UNDERSTANDING TCP/IP BASED ATTACKS (continuation from last week)

LAB ENVIRONMENT

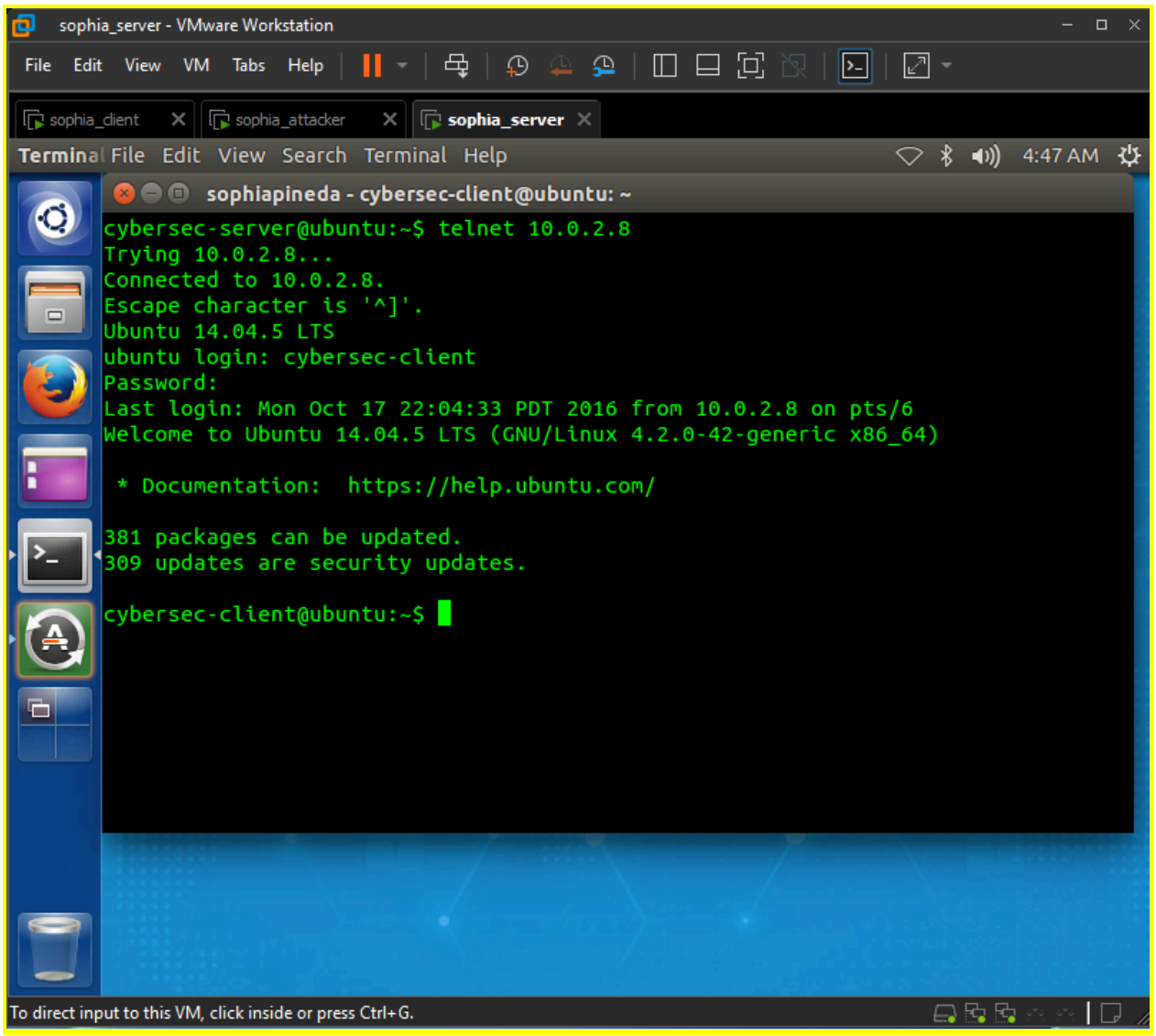
- All VMS
- Netwag
- Wireshark
- Assume attacks are in the same network as victims
- Disconnect internet from server VM

TASK 4: TCP RST ATTACKS ON TELNET AND SSH CONNECTIONS

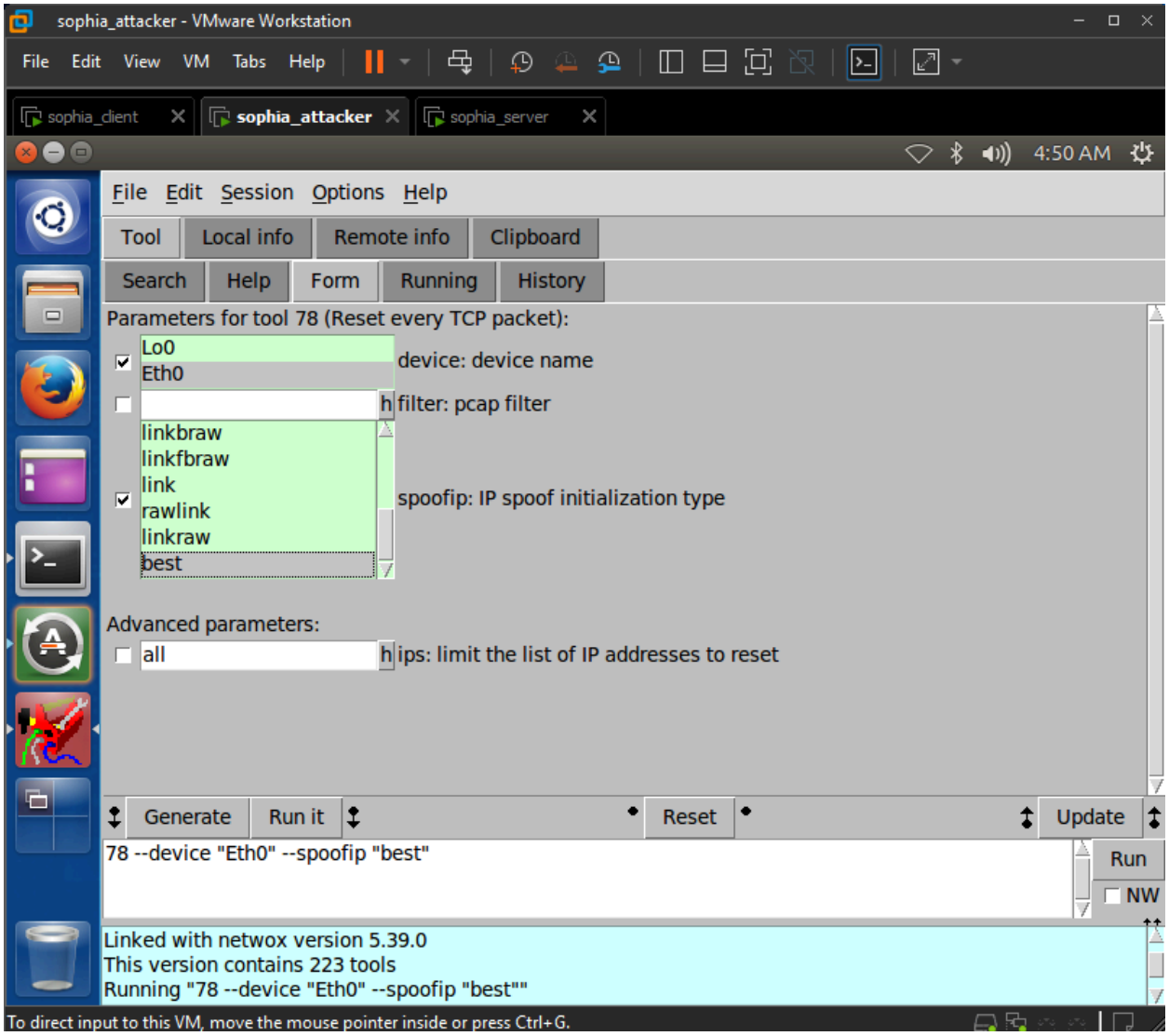
- Attack can terminate TCP connection between two victims
- Spoofs RST packet from A to B

