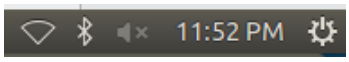
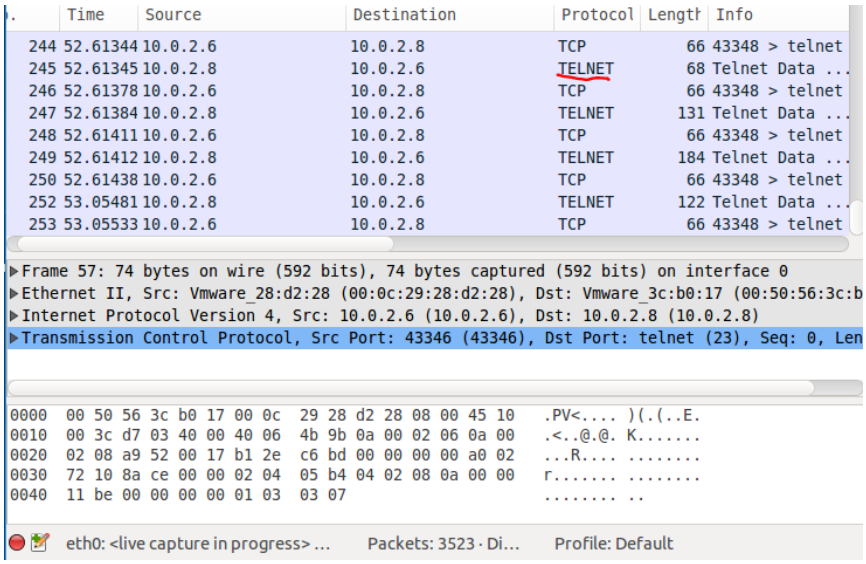
Task 4: TCP RST Attacks on telnet Connections

Turn off the connection first in the CyberSec-Server.

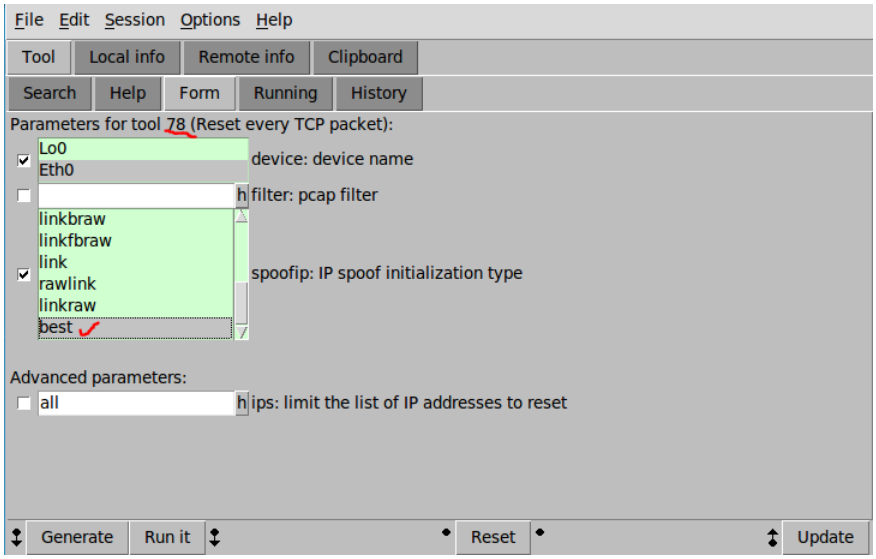


Set up Telnet connection on Cybersec-Client, open terminal then type ‘telnet’ followed by 10.0.2.8 and fill the information as seen on the screenshot. Password always use ‘cybersec’.

