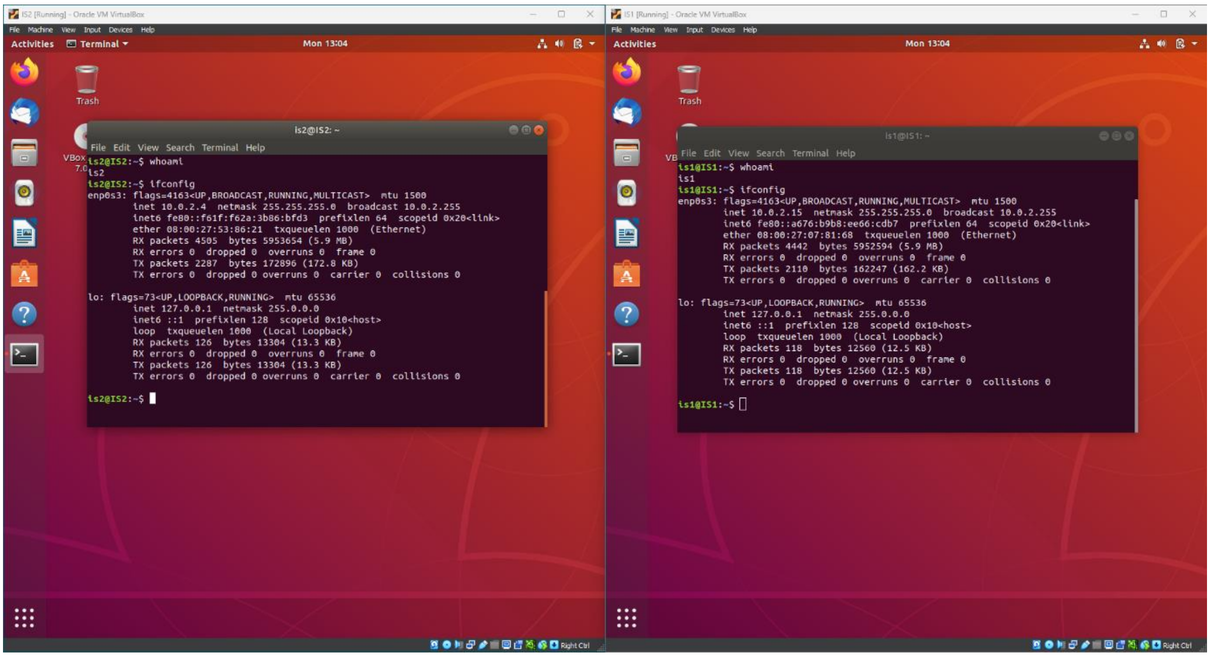
Telnet & SSH Security Analysis

- Initially we setup 2 VMs where we config the IP of the machine (note: it should be different)
- Here we setup 2 machines **is1** & **is2** and check the IP using "$ ifconfig"
- It is important to execute the following command in the terminal to able to analyse the packet.
  $ su (changes to superuser if your current user is not in sudoers file)
  $ sudo usermod -aG sudo <*user-name*> (execute this command and restart the system then execute the below commands)

  $ sudo apt install update && sudo apt upgrade
  $ sudo apt install telnetd -y
  $ sudo apt install openssh-server -y
  $ sudo apt install net-tools
  $ sudo apt install wireshark

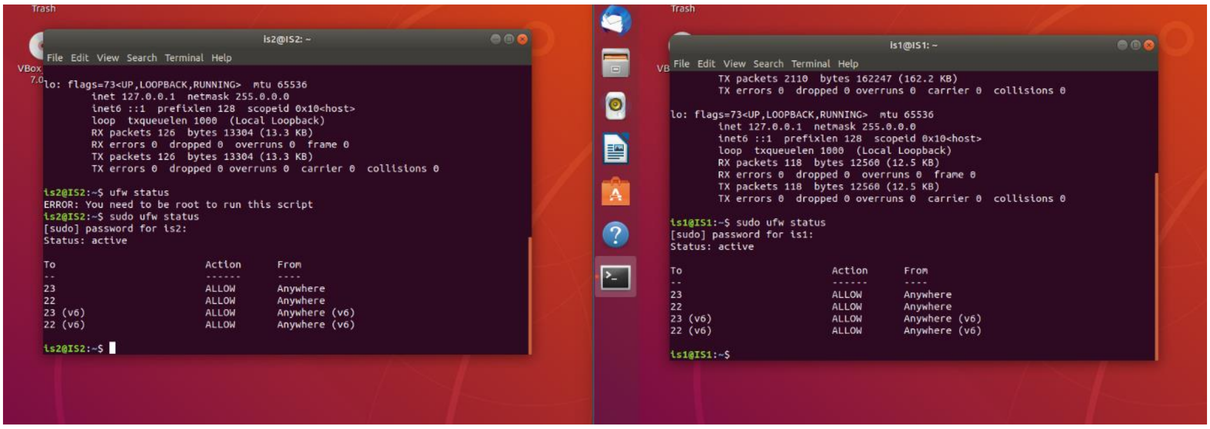

IS2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 13:04
Trash
is2@IS2: ~
File Edit View Search Terminal Help
IS1 [Running] - Oracle VM VirtualBox
is1@IS1: ~
Right Ctrl

```
is2@IS2:~$ whoami
is2
is2@IS2:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::f61f:f62a:3b86:bfd3  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:53:86:21  txqueuelen 1000  (Ethernet)
        RX packets 4505  bytes 5953654 (5.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2287  bytes 172896 (172.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 126  bytes 13304 (13.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 126  bytes 13304 (13.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

is2@IS2:~$
```

```
is1@IS1:~$ whoami
is1
is1@IS1:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a676:b9b8:ee66:cdb7  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:07:81:68  txqueuelen 1000  (Ethernet)
        RX packets 4442  bytes 5952594 (5.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2110  bytes 162247 (162.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 118  bytes 12560 (12.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 118  bytes 12560 (12.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

is1@IS1:~$
```