STEPS (for telnet)

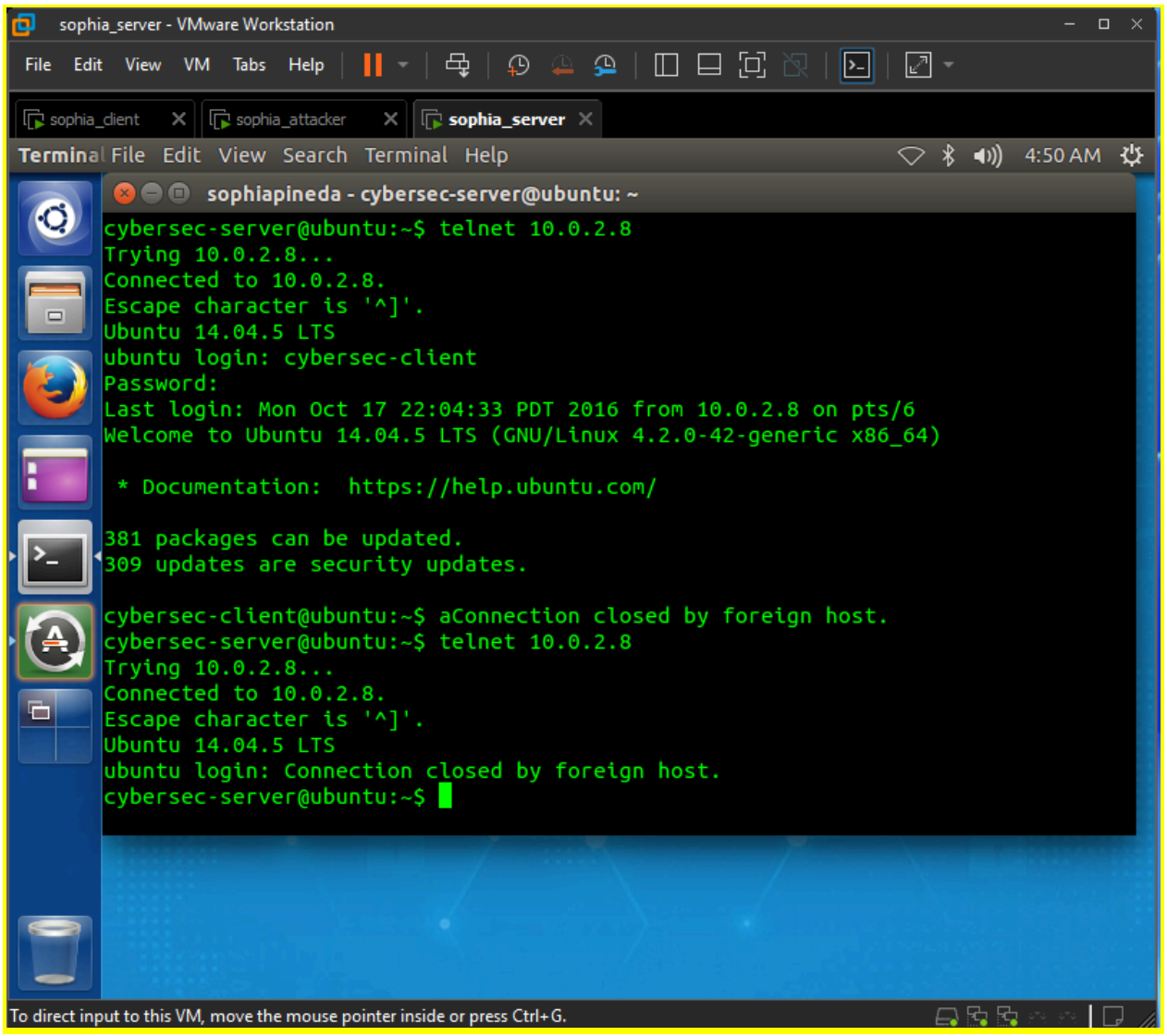
- Enter sudo wireshark in client VM
- Enter telnet <IP of client> in server VM - establishes telnet connection between client + server, fill in username and password of client (SCREENSHOT)



- Enter sudo netwag in attacker VM, select tool 78, select interface and spoofip: IP spoof initialisation type (SCREENSHOT), run

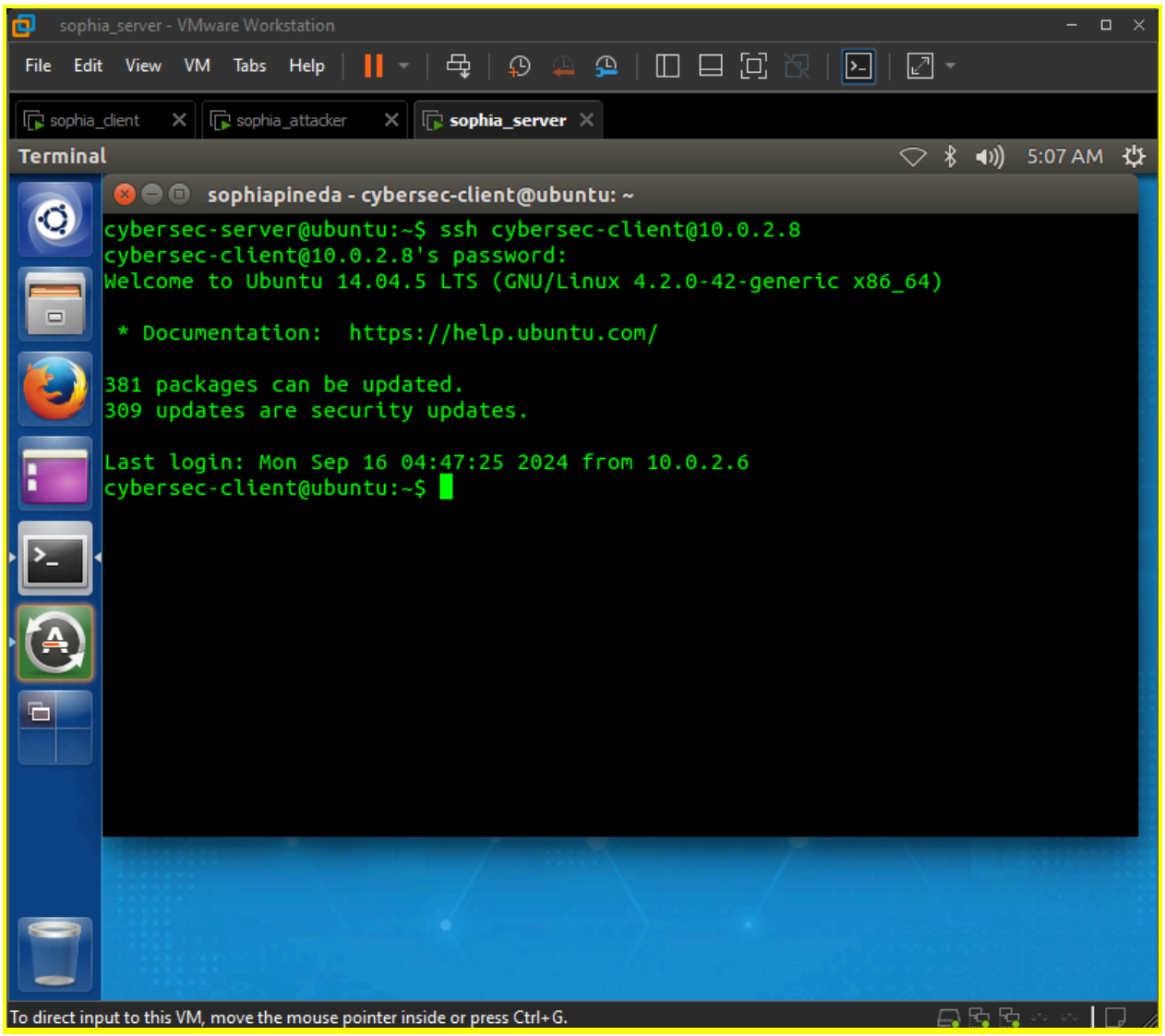


- Type in something in server VM terminal - generates data where a telnet connection with client is established (SCREENSHOT)