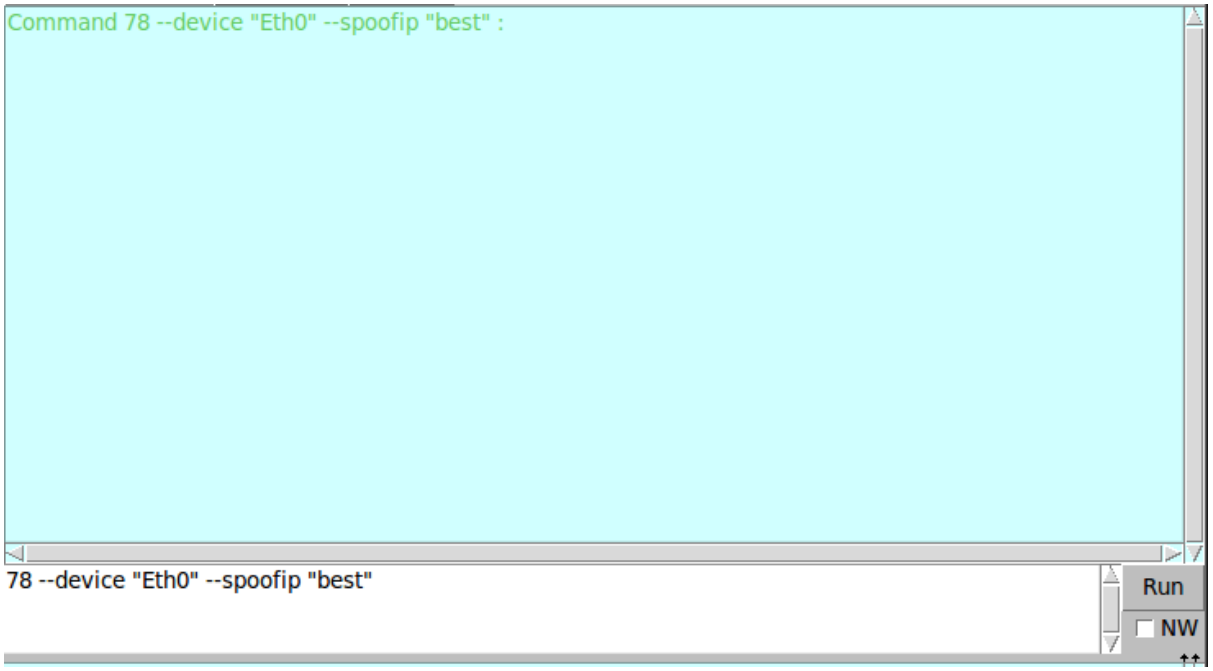
Open CyberSec-Client then wireshark, then check if telnet connection is successful



Open CyberSec-Attacker, search for tool 78 and fill in with the same information below & press run it

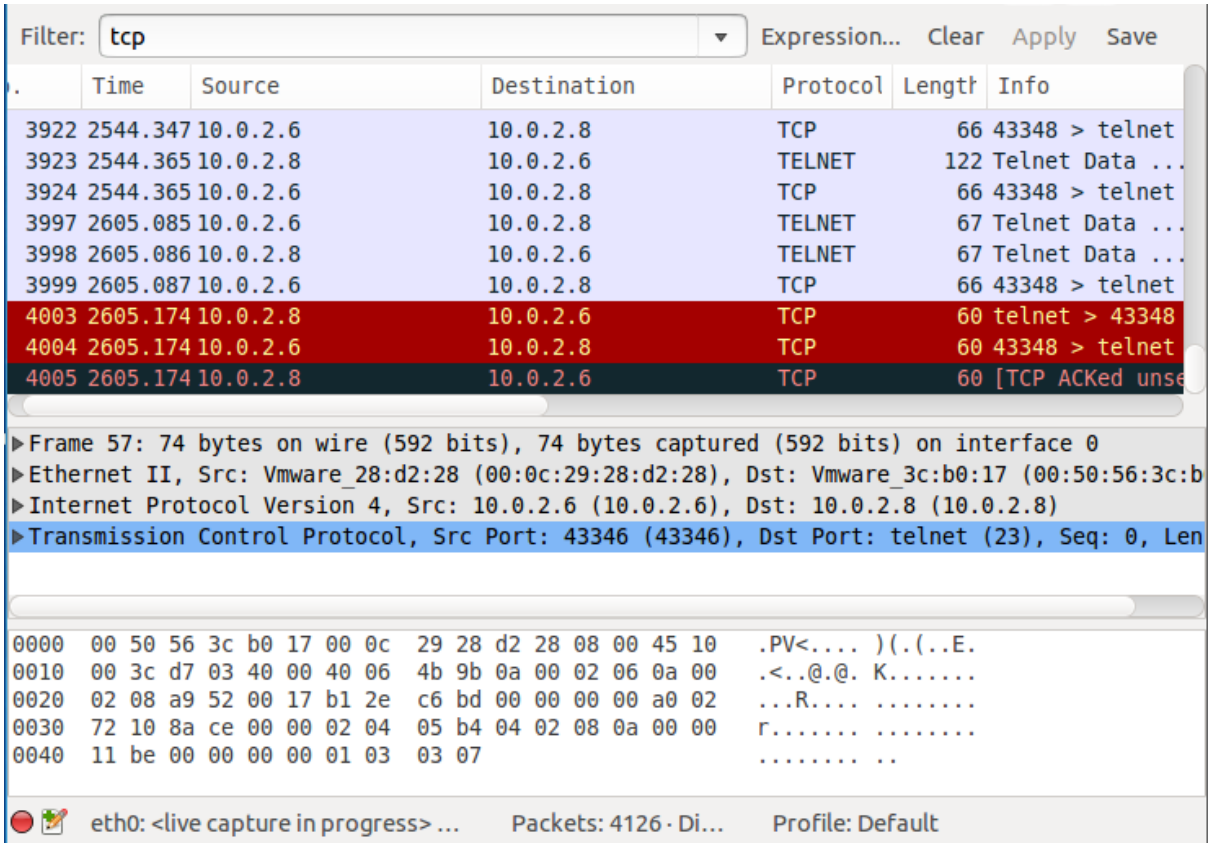


Result after pressing ‘run it’:

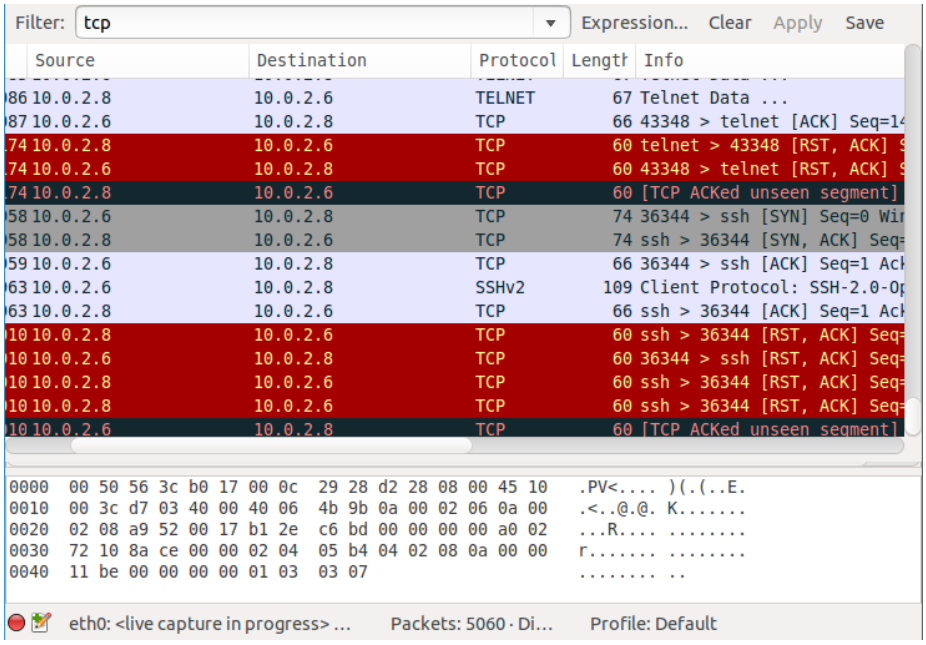


In CyberSec-Server, type anything in the command line. It’ll have ”sConnection closed by foreign host.” as the result

Open wireshark on CyberSec-Client, as can be seen that two reset packets have been send from client and server machine.

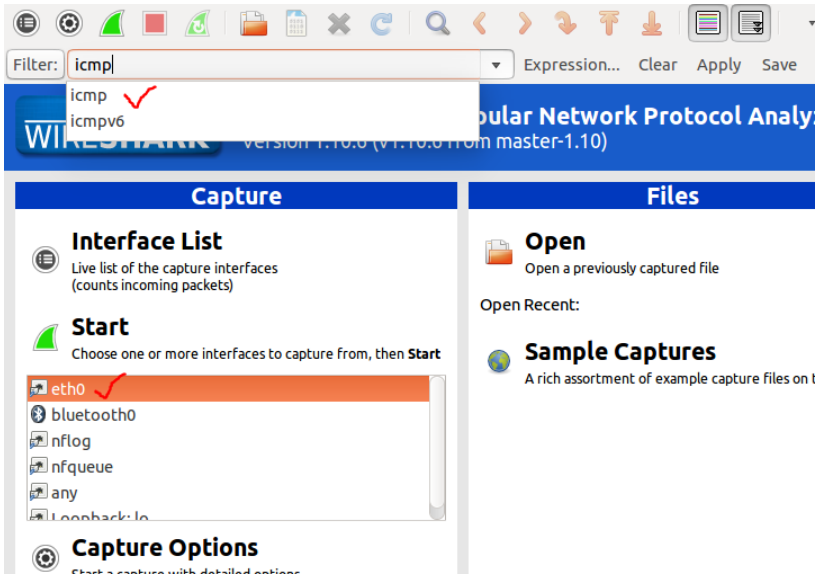


On CyberSec-Server, type ‘ssh cybersec-client@10.0.2.8’. As can be seen that SSH connection is closed because netwag is still opened.