- Now using firewall allow port 23 and port 22 for telnet & ssh connection simultaneously using the following commands:
  $ sudo ufw status (checks status of the firewall that which rules are allowed or added)
  $ sudo ufw enable (enables if disabled)
  $ sudo ufw allow 22 (open port 22 for connection)
  $ sudo ufw allow 23
  $ sudo ufw reject 22 (close the port after using as it is a good practice)

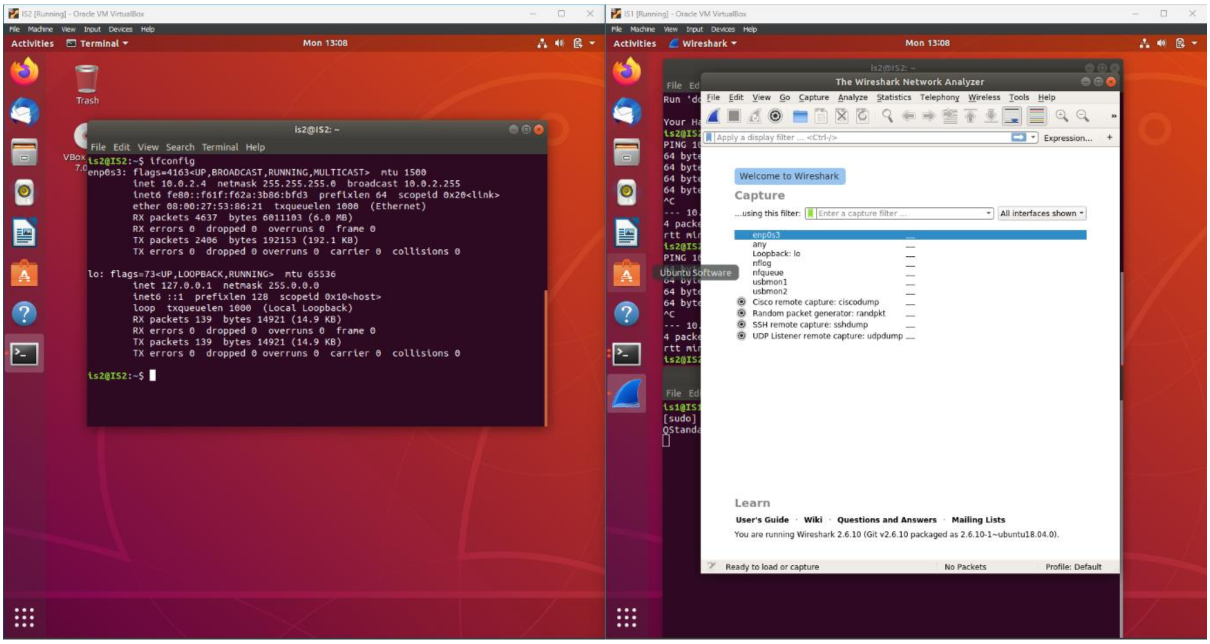
  Note: execute these commands on the server machine.



```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 126  bytes 13304 (13.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 126  bytes 13304 (13.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

is2@IS2:~$ ufw status
ERROR: You need to be root to run this script
is2@IS2:~$ sudo ufw status
[sudo] password for is2:
Status: active

To                         Action      From
--                         ------      ----
23                         ALLOW       Anywhere
22                         ALLOW       Anywhere
23 (v6)                    ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)

is2@IS2:~$
```

```
        TX packets 2110  bytes 162247 (162.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 118  bytes 12560 (12.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 118  bytes 12560 (12.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

is1@IS1:~$ sudo ufw status
[sudo] password for is1:
Status: active

To                         Action      From
--                         ------      ----
23                         ALLOW       Anywhere
22                         ALLOW       Anywhere
23 (v6)                    ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)

is1@IS1:~$
```

- Use " $ sudo wireshark" in the server side to open wireshark and analyse the packets on behalf of client side


IS2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 13:08
Trash
is2@IS2: ~
File Edit View Search Terminal Help
IS1 [Running] - Oracle VM VirtualBox
Wireshark
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
Enter a capture filter ...
All interfaces shown
Ubuntu Software
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

```
is2@IS2:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::f61f:f62a:3b86:bfd3  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:53:86:21  txqueuelen 1000  (Ethernet)
        RX packets 4637  bytes 6011103 (6.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2406  bytes 192153 (192.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 139  bytes 14921 (14.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 139  bytes 14921 (14.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

is2@IS2:~$
```

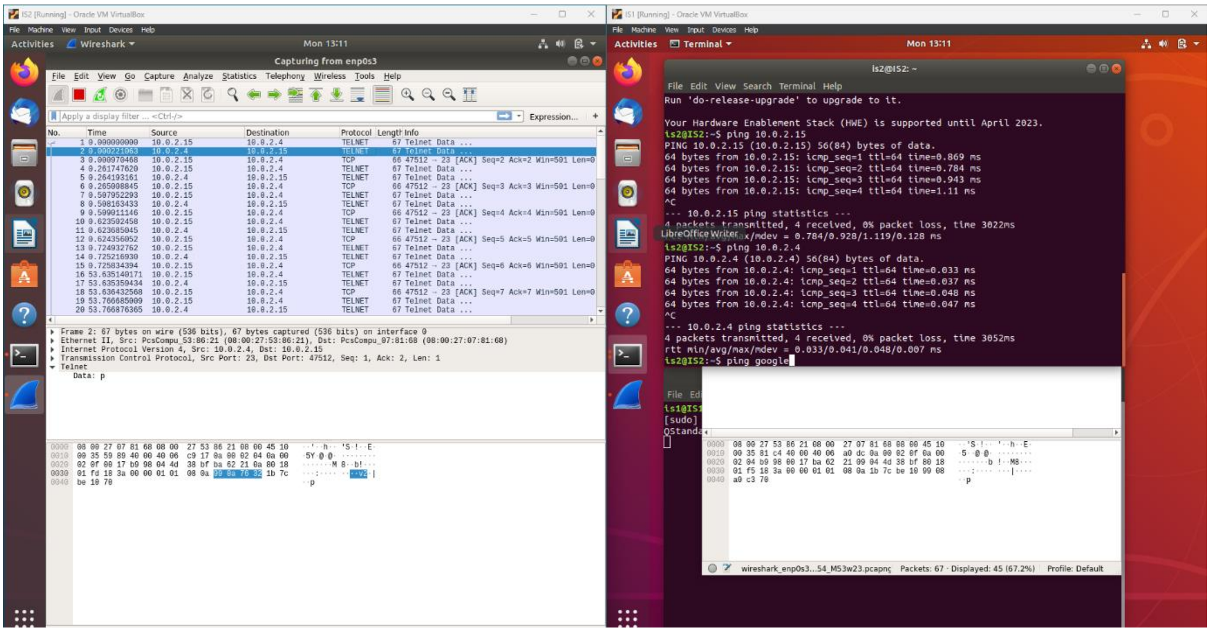
...using this filter:

enp0s3
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

Ready to load or capture   No Packets   Profile: Default

- Use " $ telnet *<ip_address of other machine or server machine>"* and login using the name & password of other machine to establish telnet connection to the server.
- In case of SSH use " $ ssh *<username_of_other_machine_or_server>@<ip_address_of_server_or_other_machine>* and login using the password of the machine.


IS2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Wireshark Mon 13:11
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
IS1 [Running] - Oracle VM VirtualBox
Activities Terminal Mon 13:11
is2@IS2: ~
File Edit View Search Terminal Help
LibreOffice Writer
wireshark_enp0s3...54_M53w23.pcapng Packets: 67 · Displayed: 45 (67.2%) Profile: Default

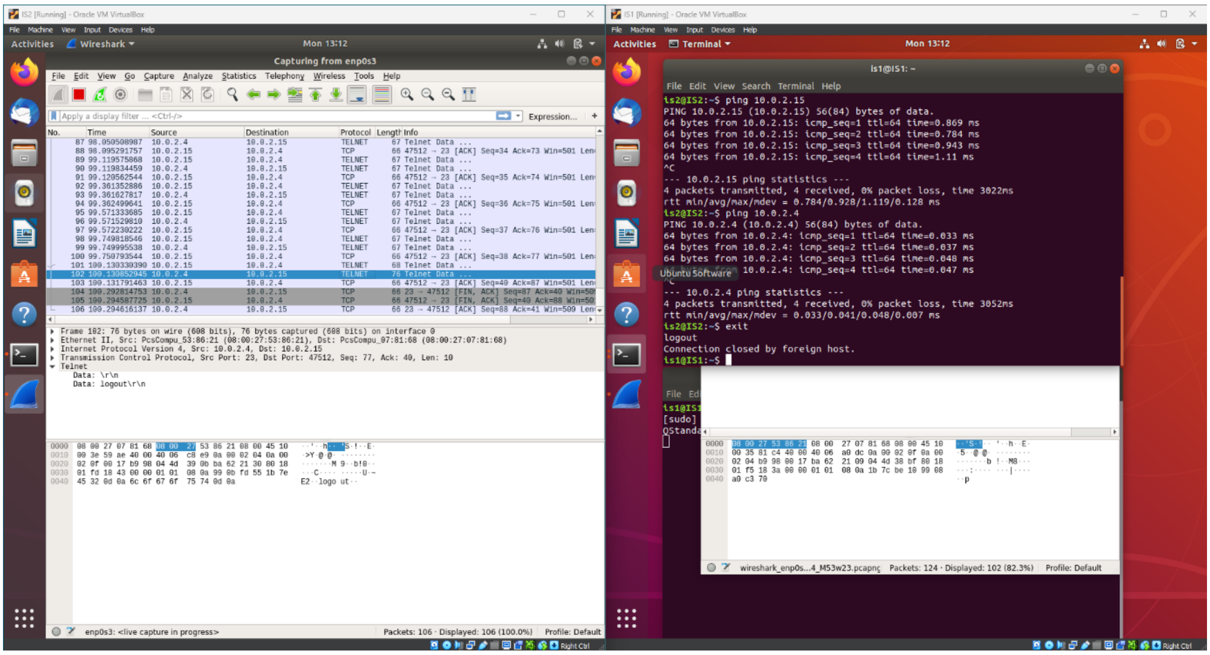
```
No.  Time          Source      Destination  Protocol Length Info
   1 0.000000000   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
   2 0.000221063   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
   3 0.000970468   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=2 Ack=2 Win=501 Len=0
   4 0.261747620   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
   5 0.264193161   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
   6 0.265008845   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=3 Ack=3 Win=501 Len=0
   7 0.507952293   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
   8 0.508163433   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
   9 0.509011146   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=4 Ack=4 Win=501 Len=0
  10 0.623502458   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
  11 0.623685045   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
  12 0.624356052   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=5 Ack=5 Win=501 Len=0
  13 0.724932762   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
  14 0.725216930   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
  15 0.725834394   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=6 Ack=6 Win=501 Len=0
  16 53.635140171  10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
  17 53.635359434  10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
  18 53.636432568  10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=7 Ack=7 Win=501 Len=0
  19 53.766685009  10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
  20 53.766876365  10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...

▸ Frame 2: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_53:86:21 (08:00:27:53:86:21), Dst: PcsCompu_07:81:68 (08:00:27:07:81:68)
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 47512, Seq: 1, Ack: 2, Len: 1
▾ Telnet
    Data: p

0000  08 00 27 07 81 68 08 00  27 53 86 21 08 00 45 10   ··'··h·· 'S·!··E·
0010  00 35 59 89 40 00 40 06  c9 17 0a 00 02 04 0a 00   ·5Y·@·@· ········
0020  02 0f 00 17 b9 98 04 4d  38 bf ba 62 21 0a 80 18   ·······M 8··b!···
0030  01 fd 18 3a 00 00 01 01  08 0a 09 0a 76 32 1b 7c   ···:···· ····v2·|
0040  be 10 70                                           ··p
```

```
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
is2@IS2:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.869 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.784 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.943 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=1.11 ms
^C
--- 10.0.2.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3022ms
rtt min/avg/max/mdev = 0.784/0.928/1.119/0.128 ms
is2@IS2:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.033 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.047 ms
^C
--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.033/0.041/0.048/0.007 ms
is2@IS2:~$ ping google
```

```
is1@IS1
[sudo]
QStanda

0000  08 00 27 53 86 21 08 00  27 07 81 68 08 00 45 10   ··'S·!·· '··h··E·
0010  00 35 81 c4 40 00 40 06  a0 dc 0a 00 02 0f 0a 00   ·5··@·@· ········
0020  02 04 b9 98 00 17 ba 62  21 09 04 4d 38 bf 80 18   ·······b !··M8···
0030  01 f5 18 3a 00 00 01 01  08 0a 1b 7c be 10 99 08   ···:···· ···|····
0040  a0 c3 70                                           ··p
```