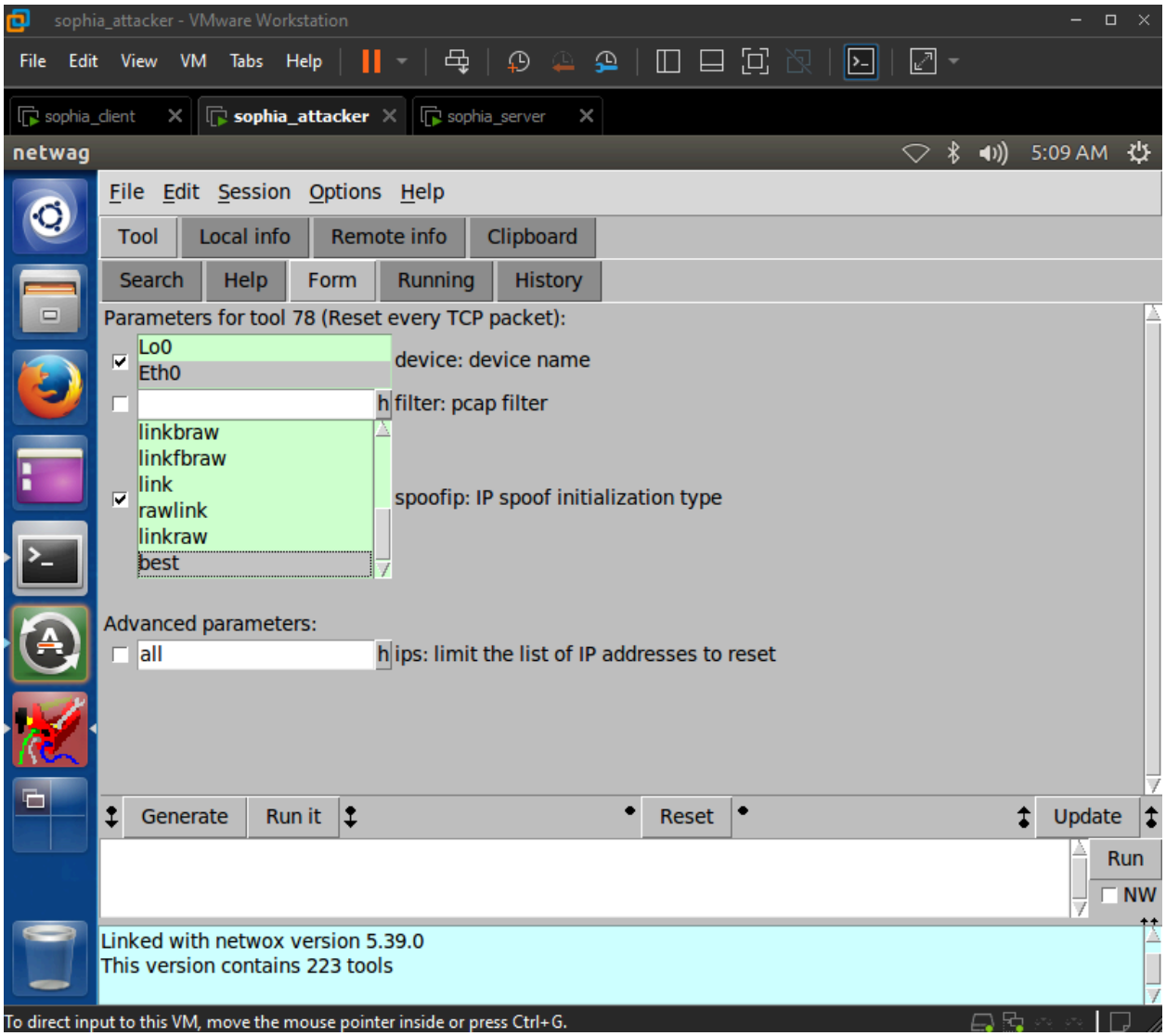


STEPS (for SSH)

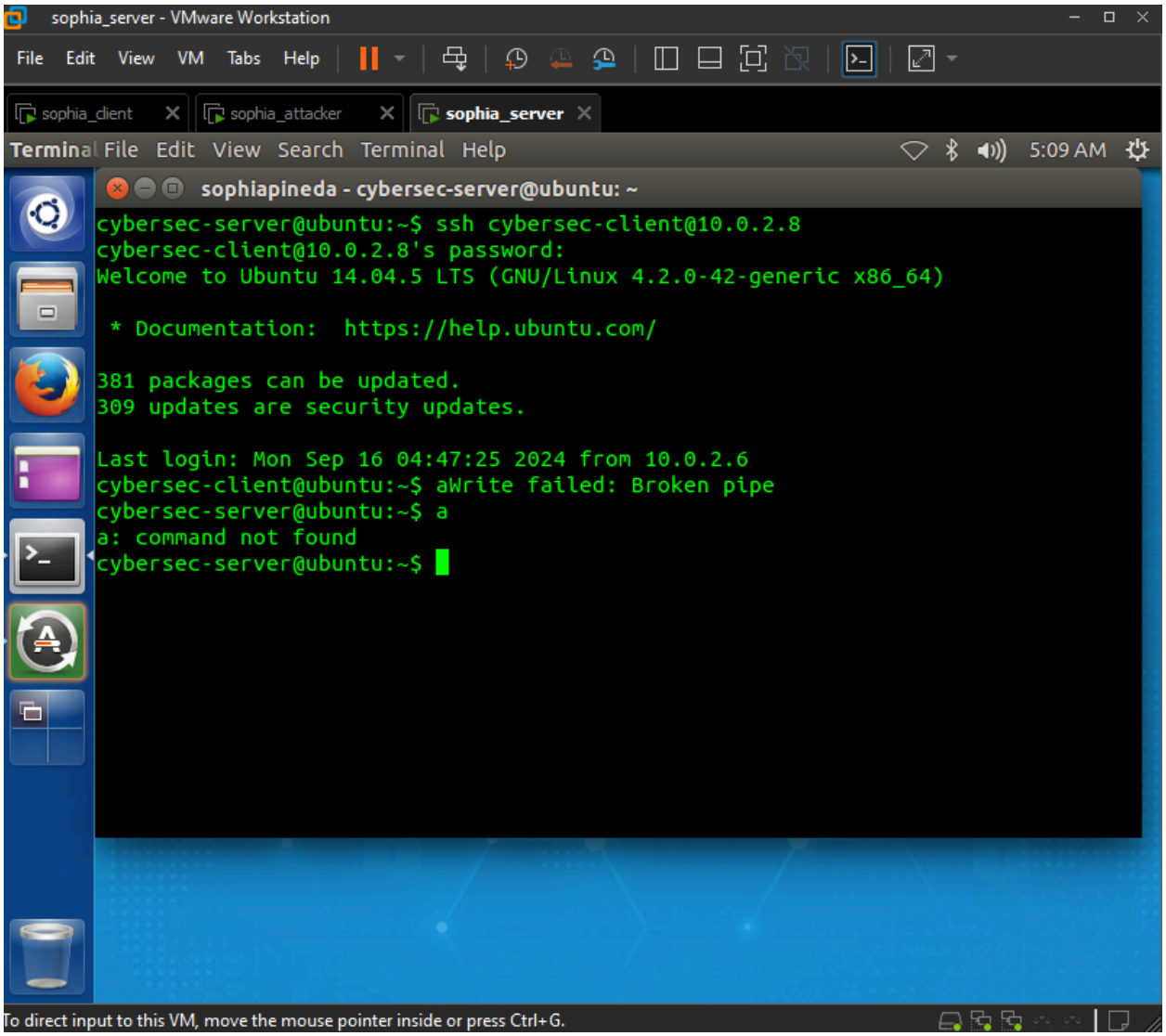
- Enter sudo wireshark in client VM
- Enter ssh username@IPaddressofclient in server VM - establishes SSH connection between client + server, fill in username and password of client (SCREENSHOT)



- Enter sudo netwag in attacker VM, select tool 78, select interface and spoofip: IP spoof initialisation type (SCREENSHOT), run