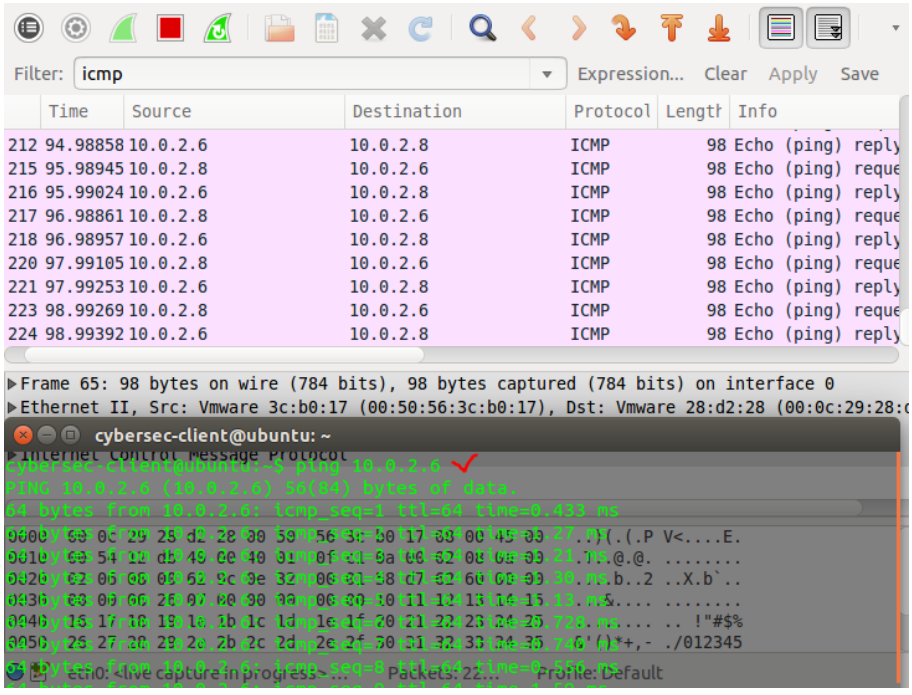


Task 5: ICMP Blind Connection-Reset

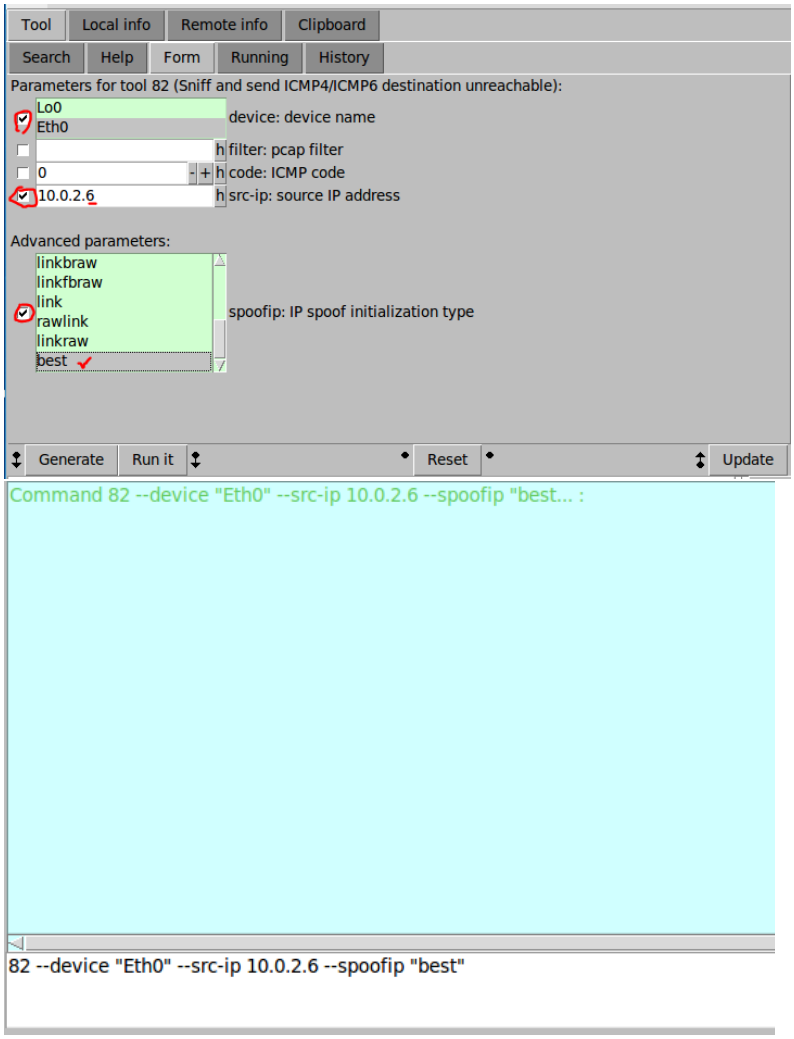
On the CyberSec-Client, open wireshark then choose ‘eth0’ and icmp on the filter, then press start.