- Here in telnet, we can see the data in the packets as when we analyse a telnet packet when we gave input in the terminal of the connected machine. Here in above screenshot, we can see under Telnet where data is “P” and in the terminal of the other screen I have given input as “ping google.com” which show packets are generated for each character and two packets can be seen in Wireshark showing one packet as incoming call and other one for the acknowledgment, hence we can analyse the packet and data residing in the packet in telnet connection like this. To filter out only those packets with port 23 connection we will write “ tcp.port==23” in the above URL space.

- After analysing the packet enter “$ exit” to logout from client side.

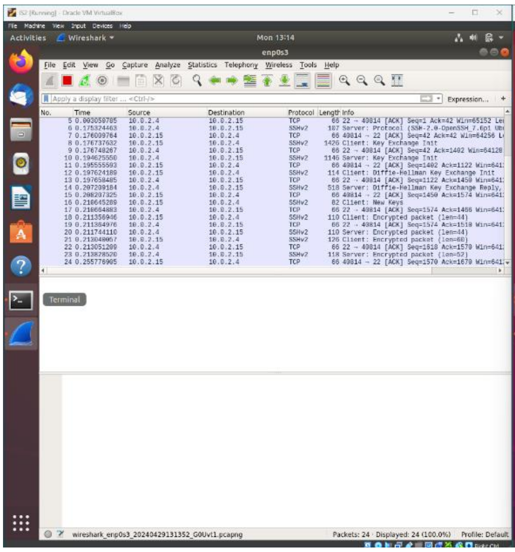

IS2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Wireshark Mon 13:12
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
enp0s3: <live capture in progress> Packets: 106 · Displayed: 106 (100.0%) Profile: Default
IS1 [Running] - Oracle VM VirtualBox
Activities Terminal Mon 13:12
is1@IS1: ~
File Edit View Search Terminal Help
Ubuntu Software
wireshark_enp0s...4_M53w23.pcapng Packets: 124 · Displayed: 102 (82.3%) Profile: Default

```
No.  Time           Source      Destination  Protocol Length Info
  87 98.050508987   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
  88 98.095291757   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=34 Ack=73 Win=501 Len=
  89 99.119575868   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
  90 99.119834459   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
  91 99.120562544   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=35 Ack=74 Win=501 Len=
  92 99.361352886   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
  93 99.361627817   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
  94 99.362499641   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=36 Ack=75 Win=501 Len=
  95 99.571333685   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
  96 99.571529810   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
  97 99.572230222   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=37 Ack=76 Win=501 Len=
  98 99.749818546   10.0.2.15   10.0.2.4     TELNET   67 Telnet Data ...
  99 99.749995538   10.0.2.4    10.0.2.15    TELNET   67 Telnet Data ...
 100 99.750793544   10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=38 Ack=77 Win=501 Len=
 101 100.130330390  10.0.2.15   10.0.2.4     TELNET   68 Telnet Data ...
 102 100.130852945  10.0.2.4    10.0.2.15    TELNET   76 Telnet Data ...
 103 100.131791463  10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [ACK] Seq=40 Ack=87 Win=501 Len=
 104 100.292814753  10.0.2.4    10.0.2.15    TCP      66 23 → 47512 [FIN, ACK] Seq=87 Ack=40 Win=50
 105 100.294587725  10.0.2.15   10.0.2.4     TCP      66 47512 → 23 [FIN, ACK] Seq=40 Ack=88 Win=50
 106 100.294616137  10.0.2.4    10.0.2.15    TCP      66 23 → 47512 [ACK] Seq=88 Ack=41 Win=509 Len=

▸ Frame 102: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_53:86:21 (08:00:27:53:86:21), Dst: PcsCompu_07:81:68 (08:00:27:07:81:68)
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 23, Dst Port: 47512, Seq: 77, Ack: 40, Len: 10
▾ Telnet
    Data: \r\n
    Data: logout\r\n

0000  08 00 27 07 81 68 08 00  27 53 86 21 08 00 45 10   ··'··h·· 'S·!··E·
0010  00 3e 59 ae 40 00 40 06  c8 e9 0a 00 02 04 0a 00   ·>Y·@·@· ········
0020  02 0f 00 17 b9 98 04 4d  39 0b ba 62 21 30 80 18   ·······M 9··b!0··
0030  01 fd 18 43 00 00 01 01  08 0a 99 0b fd 55 1b 7e   ···C···· ·····U·~
0040  45 32 0d 0a 6c 6f 67 6f  75 74 0d 0a               E2··logo ut··
```

```
is2@IS2:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.869 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.784 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.943 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=1.11 ms
^C
--- 10.0.2.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3022ms
rtt min/avg/max/mdev = 0.784/0.928/1.119/0.128 ms
is2@IS2:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.033 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.047 ms
^C
--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.033/0.041/0.048/0.007 ms
is2@IS2:~$ exit
logout
Connection closed by foreign host.
is1@IS1:~$
```

