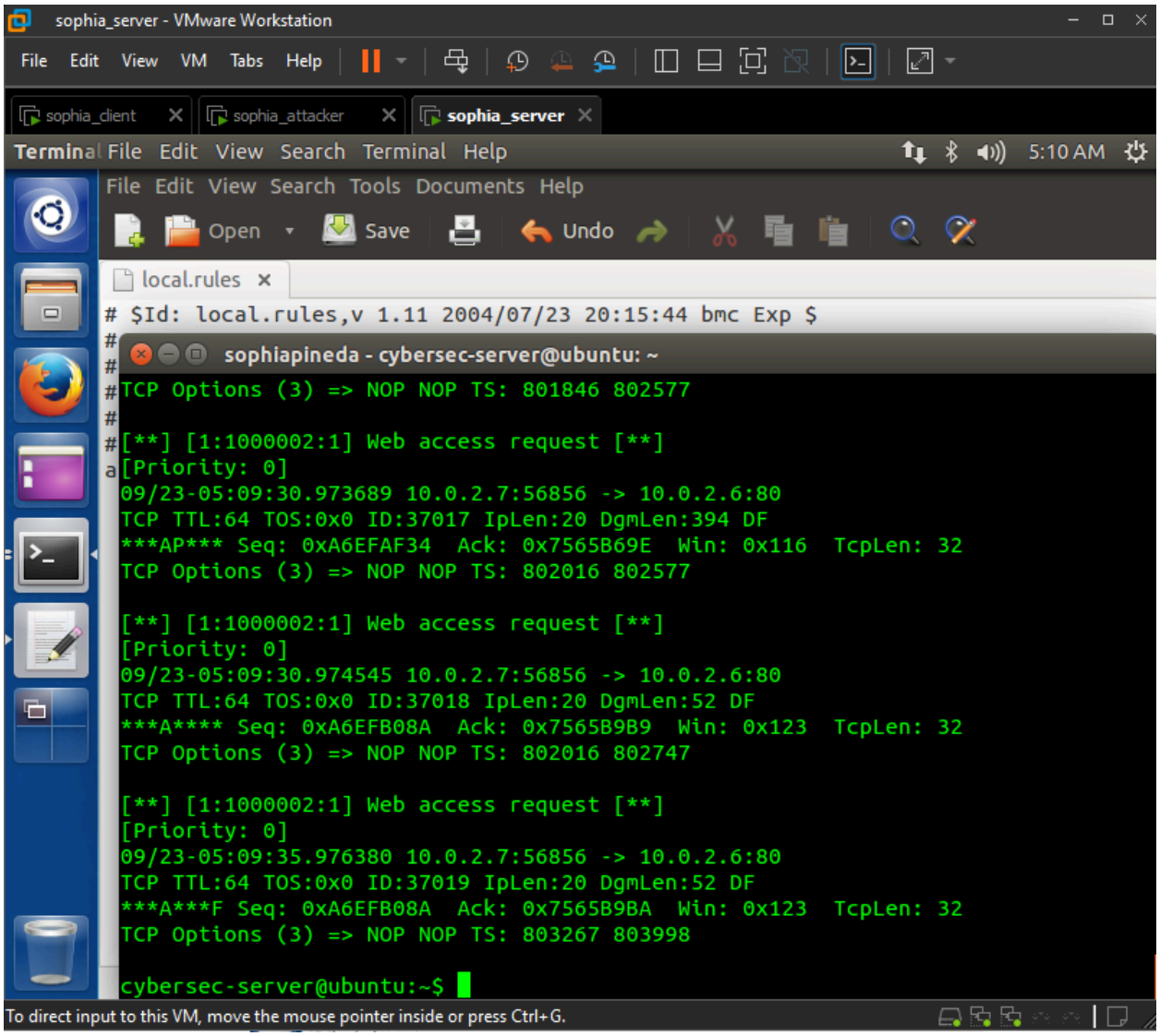
STEPS

1. Enter 10.0.2.6 in web browser of attackerVM
2. Enter sudo gedit /etc/snort/rules/local.rules



3. Enter sudo service snort restart
4. Refresh the webpage in Attacker VM
5. Enter cat /var/log/snort/alert

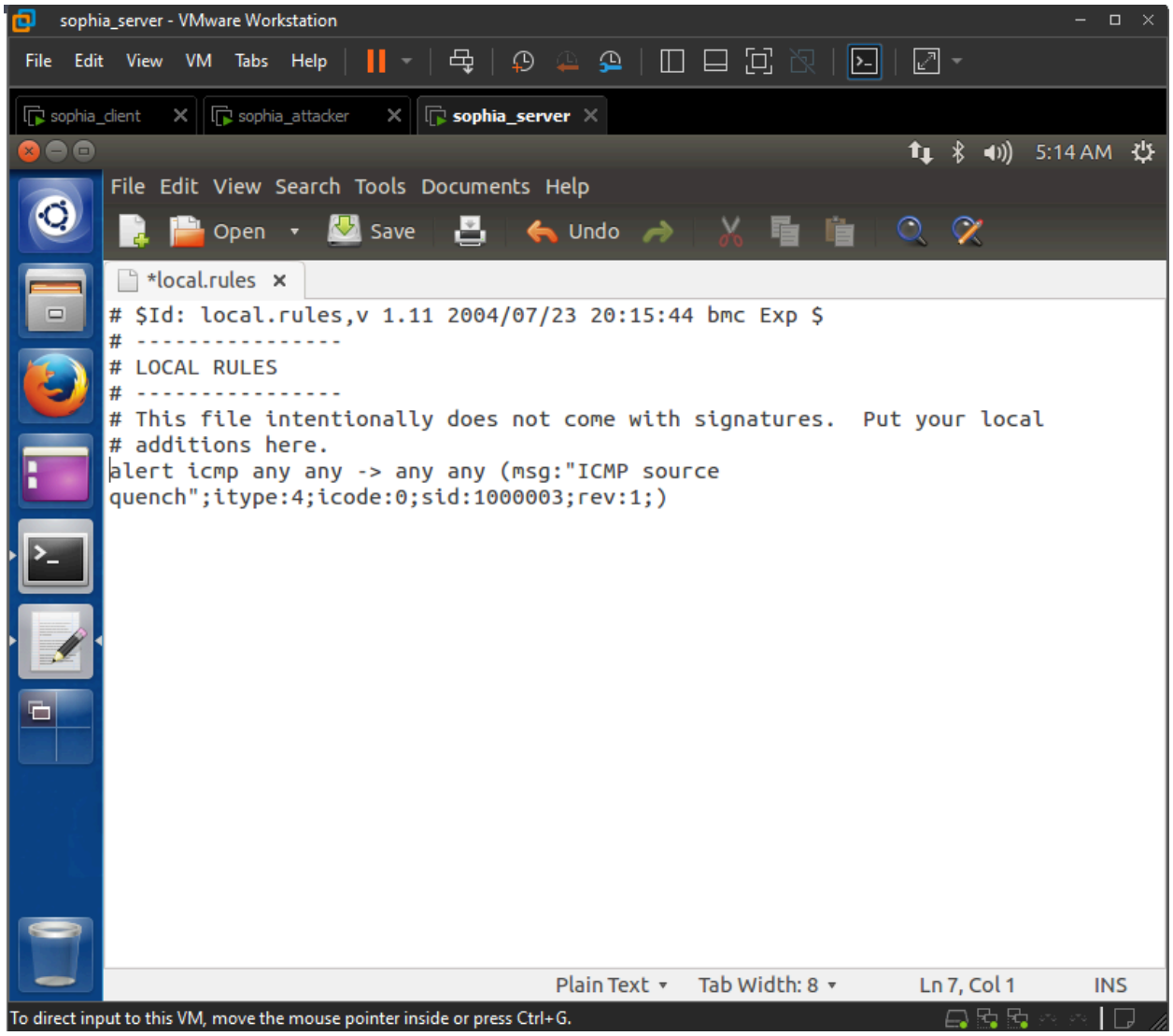
QUESTION 3. Have you received alert messages for Web access? Please provide a screenshot to support your answer.