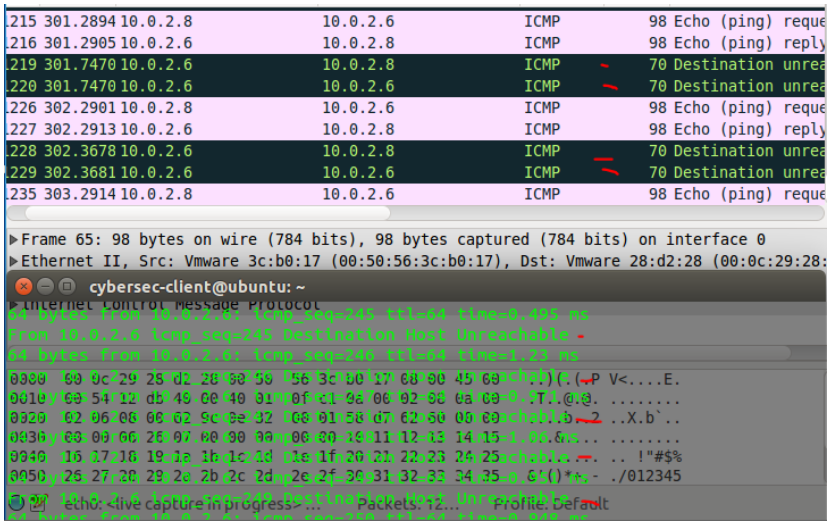
To see traffic, ping 10.0.2.6



To run the attack, open Netwag on the Cybersec-Attacker , type icmp and use number 82 and type the following information and run it



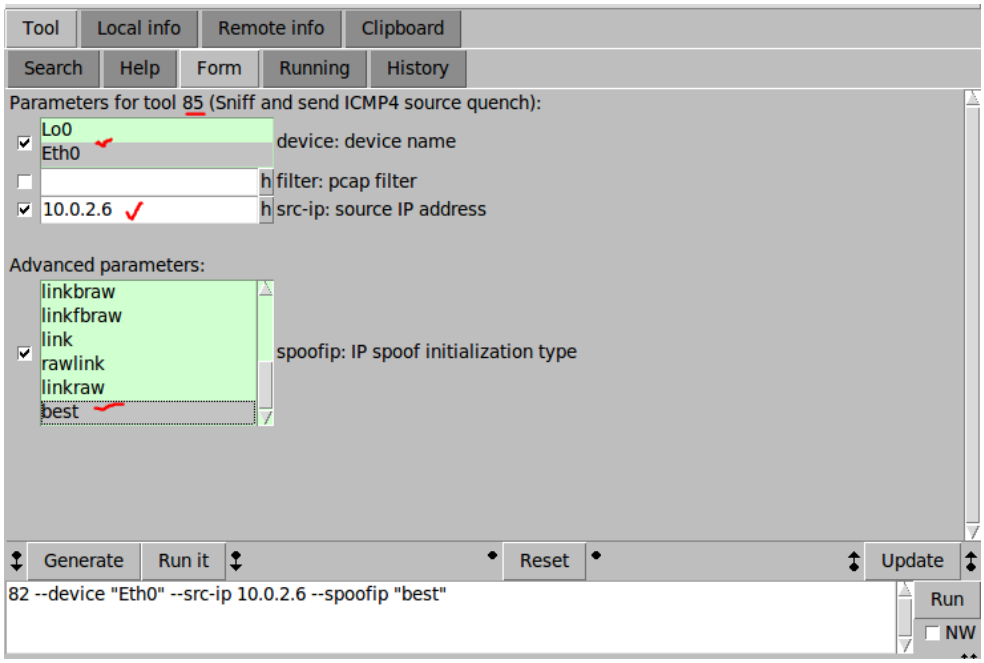
See again the traffic on CyberSec-Client

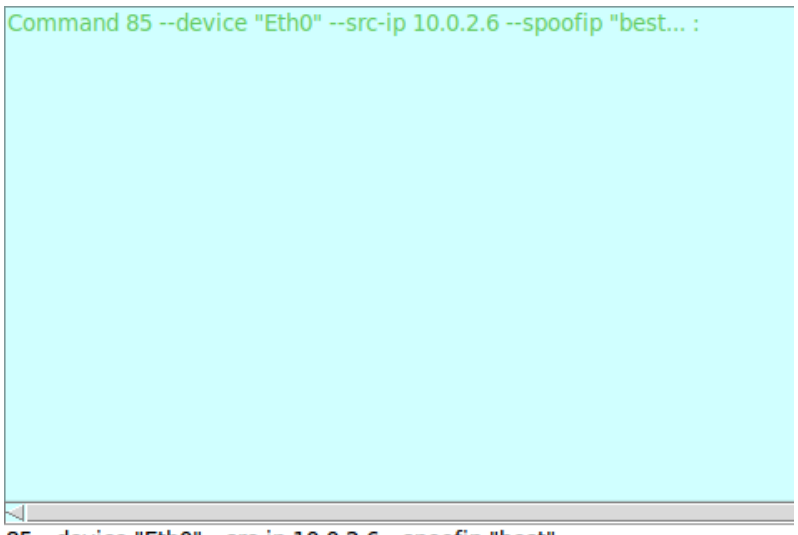


Source-Quench Attacks

Open CyberSec-Client then ping 10.0.2.6

Open netwag on CyberSec-Attacker, then choose '85' and follow as seen in the screenshot, then press run it.