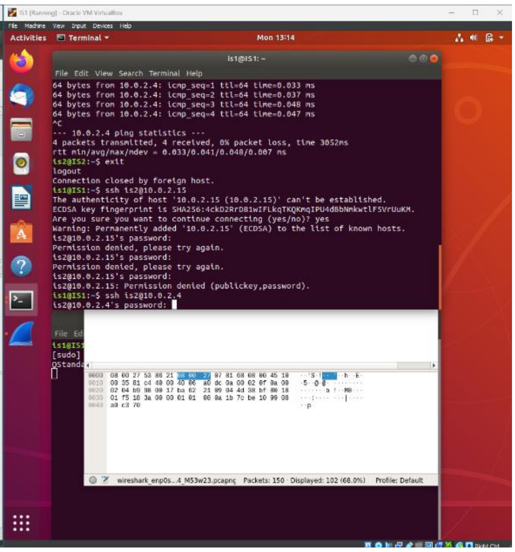
```
is1@IS1
[sudo]
QStanda

0000  08 00 27 53 86 21 08 00  27 07 81 68 08 00 45 10   ··'S·!·· '··h··E·
0010  00 35 81 c4 40 00 40 06  a0 dc 0a 00 02 0f 0a 00   ·5··@·@· ········
0020  02 04 b9 98 00 17 ba 62  21 09 04 4d 38 bf 80 18   ·······b !··M8···
0030  01 f5 18 3a 00 00 01 01  08 0a 1b 7c be 10 99 08   ···:···· ···|····
0040  a0 c3 70                                           ··p
```

- Now connect via SSH using the command mentioned above and analyse the packets in the same way as we did for telnet connection but remember while filtering out use port 22 to filter out ssh connection's packet.



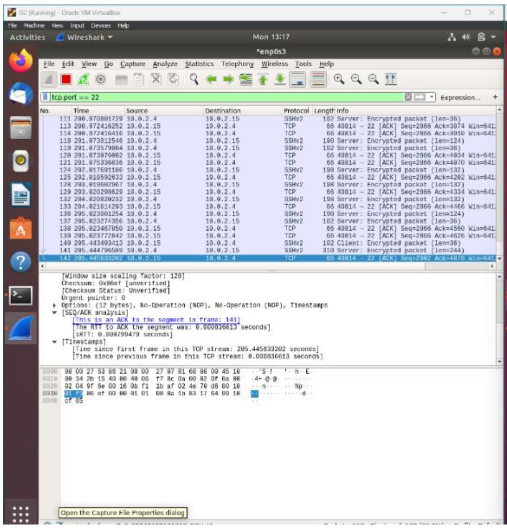
```
No. Time          Source     Destination Protocol Length Info
  5 0.003050785   10.0.2.4   10.0.2.15   TCP        66 22 → 40814 [ACK] Seq=1 Ack=42 Win=65152 Le
  6 0.175324463   10.0.2.4   10.0.2.15   SSHv2     107 Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Ub
  7 0.176009764   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=42 Ack=42 Win=64256 L
  8 0.176737632   10.0.2.15  10.0.2.4    SSHv2    1426 Client: Key Exchange Init
  9 0.176748267   10.0.2.4   10.0.2.15   TCP        66 22 → 40814 [ACK] Seq=42 Ack=1402 Win=64128
 10 0.194625550   10.0.2.4   10.0.2.15   SSHv2    1146 Server: Key Exchange Init
 11 0.195555593   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=1402 Ack=1122 Win=641
 12 0.197624189   10.0.2.15  10.0.2.4    SSHv2     114 Client: Diffie-Hellman Key Exchange Init
 13 0.197658485   10.0.2.4   10.0.2.15   TCP        66 22 → 40814 [ACK] Seq=1122 Ack=1450 Win=641
 14 0.207209184   10.0.2.4   10.0.2.15   SSHv2     518 Server: Diffie-Hellman Key Exchange Reply,
 15 0.208207325   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=1450 Ack=1574 Win=641
 16 0.210645289   10.0.2.15  10.0.2.4    SSHv2      82 Client: New Keys
 17 0.210664883   10.0.2.4   10.0.2.15   TCP        66 22 → 40814 [ACK] Seq=1574 Ack=1466 Win=641
 18 0.211356946   10.0.2.15  10.0.2.4    SSHv2     110 Client: Encrypted packet (len=44)
 19 0.211364976   10.0.2.4   10.0.2.15   TCP        66 22 → 40814 [ACK] Seq=1574 Ack=1510 Win=641
 20 0.211744110   10.0.2.4   10.0.2.15   SSHv2     110 Server: Encrypted packet (len=44)
 21 0.213048057   10.0.2.15  10.0.2.4    SSHv2     126 Client: Encrypted packet (len=60)
 22 0.213051209   10.0.2.4   10.0.2.15   TCP        66 22 → 40814 [ACK] Seq=1618 Ack=1570 Win=641
 23 0.213828520   10.0.2.4   10.0.2.15   SSHv2     118 Server: Encrypted packet (len=52)
 24 0.255776905   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=1570 Ack=1670 Win=641
```

wireshark_enp0s3_20240429131352_G0Uvt1.pcapng Packets: 24 · Displayed: 24 (100.0%) Profile: Default



```
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.033 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.047 ms
^C
--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.033/0.041/0.048/0.007 ms
is2@IS2:~$ exit
logout
Connection closed by foreign host.
is1@IS1:~$ ssh is2@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ECDSA key fingerprint is SHA256:4ckD2RrD81wIFLkqTKQKmqIPU4dBbNmkwtlF5VrUuKM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.15' (ECDSA) to the list of known hosts.
is2@10.0.2.15's password:
Permission denied, please try again.
is2@10.0.2.15's password:
Permission denied, please try again.
is2@10.0.2.15's password:
is2@10.0.2.15: Permission denied (publickey,password).
is1@IS1:~$ ssh is2@10.0.2.4
is2@10.0.2.4's password:
```

wireshark_enp0s...4_M53w23.pcapng Packets: 150 · Displayed: 102 (68.0%) Profile: Default