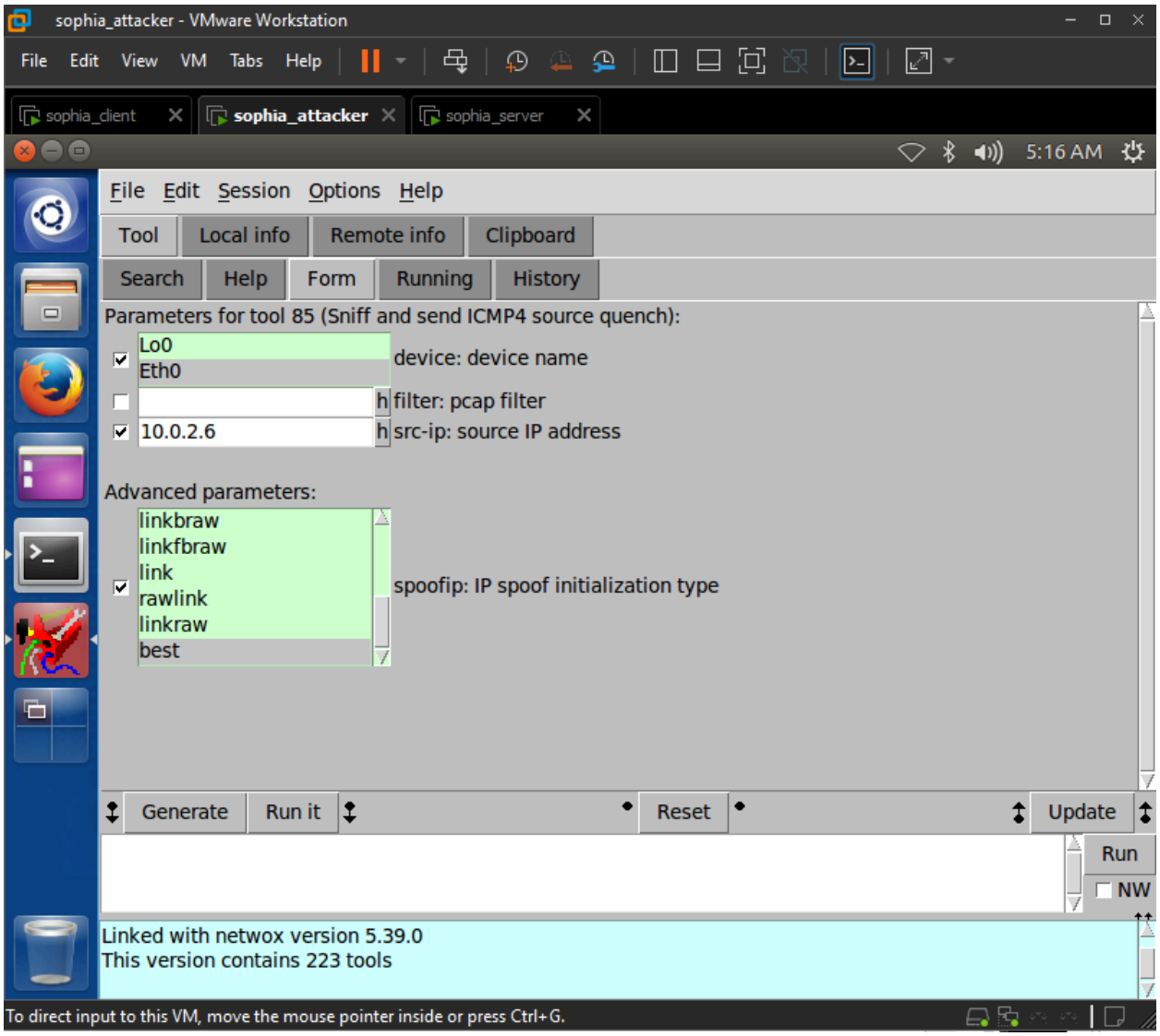
TASK 4: GENERATING ALERTS FOR ICMP SOURCE QUENCH PACKETS

STEPS

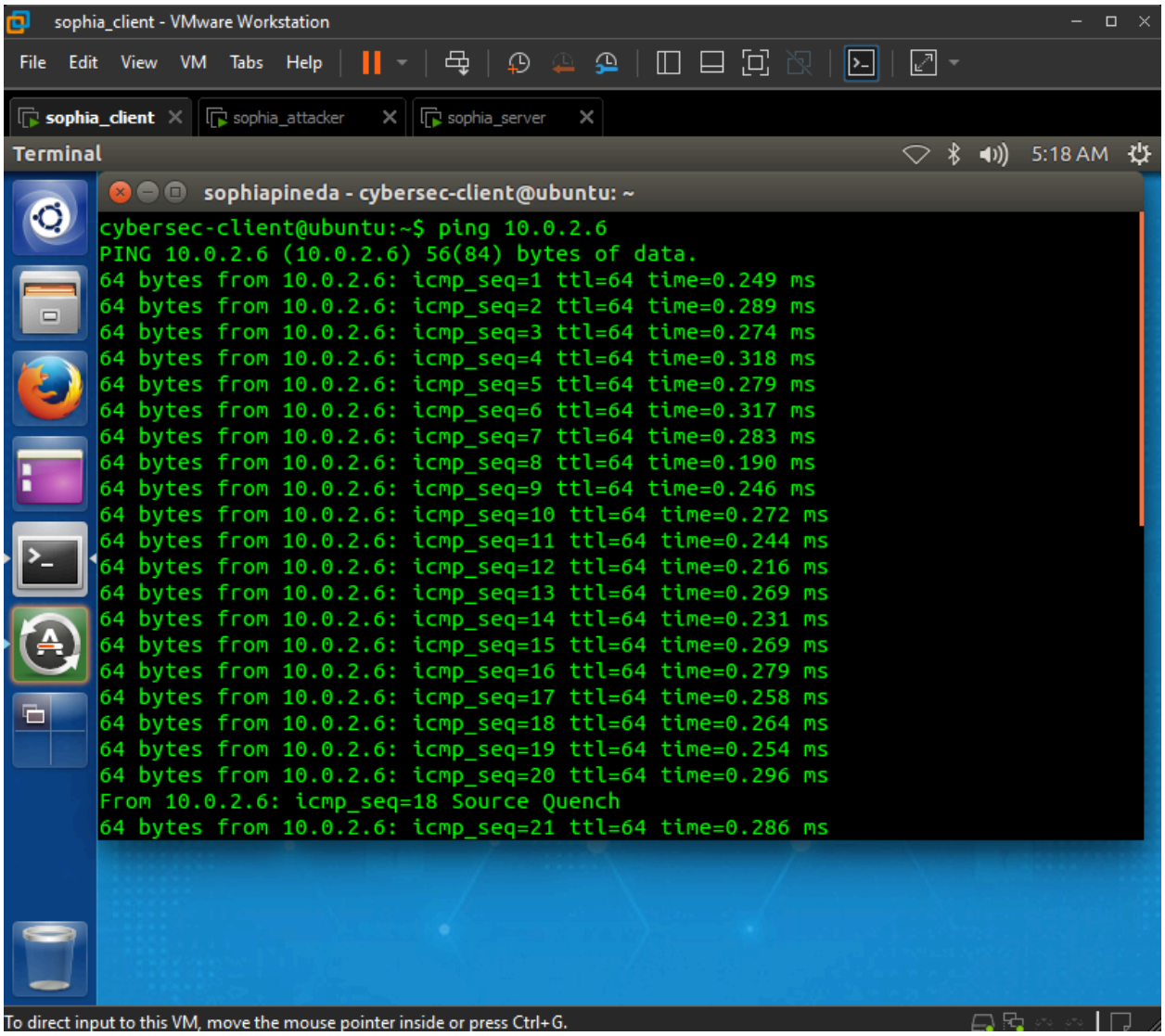
1. Enter sudo gedit /etc/snort/rules/local.rules in serverVM
2. Add “alert icmp any any -> any any (msg:"ICMP source uench"; itype:4; icode:0; sid:1000003; rev:1;)”