- Type in something in server VM terminal - generates data where a telnet connection with client is established (SCREENSHOT)



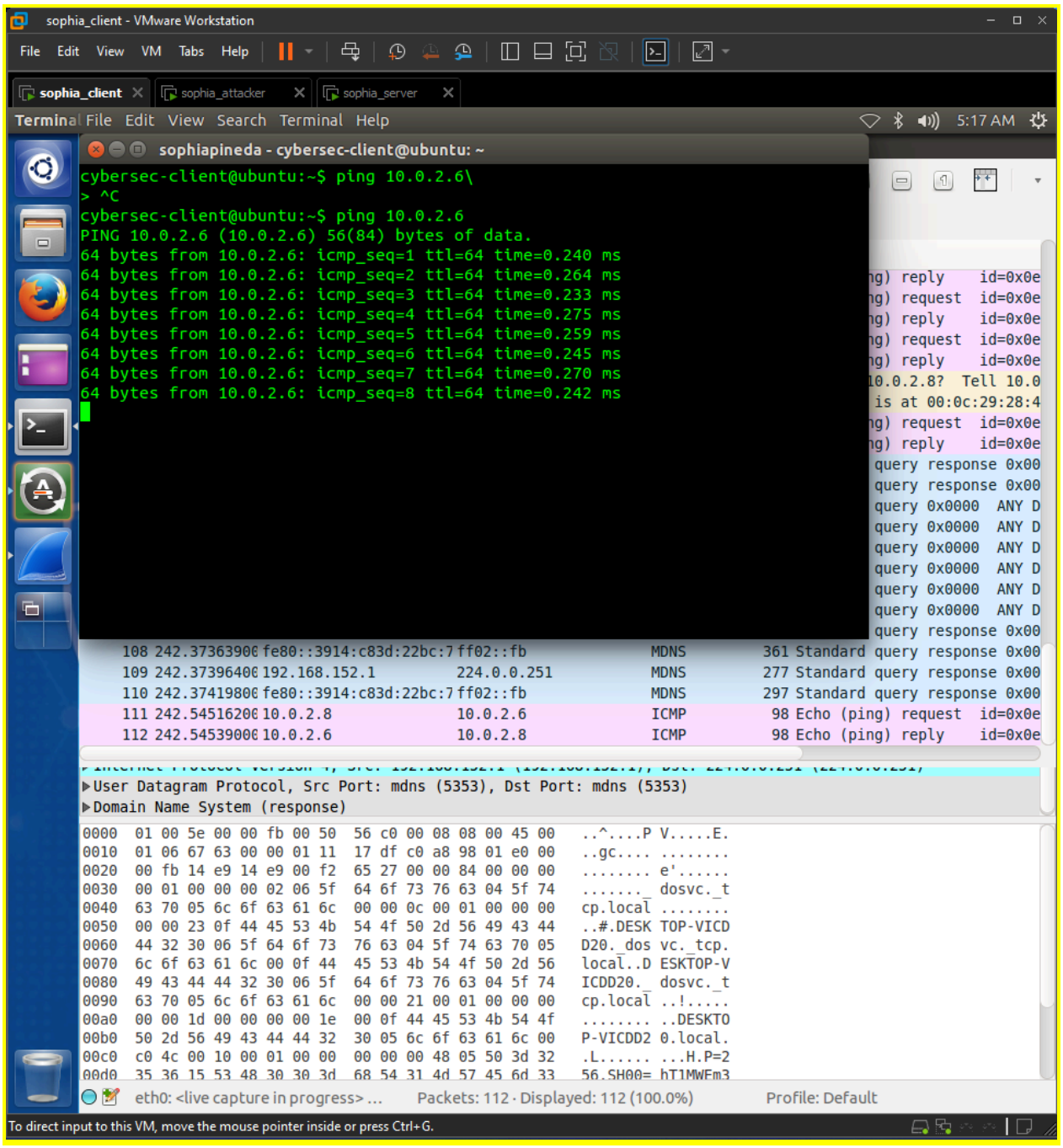
TASK 5 ICMP BLIND CONNECTION-RESET AND SOURCE-QUENCH ATTACKS

1. **ICMP BLIND CONNECTION-RESET**

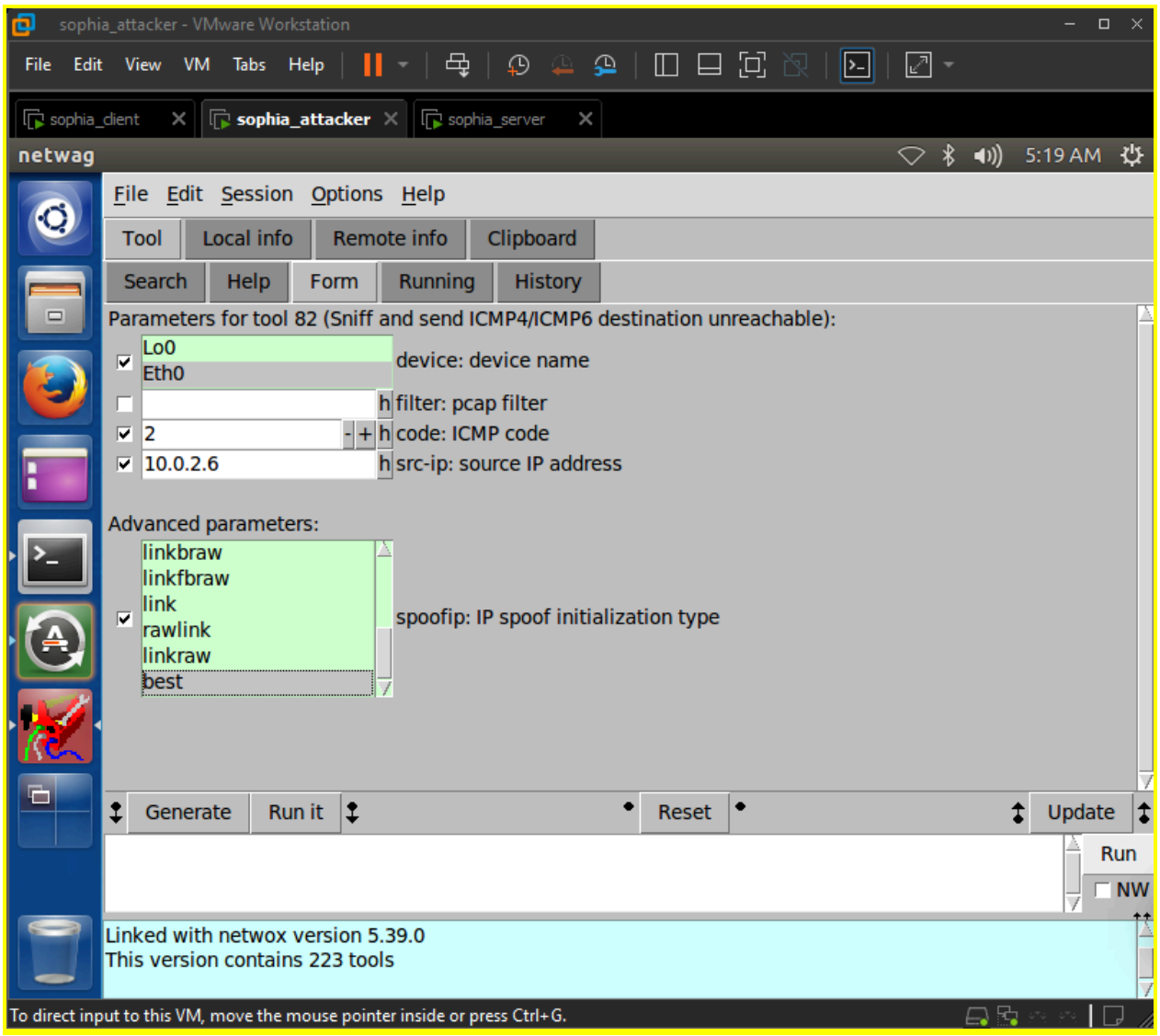
- Icmp messages can be used for the connection-resetting attack
  - Attackers send an ICMP error message that indicates hard error to one of the endpoints in the TCP connection
  - Connection is torn down as RFC 1122- stating that host should abort the connection when this error message is received
    - Type 3 (destination unreachable), code 2 (protocol unreachable), 3 (port unreachable), 4 (fragmentation needed and DF bit set)