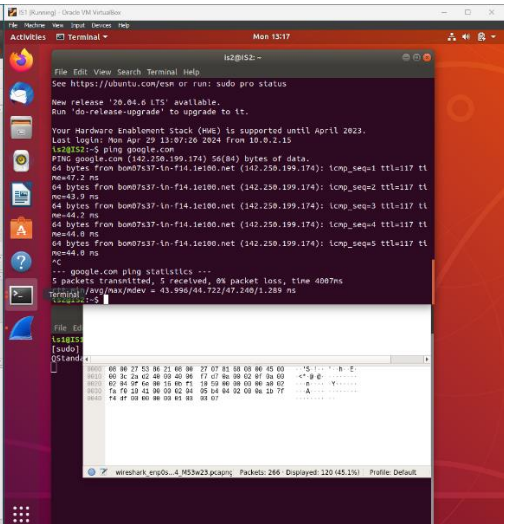
tcp.port == 22

```
No. Time            Source     Destination Protocol Length Info
111 200.970801729   10.0.2.4   10.0.2.15   SSHv2     102 Server: Encrypted packet (len=36)
113 200.972416252   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=3874 Win=641
114 200.972416416   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=3910 Win=641
118 201.073812546   10.0.2.4   10.0.2.15   SSHv2     190 Server: Encrypted packet (len=124)
119 201.073579804   10.0.2.4   10.0.2.15   SSHv2     102 Server: Encrypted packet (len=36)
120 201.073876002   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4034 Win=641
121 201.075336836   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4070 Win=641
124 202.017691186   10.0.2.4   10.0.2.15   SSHv2     198 Server: Encrypted packet (len=132)
125 202.018592633   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4202 Win=641
128 203.019602967   10.0.2.4   10.0.2.15   SSHv2     198 Server: Encrypted packet (len=132)
129 203.020298629   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4334 Win=641
132 204.020820232   10.0.2.4   10.0.2.15   SSHv2     198 Server: Encrypted packet (len=132)
133 204.021614293   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4466 Win=641
136 205.023001254   10.0.2.4   10.0.2.15   SSHv2     190 Server: Encrypted packet (len=124)
137 205.023274356   10.0.2.4   10.0.2.15   SSHv2     102 Server: Encrypted packet (len=36)
138 205.023467850   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4590 Win=641
139 205.023772842   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4626 Win=641
140 205.443493413   10.0.2.15  10.0.2.4    SSHv2     102 Client: Encrypted packet (len=36)
141 205.444796589   10.0.2.4   10.0.2.15   SSHv2     310 Server: Encrypted packet (len=244)
142 205.445633202   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2902 Ack=4870 Win=641
```

```
      [Window size scaling factor: 128]
      Checksum: 0x86ef [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
    ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    ▾ [SEQ/ACK analysis]
         [This is an ACK to the segment in frame: 141]
         [The RTT to ACK the segment was: 0.000036613 seconds]
         [iRTT: 0.000799479 seconds]
    ▾ [Timestamps]
         [Time since first frame in this TCP stream: 205.445633202 seconds]
         [Time since previous frame in this TCP stream: 0.000836613 seconds]
```

```
0000  08 00 27 53 86 21 08 00  27 07 81 68 08 00 45 10   ··'S·!·· '··h··E·
0010  00 34 2b 15 40 00 40 06  f7 8c 0a 00 02 0f 0a 00   ·4+·@·@· ········
0020  02 04 9f 6e 00 16 0b f1  1b af 02 4e 70 d8 80 10   ···n···· ···Np···
0030  01 f5 86 ef 00 00 01 01  08 0a 1b 83 17 64 99 10   ········ ·····d··
0040  cf 65                                              ··
```

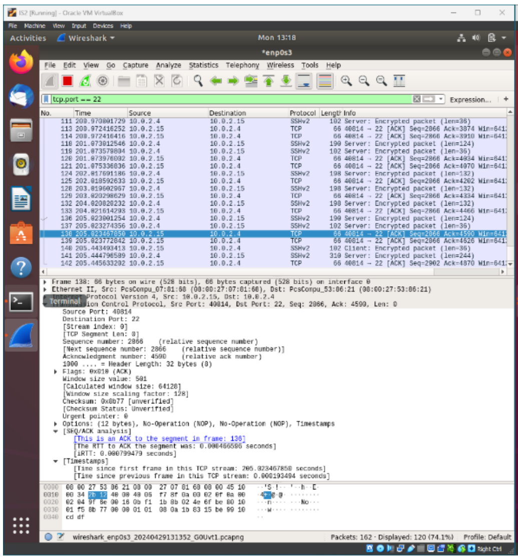
Open the Capture File Properties dialog



```
See https://ubuntu.com/esm or run: sudo pro status

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Mon Apr 29 13:07:26 2024 from 10.0.2.15
is2@IS2:~$ ping google.com
PING google.com (142.250.199.174) 56(84) bytes of data.
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=1 ttl=117 ti
me=47.2 ms
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=2 ttl=117 ti
me=43.9 ms
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=3 ttl=117 ti
me=44.2 ms
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=4 ttl=117 ti
me=44.0 ms
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=5 ttl=117 ti
me=44.0 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 43.996/44.722/47.240/1.289 ms
is2@IS2:~$
```

```
0000  08 00 27 53 86 21 08 00  27 07 81 68 08 00 45 00   ··'S·!·· '··h··E·
0010  00 3c 2a d2 40 00 40 06  f7 d7 0a 00 02 0f 0a 00   ·<*·@·@· ········
0020  02 04 9f 6e 00 16 0b f1  18 59 00 00 00 00 a0 02   ···n···· ·Y······
0030  fa f0 18 41 00 00 02 04  05 b4 04 02 08 0a 1b 7f   ···A···· ········
0040  f4 df 00 00 00 00 01 03  03 07                     ········ ··
```

wireshark_enp0s...4_M53w23.pcapng Packets: 266 · Displayed: 120 (45.1%) Profile: Default