3. Enter sudo netwag in attackerVM, tool 85, 10.0.2.6

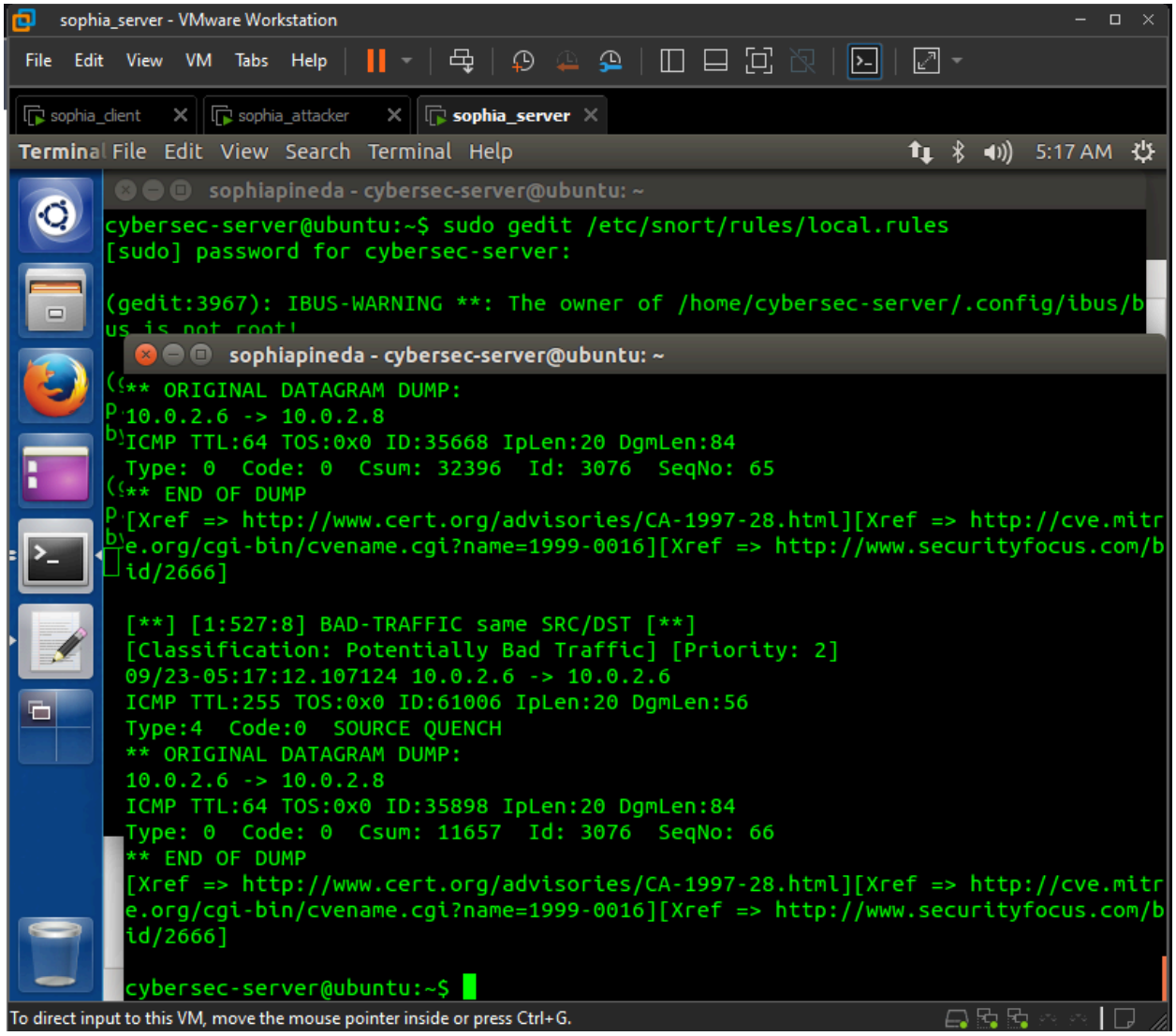


4. Ping 10.0.2.6 in clientVM



5. Enter cat /var/log/snort/alert in serverVM

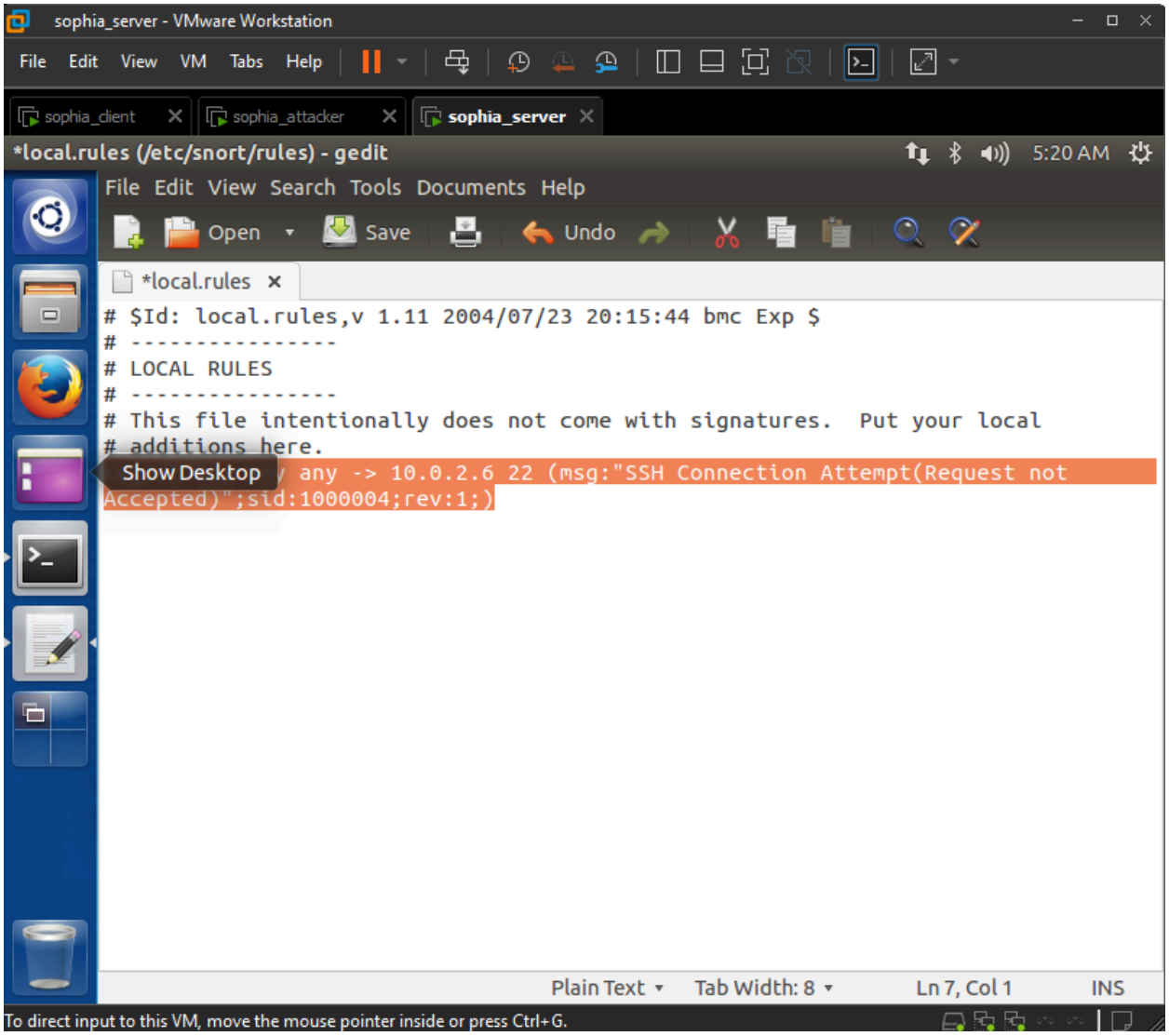
QUESTION 4. Have you received alert messages for Source Quench packets? Please provide a screenshot to support your answer.