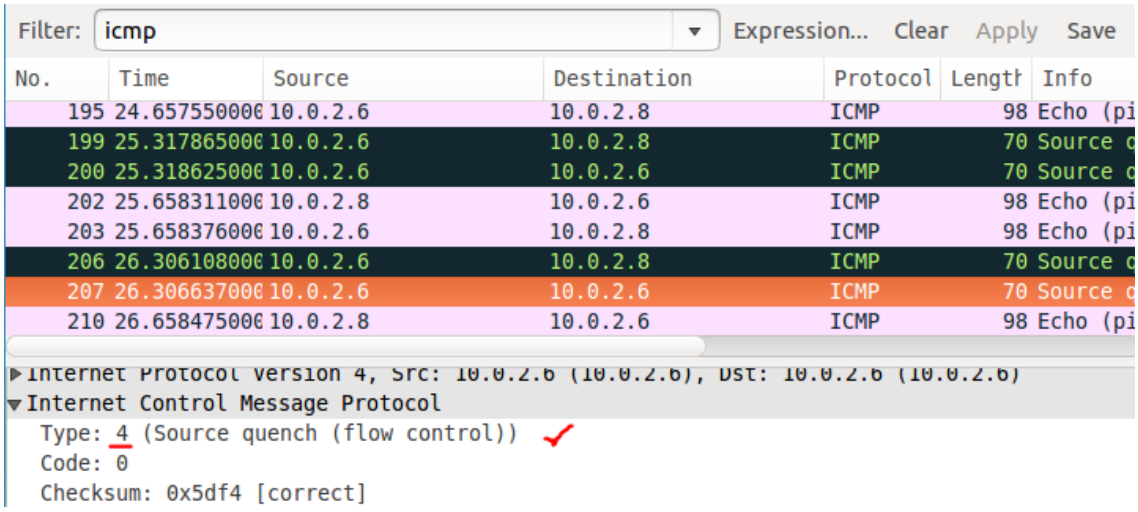




85 --device "Eth0" --src-ip 10.0.2.6 --spoofip "best"

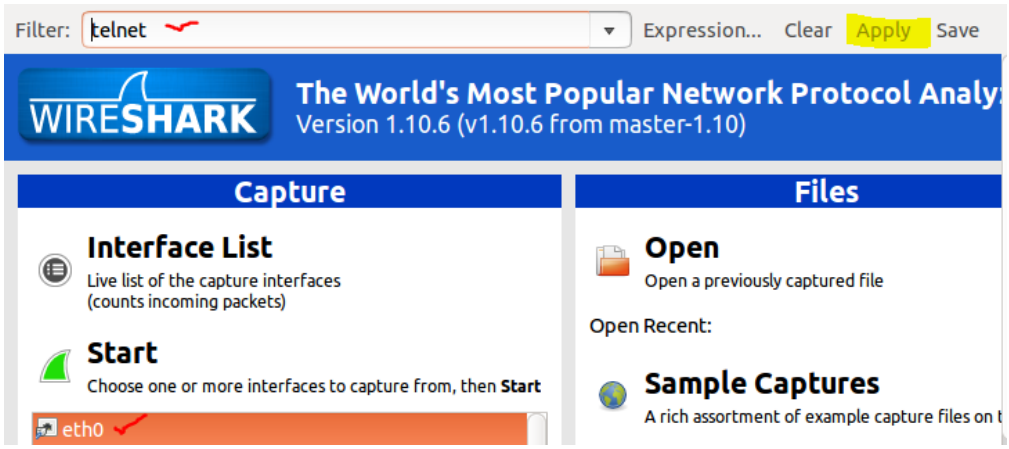
Source Quench coming through

Open wireshark on CyberSec-Server, press icmp on the filter and ‘eth0’. As can be seen, Type 4 means Source quench (flow control).