STEPS

- Enter sudo wireshark in client VM, set ICMP as filter
- Enter ping <server IP> in client VM, capture packets in wireshark (SCREENSHOT)



- Enter sudo netwag in attacker VM, select tool 82, select interface and spoofip: IP spoof initialisation type, input the ICMP code and source IP address (SCREENSHOT)



- SCREENSHOT wireshark

sophia_client - VMware Workstation

File Edit View VM Tabs Help

sophia_client | sophia_attacker | sophia_server

Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)] 5:19 AM

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Search your computer and online sources

Filter: icmp Expression... Clear Apply Save

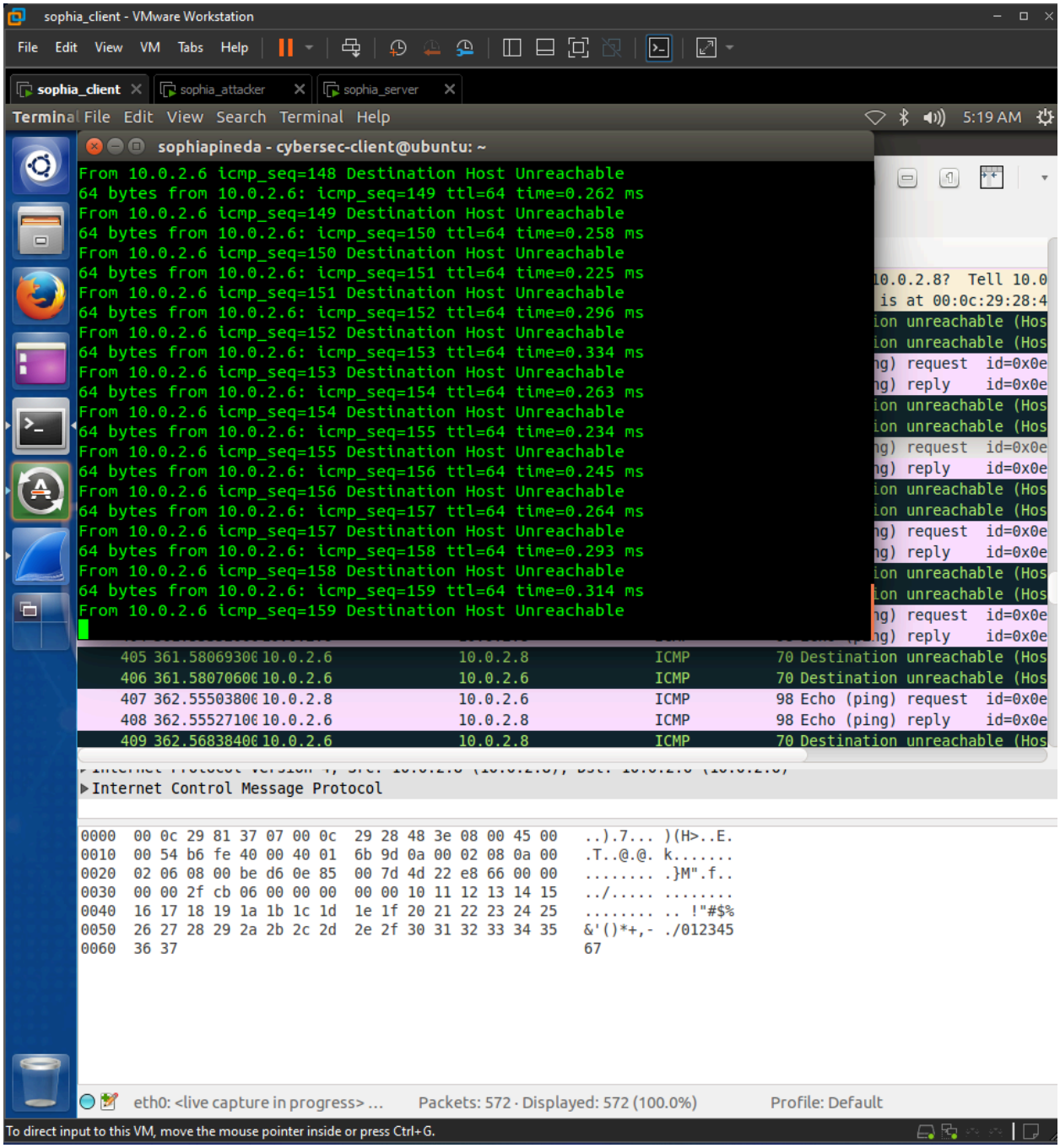
No.	Time	Source	Destination	Protocol	Length	Info
387	357.57857600	Vmware_27:a9:e1	Broadcast	ARP	60	Who has 10.0.2.8? Tell 10.0
388	357.57858900	Vmware_28:48:3e	Vmware_27:a9:e1	ARP	42	10.0.2.8 is at 00:0c:29:28:4
389	357.62884700	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Hos
390	357.62886600	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Hos
391	358.54735100	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0e
392	358.54756700	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0e
393	358.56441500	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Hos
394	358.56450000	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Hos
395	359.54870500	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0e
396	359.54899400	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0e
397	359.55244000	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Hos
398	359.55244700	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Hos
399	360.55116200	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0e
400	360.55142800	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0e
401	360.59265300	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Hos
402	360.59267000	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Hos
403	361.55327100	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0e
404	361.55352000	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0e
405	361.58069300	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Hos
406	361.58070600	10.0.2.6	10.0.2.6	ICMP	70	Destination unreachable (Hos
407	362.55503800	10.0.2.8	10.0.2.6	ICMP	98	Echo (ping) request id=0x0e
408	362.55527100	10.0.2.6	10.0.2.8	ICMP	98	Echo (ping) reply id=0x0e
409	362.56838400	10.0.2.6	10.0.2.8	ICMP	70	Destination unreachable (Hos