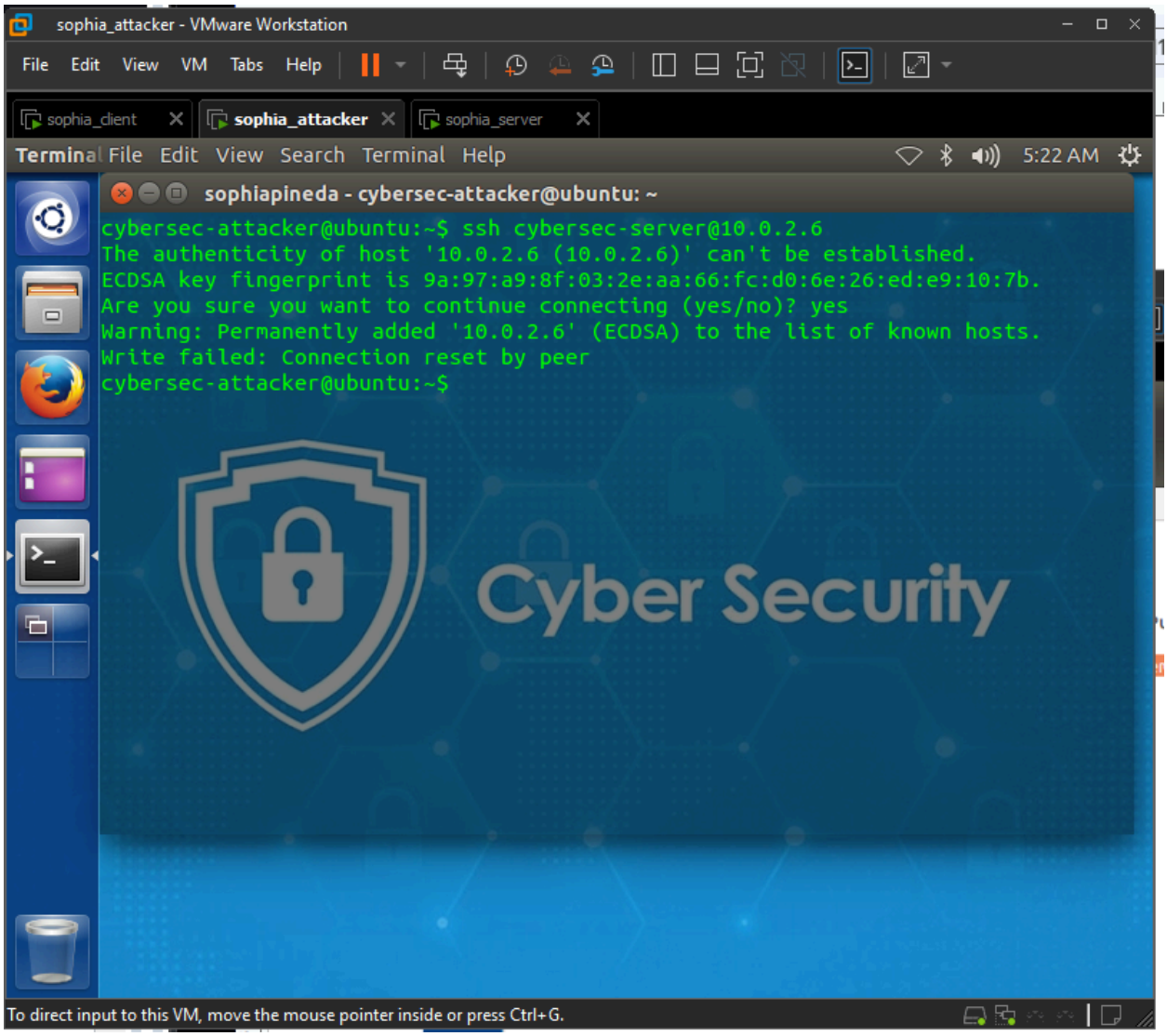
TASK 5: RUNNING SNORT AS INTRUSION PREVENTION SYSTEM

STEPS

1. Enter sudo gedit /etc/snort/rules/local.rules in serverVM
2. Add “reject tcp any any -> 10.0.2.6 22 (msg:”SSH Connection Attempt(Request not Accepted)”;sid:1000004;rev:1;)” in file