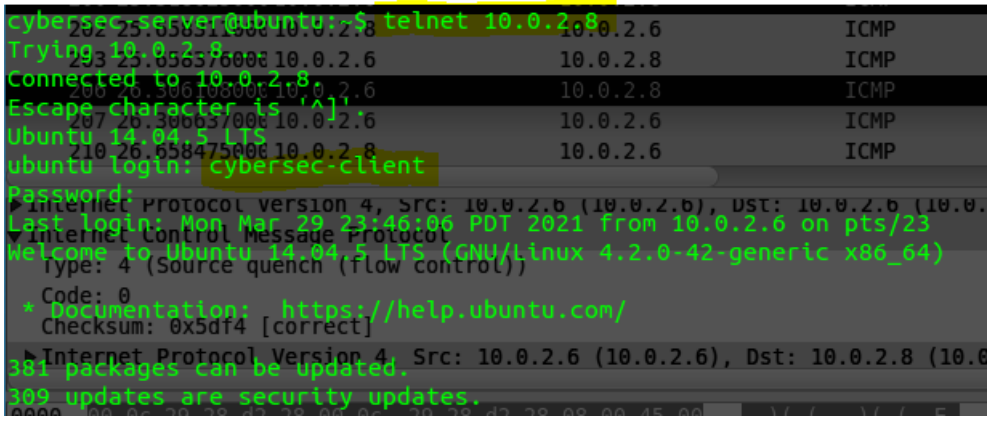


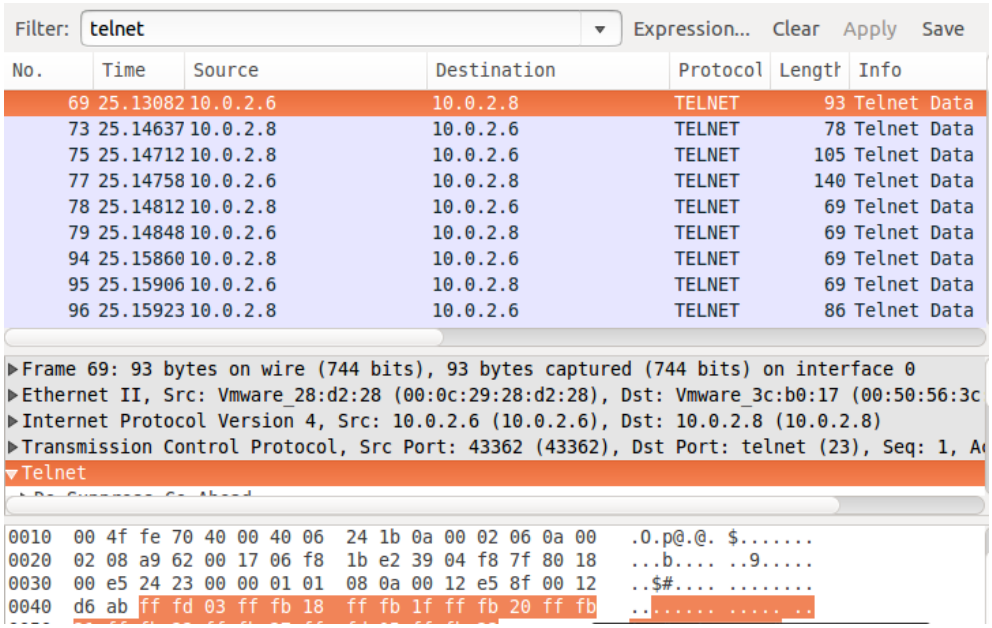
Task 6: TCP Session Hijacking

Open wireshark on CyberSec-Client, then choose ‘eth0’ and type ‘telnet’ on filter then press start.