▶ Internet Control Message Protocol

```
0000  00 0c 29 81 37 07 00 0c  29 28 48 3e 08 00 45 00   ..).7... )(H>..E.
0010  00 54 b6 fe 40 00 40 01  6b 9d 0a 00 02 08 0a 00   .T..@.@. k.......
0020  02 06 08 00 be d6 0e 85  00 7d 4d 22 e8 66 00 00   ........ .}M".f..
0030  00 00 2f cb 06 00 00 00  00 00 10 11 12 13 14 15   ../..... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

eth0: <live capture in progress> ... Packets: 453 · Displayed: 453 (100.0%) Profile: Default

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

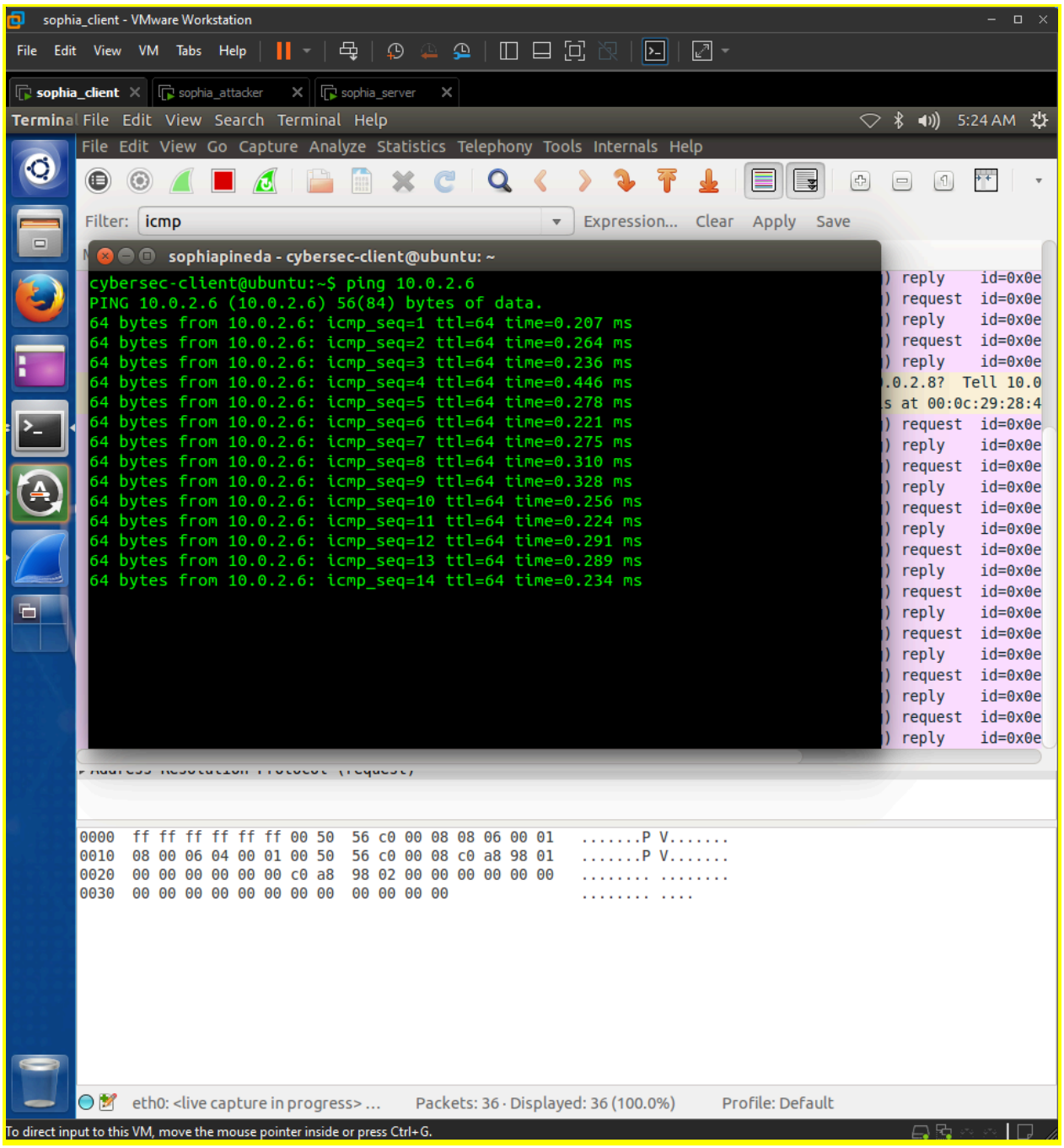


2. SOURCE-QUENCH ATTACKS

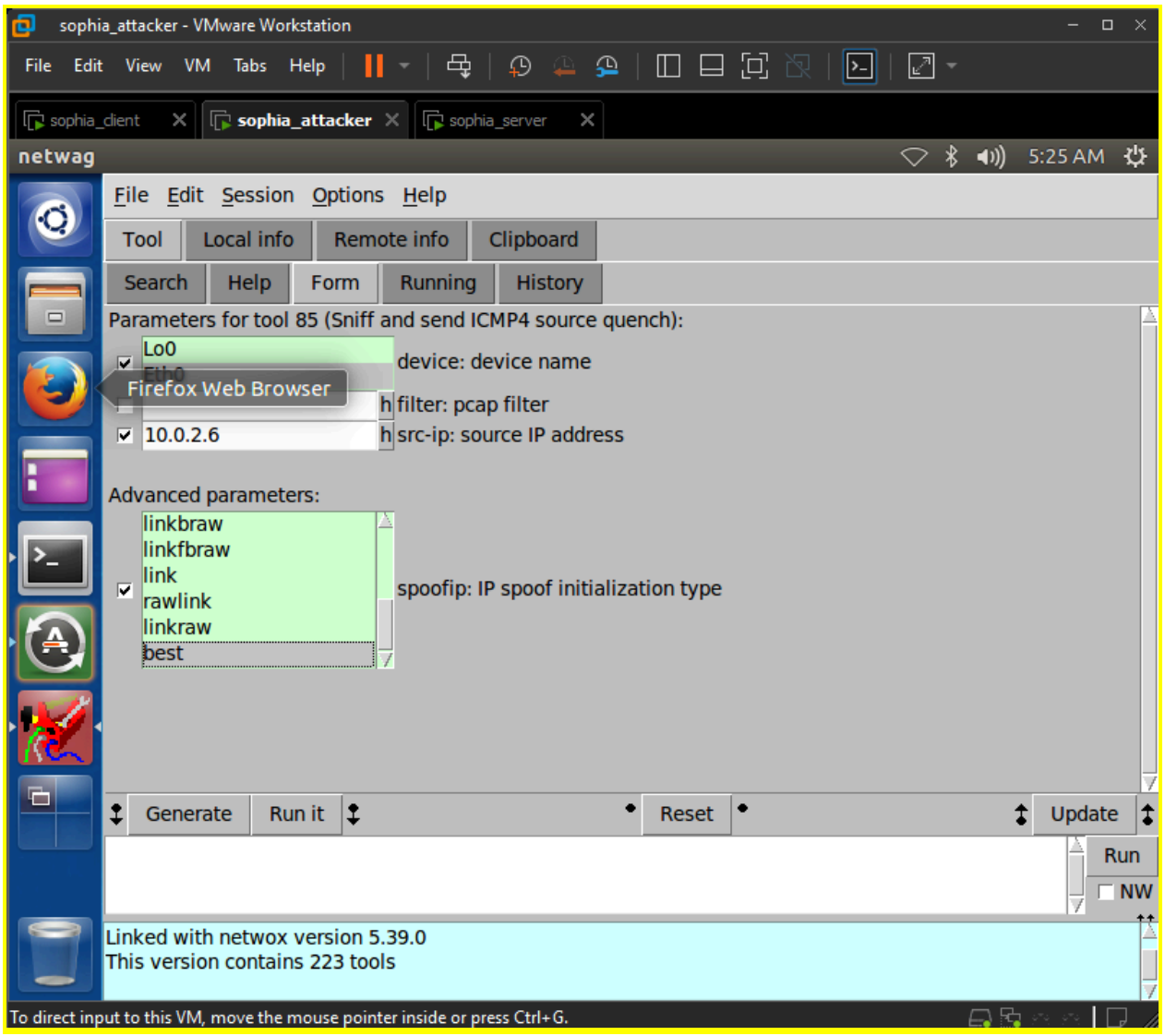
- Used by congested routers- telling TCP senders to slow down
    - Attackers can forge these messages to conduct denial of service attacks
- Launch ICMP blind connect-reset attacks and ICMP source quench attacks

STEPS

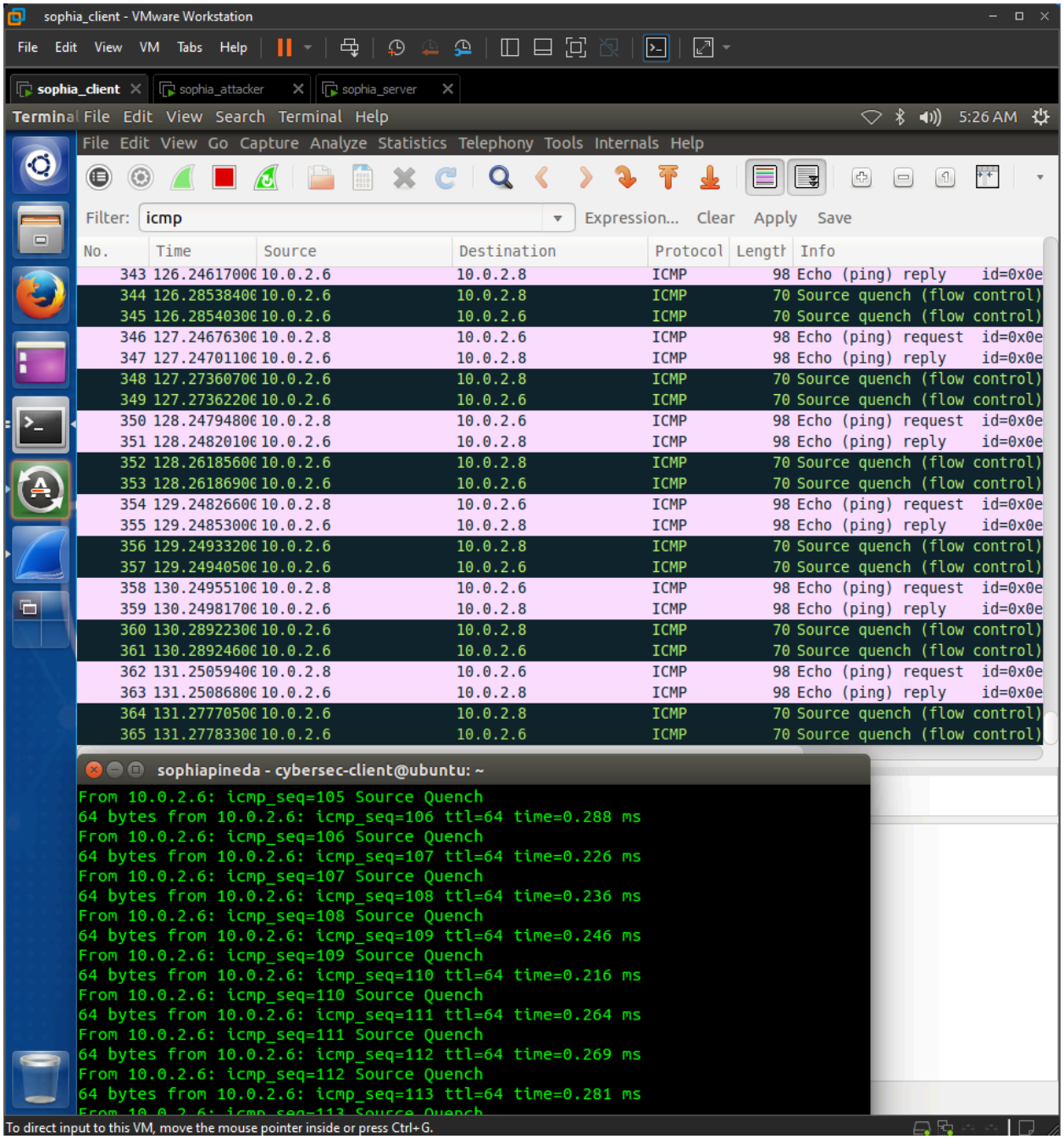
- Enter sudo wireshark in client VM, ICMP filter
- Enter ping <server IP> in client VM, capture packets in wireshark (SCREENSHOT)



- Enter sudo netwag in attacker VM, select tool 85, select interface and spoofip: IP spoof initialisation type, input the source IP address (SCREENSHOT)