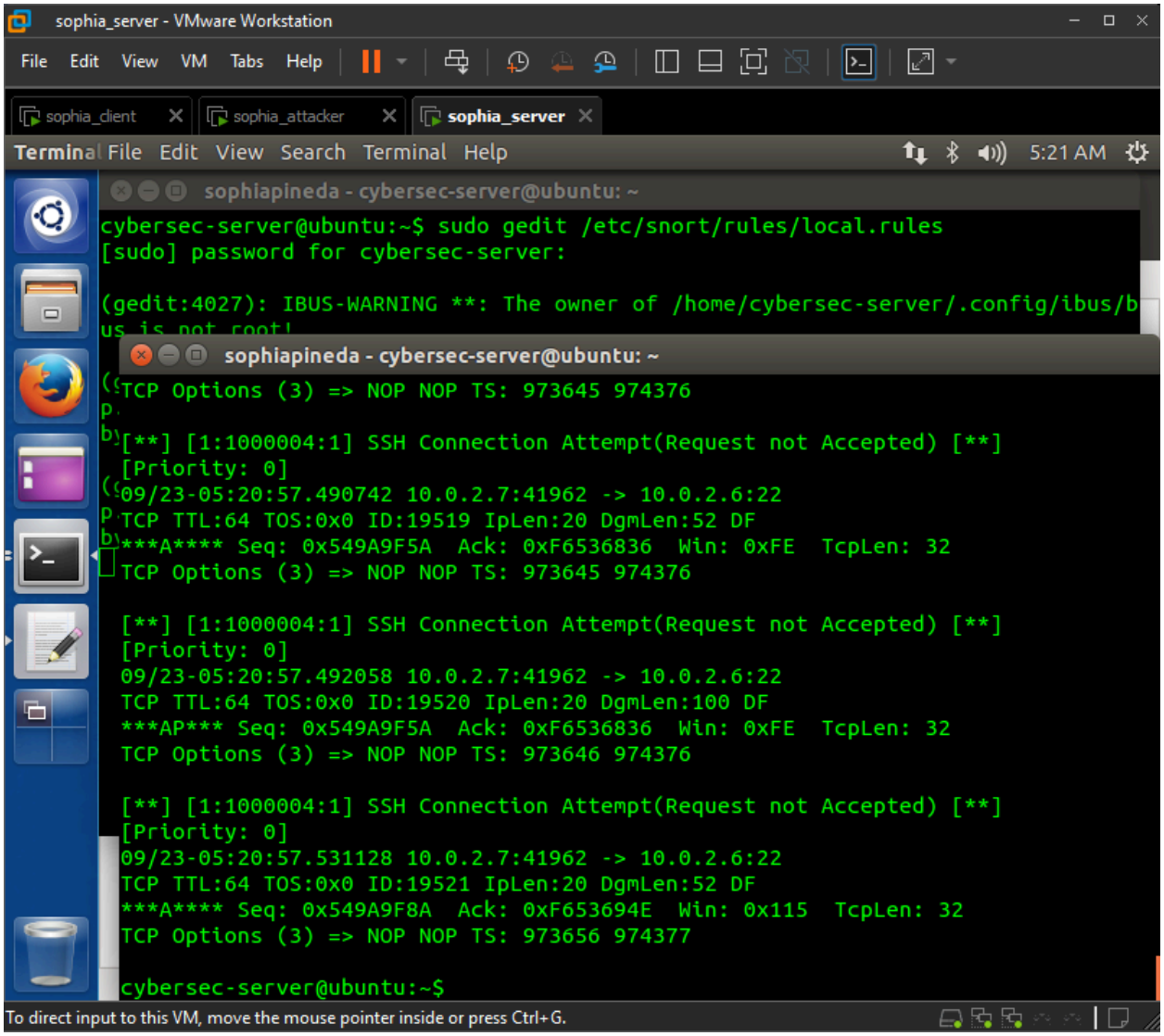


3. Enter sudo service snort restart
4. Enter ssh cybersec-server@10.0.2.6 in attackerVM



5. Enter cat /var/log/snort/alert in serverVM

QUESTION 5. Have you received alert messages for SSH connection Attempt? Did the connection attempt succeed? Please provide a screenshot to support your answer.