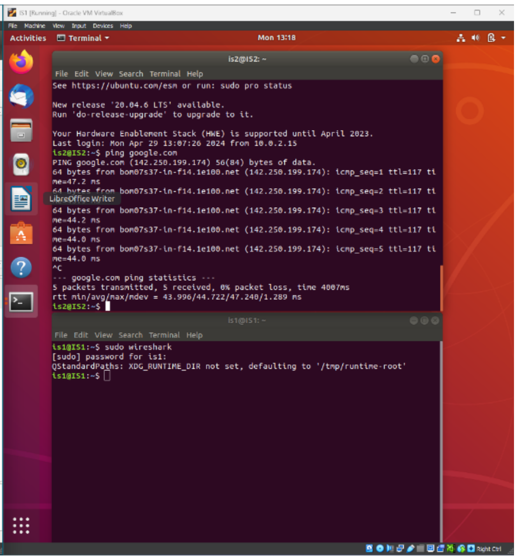
tcp.port == 22

```
No. Time            Source     Destination Protocol Length Info
111 200.970801729   10.0.2.4   10.0.2.15   SSHv2     102 Server: Encrypted packet (len=36)
113 200.972416252   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=3874 Win=641
114 200.972416416   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=3910 Win=641
118 201.073012546   10.0.2.4   10.0.2.15   SSHv2     190 Server: Encrypted packet (len=124)
119 201.073579804   10.0.2.4   10.0.2.15   SSHv2     102 Server: Encrypted packet (len=36)
120 201.073876002   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4034 Win=641
121 201.075336836   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4070 Win=641
124 202.017691186   10.0.2.4   10.0.2.15   SSHv2     198 Server: Encrypted packet (len=132)
125 202.018592633   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4202 Win=641
128 203.019602967   10.0.2.4   10.0.2.15   SSHv2     198 Server: Encrypted packet (len=132)
129 203.020298629   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4334 Win=641
132 204.020820232   10.0.2.4   10.0.2.15   SSHv2     198 Server: Encrypted packet (len=132)
133 204.021614293   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4466 Win=641
136 205.023001254   10.0.2.4   10.0.2.15   SSHv2     190 Server: Encrypted packet (len=124)
137 205.023274356   10.0.2.4   10.0.2.15   SSHv2     102 Server: Encrypted packet (len=36)
138 205.023467850   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4590 Win=641
139 205.023772842   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2866 Ack=4626 Win=641
140 205.443493413   10.0.2.15  10.0.2.4    SSHv2     102 Client: Encrypted packet (len=36)
141 205.444796589   10.0.2.4   10.0.2.15   SSHv2     310 Server: Encrypted packet (len=244)
142 205.445633202   10.0.2.15  10.0.2.4    TCP        66 40814 → 22 [ACK] Seq=2902 Ack=4870 Win=641
```

```
▸ Frame 138: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_07:81:68 (08:00:27:07:81:68), Dst: PcsCompu_53:86:21 (08:00:27:53:86:21)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
▾ Transmission Control Protocol, Src Port: 40814, Dst Port: 22, Seq: 2866, Ack: 4590, Len: 0
    Source Port: 40814
    Destination Port: 22
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 2866    (relative sequence number)
    [Next sequence number: 2866    (relative sequence number)]
    Acknowledgment number: 4590    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window size value: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0x8b77 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▾ [SEQ/ACK analysis]
       [This is an ACK to the segment in frame: 136]
       [The RTT to ACK the segment was: 0.000466596 seconds]
       [iRTT: 0.000799479 seconds]
  ▾ [Timestamps]
       [Time since first frame in this TCP stream: 205.023467850 seconds]
       [Time since previous frame in this TCP stream: 0.000193494 seconds]
```

```
0000  08 00 27 53 86 21 08 00  27 07 81 68 08 00 45 10   ··'S·!·· '··h··E·
0010  00 34 2b 12 40 00 40 06  f7 8f 0a 00 02 0f 0a 00   ·4+·@·@· ········
0020  02 04 9f 6e 00 16 0b f1  1b 8b 02 4e 6f be 80 10   ···n···· ···No···
0030  01 f5 8b 77 00 00 01 01  08 0a 1b 83 15 be 99 10   ···w···· ········
0040  cd df                                              ··
```

wireshark_enp0s3_20240429131352_G0Uvt1.pcapng Packets: 162 · Displayed: 120 (74.1%) Profile: Default