- SCREENSHOT wireshark



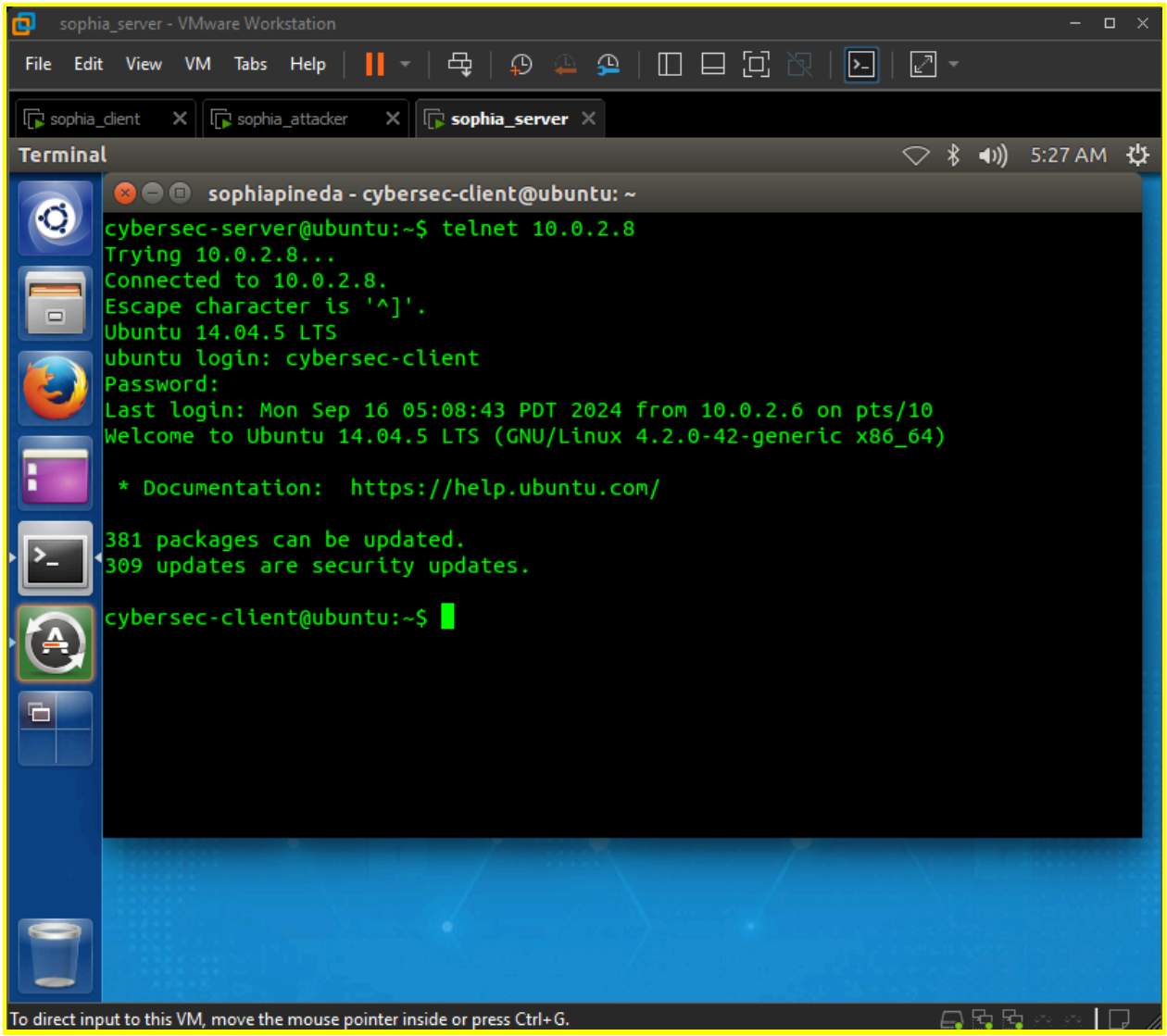
TASK 6: TCP SESSION HIJACKING

- Hijack a TCP connection by injecting malicious contents into the session
- If telnet connection, attackers can inject malicious commands into the session, causing victims to execute malicious commands

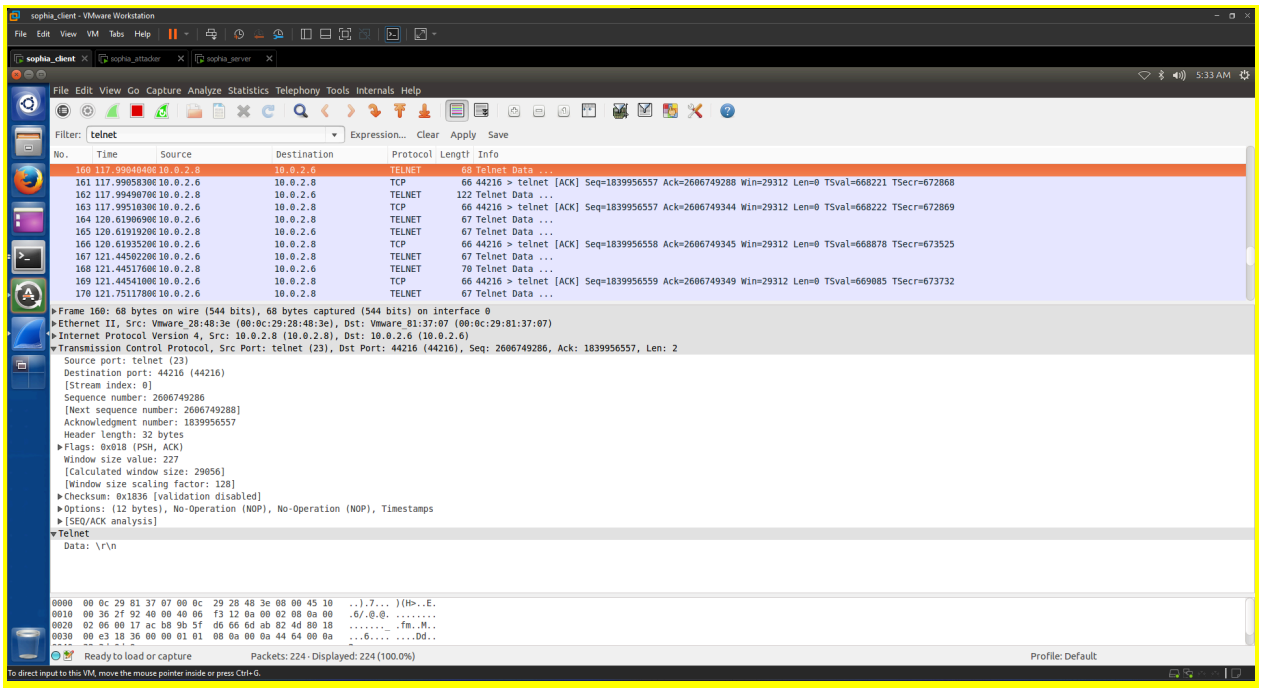
STEPS

- Enter sudo wireshark in client VM, filter telnet

- Enter telnet <IP address> in server VM, fill in username and password of client to establish telnet connection (SCREENSHOT)



- Type in something in the server VM terminal
- Ensure that relative sequence numbers is disabled (in protocol preferences)
- Expand on details of TCP and last telnet packet sent from server to client (SCREENSHOT)



- Convert mkdir hello + return key to hexadecimal: 6d 6b 64 69 72 20 68 65 6c 6c 6f
- Enter sudo netwag in attacker VM, select tool 36
- Provide info (SCREENSHOT)

sophia_attacker - VMware Workstation

File Edit View VM Tabs Help

sophia_client | sophia_attacker | sophia_server

File Edit Session Options Help

Tool | Local info | Remote info | Clipboard

Search | Help | Form | Running | History

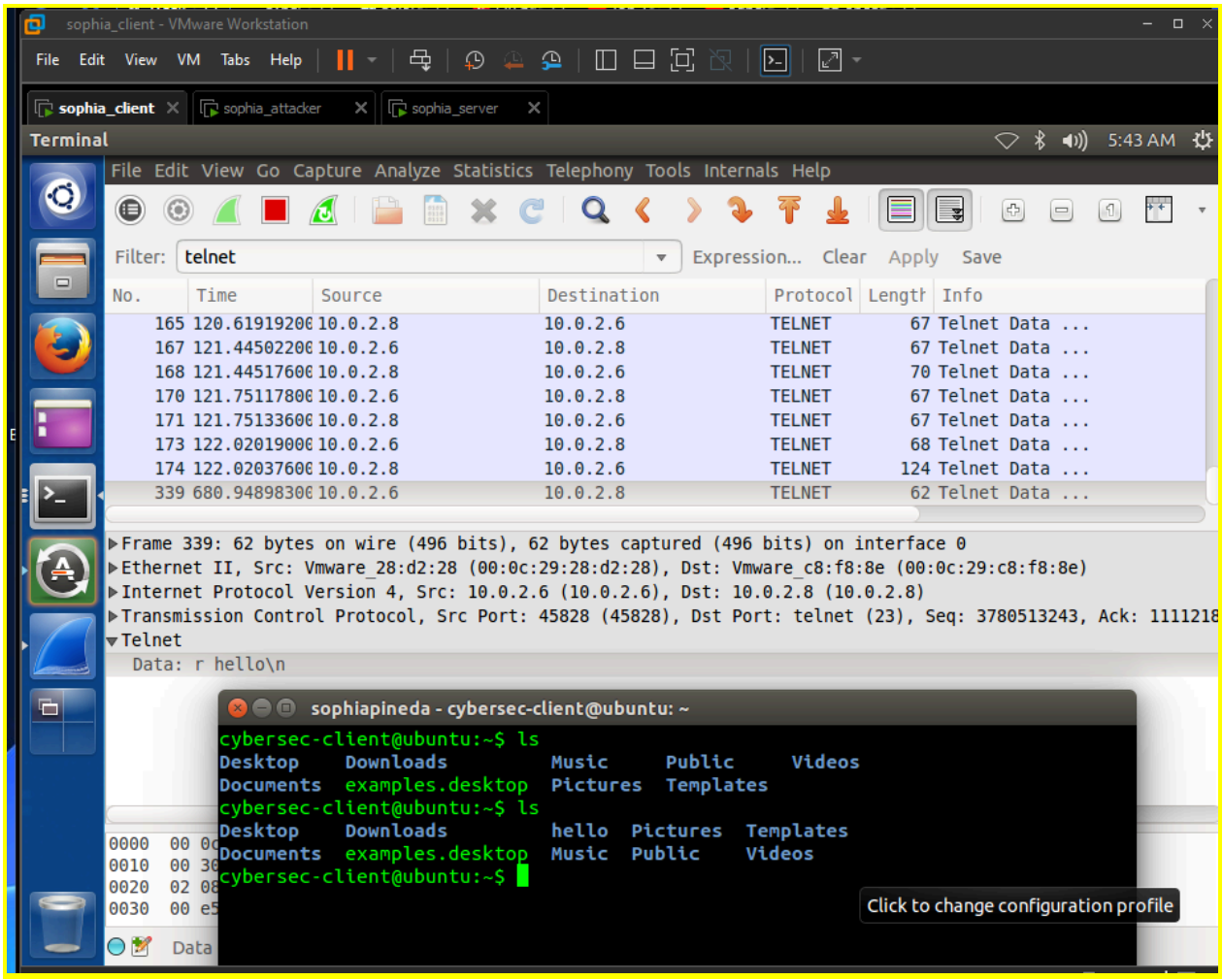