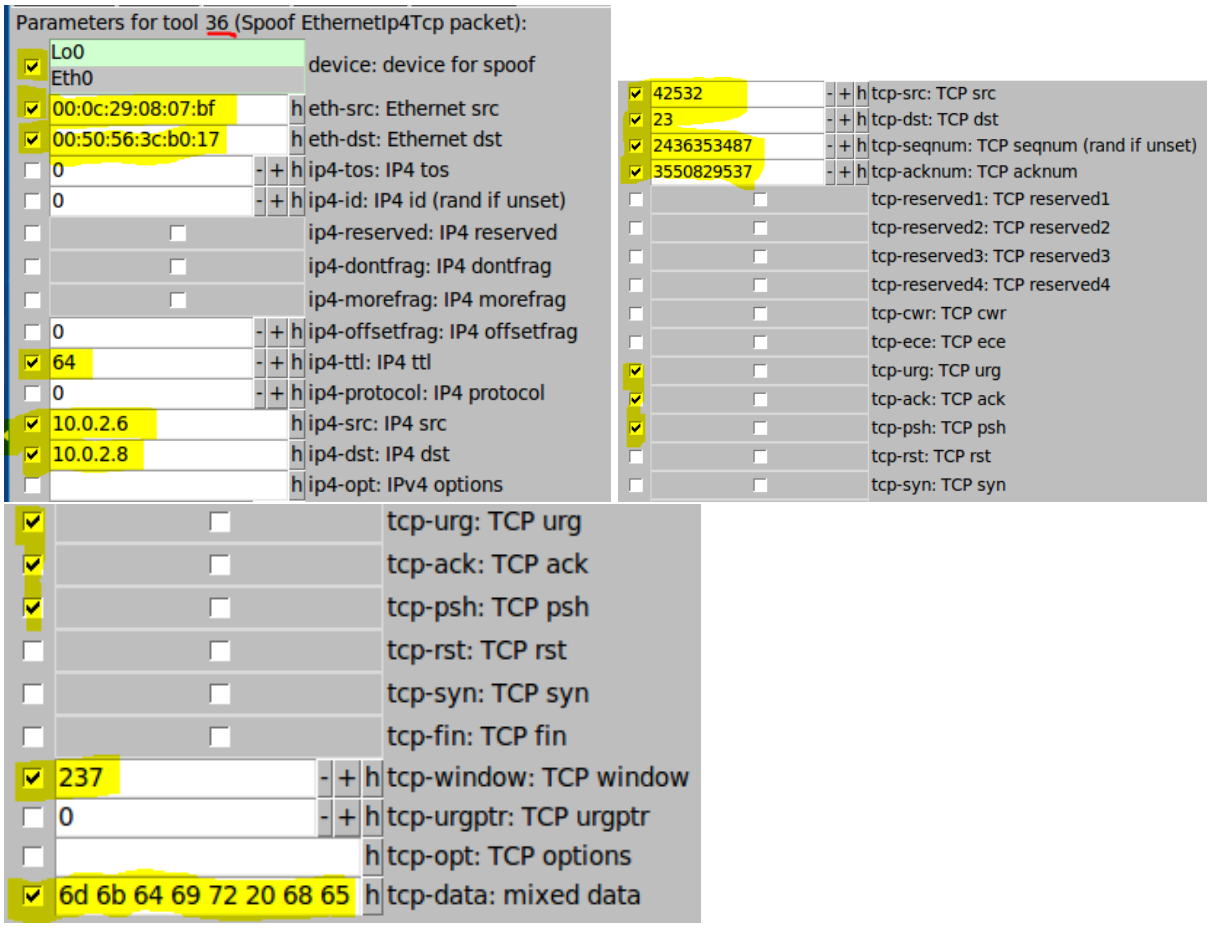


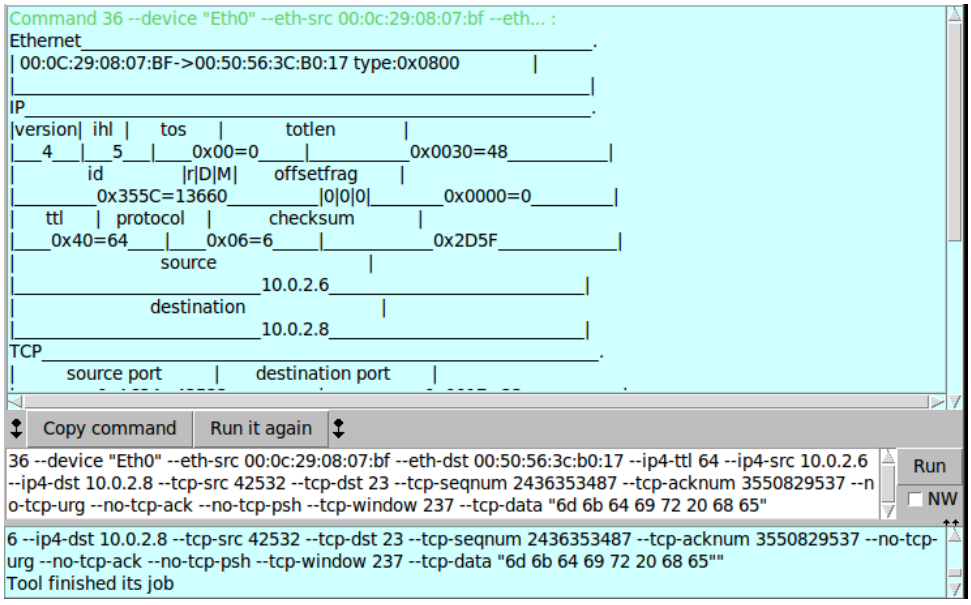
On CyberSec-Server, type ‘telnet 10.0.2.8’ on the terminal and fill ‘cybersec-client’ on Ubuntu login also ‘cybersec’ as the password.





Open netwag on CyberSec-Attacker, tick the column and change the data as can be seen below. For mixed data, type ‘6d 6b 64 69 72 20 68 65 6c 6c 6f 0a’ which create ‘mkdir hello’ and run it.





After running the netwag, go back to CyberSec-Client, as seen below it changes into ‘mk dir hello’ which mean make new directory name hello.

```
2820 1581.152 10.0.2.6          10.0.2.8          TELNET      66

  Window size value: 237
  [Calculated window size: 237]
  [Window size scaling factor: -1 (unknown)]
▶ Checksum: 0xda42 [validation disabled]
▶ [SEQ/ACK analysis]
▼ Telnet
  Data: mkdir hello\n

0010  00 34 b8 06 00 00 40 06  aa b0 0a 00 02 06 0a 00   .4....@. ........
0020  02 08 a6 24 00 17 91 37  cd cf d3 a5 5b e1 50 00   ...$...7 ....[.P.
0030  00 ed da 42 00 00 6d 6b  64 69 72 20 68 65 6c 6c   ...B..mk dir hell
0040  6f 0a                                             o.
```

hello directory has been made.