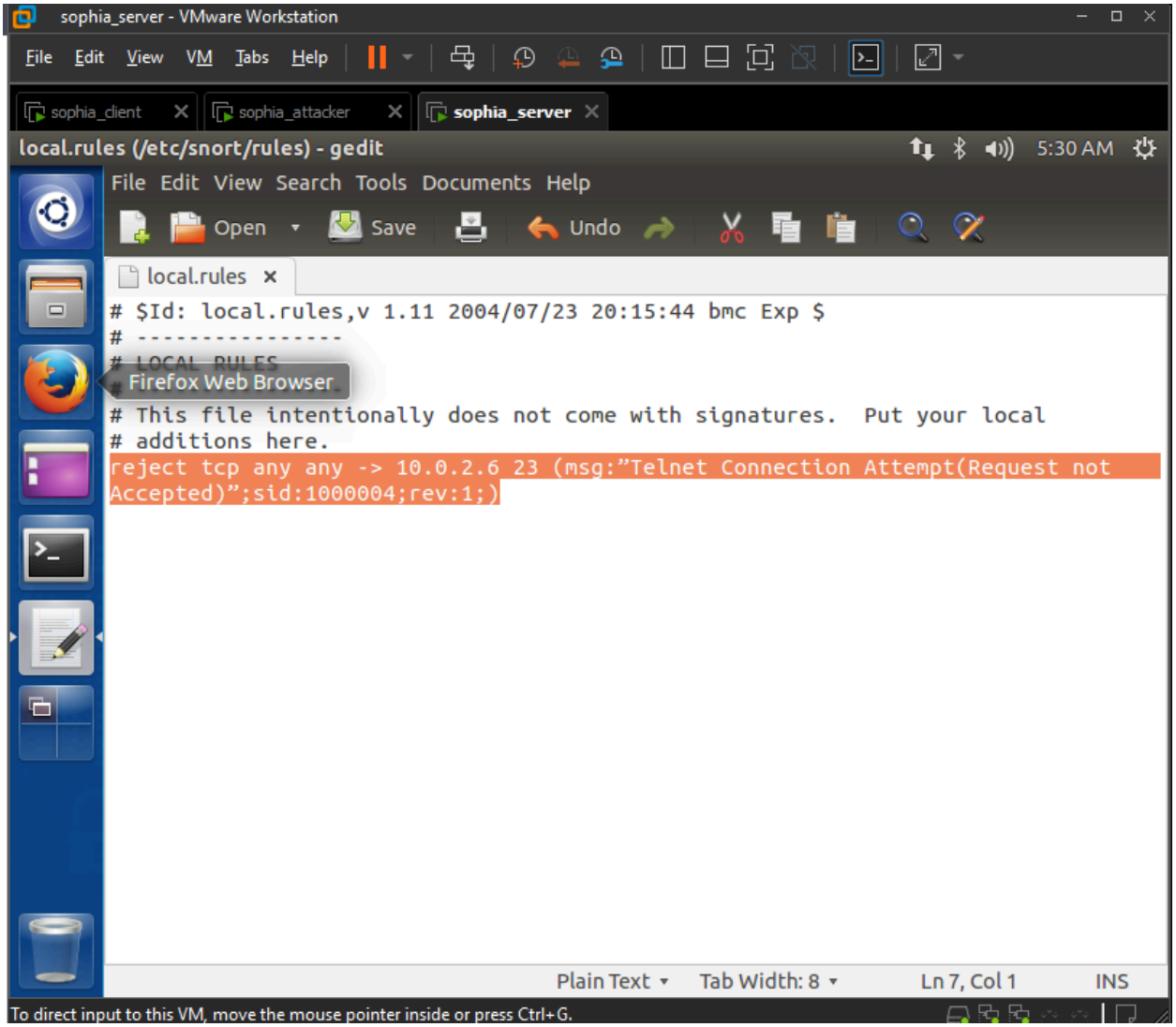


TASK 6: GENERATE ALERTS FOR TELNET CONNECTION ATTEMPTS FROM ATTACKER TO SERVER AND REJECT TELNET CONNECTION ATTEMPTS FROM ATTACKER

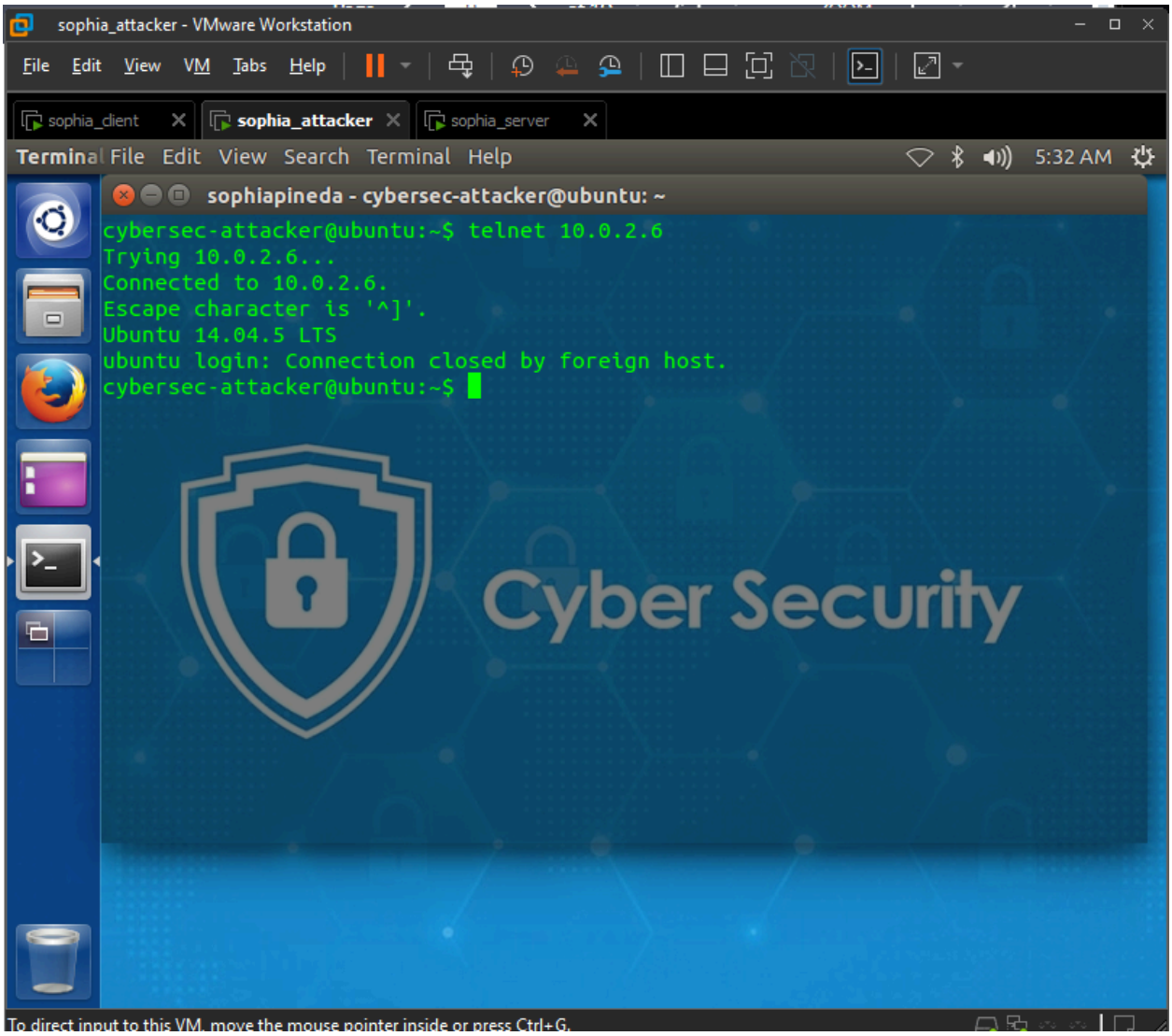
STEPS

1. Enter sudo gedit /etc/snort/rules/local.rules in serverVM

reject tcp any any -> 10.0.2.6 23 (msg:"Telnet Connection Attempt(Request not Accepted)";sid:1000004;rev:1;)