Parameters for tool 36 (Spoof EthernetIp4Tcp packet):

☑	Lo0 Eth0	device: device for spoof
☑	00:0c:29:28:d2:28 h	eth-src: Ethernet src
☑	00:0c:29:c8:f8:8e h	eth-dst: Ethernet dst
☐	0 - + h	ip4-tos: IP4 tos
☐	0 - + h	ip4-id: IP4 id (rand if unset)
☐	☐	ip4-reserved: IP4 reserved
☐	☐	ip4-dontfrag: IP4 dontfrag
☐	☐	ip4-morefrag: IP4 morefrag
☐	0 - + h	ip4-offsetfrag: IP4 offsetfrag
☑	64 - + h	ip4-ttl: IP4 ttl
☐	0 - + h	ip4-protocol: IP4 protocol
☑	10.0.2.6 h	ip4-src: IP4 src
☑	10.0.2.8 h	ip4-dst: IP4 dst
☐	h	ip4-opt: IPv4 options
☑	45828 - + h	tcp-src: TCP src
☑	23 - + h	tcp-dst: TCP dst
☑	3780513243 - + h	tcp-seqnum: TCP seqnum (rand if unset)
☑	1111218671 - + h	tcp-acknum: TCP acknum
☐	☐	tcp-reserved1: TCP reserved1
☐	☐	tcp-reserved2: TCP reserved2
☐	☐	tcp-reserved3: TCP reserved3
☐	☐	tcp-reserved4: TCP reserved4
☐	☐	tcp-cwr: TCP cwr
☐	☐	tcp-ece: TCP ece
☑	☑	tcp-urg: TCP urg
☑	☑	tcp-ack: TCP ack
☑	☑	tcp-psh: TCP psh
☐	☐	tcp-rst: TCP rst

Generate | Run it

Linked with netwox version 5.39.0
This version contains 223 tools

- On wireshark, look for last telnet packet sent from server to client before TCP retransmission
- Expand on details of telnet for that packet (SCREENSHOT)



- Check home directory of client