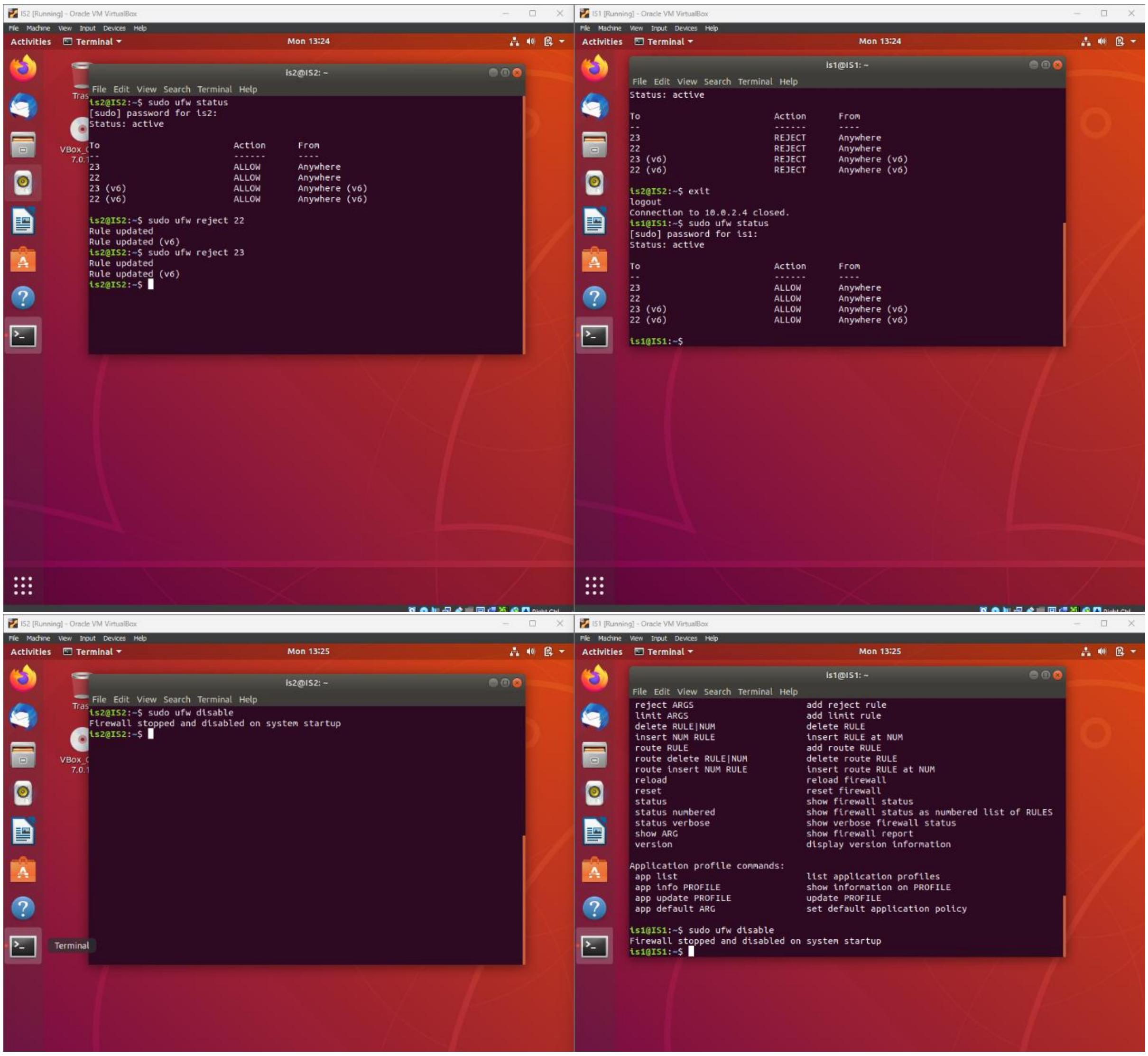


```
See https://ubuntu.com/esm or run: sudo pro status

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Mon Apr 29 13:07:26 2024 from 10.0.2.15
is2@IS2:~$ ping google.com
PING google.com (142.250.199.174) 56(84) bytes of data.
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=1 ttl=117 ti
me=47.2 ms
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=2 ttl=117 ti
me=43.9 ms
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=3 ttl=117 ti
me=44.2 ms
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=4 ttl=117 ti
me=44.0 ms
64 bytes from bom07s37-in-f14.1e100.net (142.250.199.174): icmp_seq=5 ttl=117 ti
me=44.0 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 43.996/44.722/47.240/1.289 ms
is2@IS2:~$
```

```
is1@IS1:~$ sudo wireshark
[sudo] password for is1:
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
is1@IS1:~$
```

- While analysing the ssh packets you will note you aren’t able to see the data in it and in place it you are able to see message which is started by “encrypted…” which show ssh uses encryption to establish the connection and data is transferred in encrypted manner.

- After analysing the packets logout from the client side and reject or close the port which you have opened to establish the connection as it a good practice and will keep your system less vulnerable to attacks.


IS2 [Running] - Oracle VM VirtualBox
IS1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 13:24
Mon 13:25
is2@IS2: ~
is1@IS1: ~
File Edit View Search Terminal Help

```
is2@IS2:~$ sudo ufw status
[sudo] password for is2:
Status: active

To                         Action      From
--                         ------      ----
23                         ALLOW       Anywhere
22                         ALLOW       Anywhere
23 (v6)                    ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)

is2@IS2:~$ sudo ufw reject 22
Rule updated
Rule updated (v6)
is2@IS2:~$ sudo ufw reject 23
Rule updated
Rule updated (v6)
is2@IS2:~$
```

```
Status: active

To                         Action      From
--                         ------      ----
23                         REJECT      Anywhere
22                         REJECT      Anywhere
23 (v6)                    REJECT      Anywhere (v6)
22 (v6)                    REJECT      Anywhere (v6)

is2@IS2:~$ exit
logout
Connection to 10.0.2.4 closed.
is1@IS1:~$ sudo ufw status
[sudo] password for is1:
Status: active

To                         Action      From
--                         ------      ----
23                         ALLOW       Anywhere
22                         ALLOW       Anywhere
23 (v6)                    ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)

is1@IS1:~$
```

```
is2@IS2:~$ sudo ufw disable
Firewall stopped and disabled on system startup
is2@IS2:~$
```

```
 reject ARGS                     add reject rule
 limit ARGS                      add limit rule
 delete RULE|NUM                 delete RULE
 insert NUM RULE                 insert RULE at NUM
 route RULE                      add route RULE
 route delete RULE|NUM           delete route RULE
 route insert NUM RULE           insert route RULE at NUM
 reload                          reload firewall
 reset                           reset firewall
 status                          show firewall status
 status numbered                 show firewall status as numbered list of RULES
 status verbose                  show verbose firewall status
 show ARG                        show firewall report
 version                         display version information

Application profile commands:
 app list                        list application profiles
 app info PROFILE                show information on PROFILE
 app update PROFILE              update PROFILE
 app default ARG                 set default application policy

is1@IS1:~$ sudo ufw disable
Firewall stopped and disabled on system startup
is1@IS1:~$
```

So, we can say that telnet is not secure way of establishing TCP connection or to access a server as it is not encrypted and vulnerable to get hijacked or attacked as the hacker can easily analyse the packet and snoop the data and can cause harm to you so in place of it use SSH connection as it is encrypted way of connection and data is encrypted while transferring data.