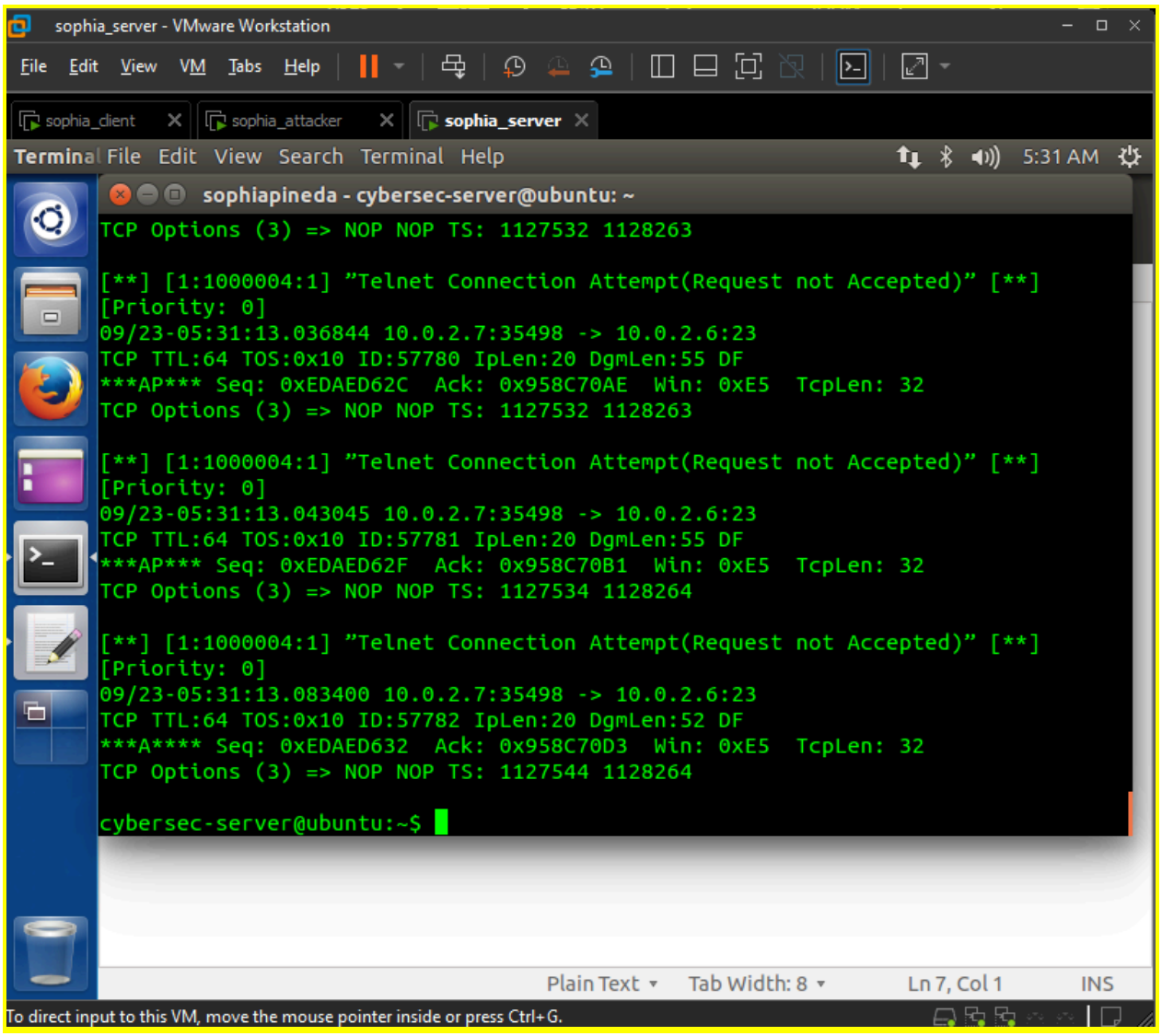


2. Enter sudo service snort restart
3. Enter telnet 10.0.2.6 from attackerVM



4. Enter cat /var/log/snort/alert in serverVM

QUESTION 6. Have you received alert messages for Telnet connection established from Attacker to Server? Did the telnet connection attempt from Attacker to Server succeed? Please provide a screenshot to support your answer. Also, mention the rule that was added to “local.rules” to create this alert.


sophia_server - VMware Workstation
File Edit View VM Tabs Help
sophia_client
sophia_attacker
sophia_server
Terminal File Edit View Search Terminal Help
5:31 AM
sophiapineda - cybersec-server@ubuntu: ~
TCP Options (3) => NOP NOP TS: 1127532 1128263
[**] [1:1000004:1] "Telnet Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/23-05:31:13.036844 10.0.2.7:35498 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:57780 IpLen:20 DgmLen:55 DF
AP Seq: 0xEDAED62C Ack: 0x958C70AE Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1127532 1128263
[**] [1:1000004:1] "Telnet Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/23-05:31:13.043045 10.0.2.7:35498 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:57781 IpLen:20 DgmLen:55 DF
AP Seq: 0xEDAED62F Ack: 0x958C70B1 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1127534 1128264
[**] [1:1000004:1] "Telnet Connection Attempt(Request not Accepted)" [**]
[Priority: 0]
09/23-05:31:13.083400 10.0.2.7:35498 -> 10.0.2.6:23
TCP TTL:64 TOS:0x10 ID:57782 IpLen:20 DgmLen:52 DF
A* Seq: 0xEDAED632 Ack: 0x958C70D3 Win: 0xE5 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1127544 1128264
cybersec-server@ubuntu:~$
Plain Text
Tab Width: 8
Ln 7, Col 1
INS
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.