9. Analysing network packet stream using tcpdump and wireshark. Perform basic network service tests using nc.

Installing tcpdump and analysing network packet stream

Procedure:

Step 1: Update the system

sudo apt-get update

Step 2: Install tcpdump on the system

sudo apt-get install tcpdump

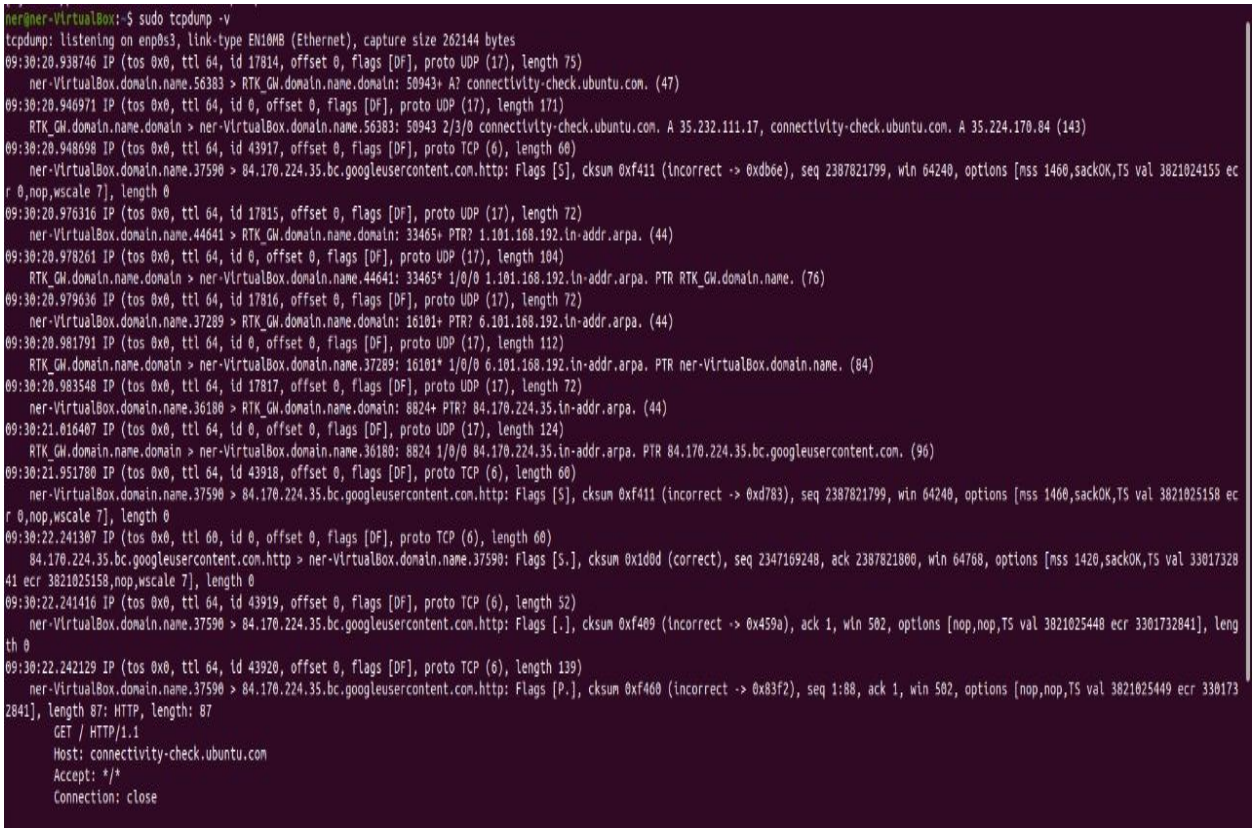
Step 3: Check the version

tcpdump --version

To capture packets from a source ip.

tcpdump –n src host ip-address

OUTPUT



Installing wireshark and analysing network packet stream

Wireshark is a free and open-source network protocol analyser widely used around the globe. With Wireshark, you can capture incoming and outgoing packets of a network in real-time and use it for network troubleshooting, packet analysis, software and communication protocol development, and many more.

Procedure:

Step 1: Update the system

sudo apt-get update

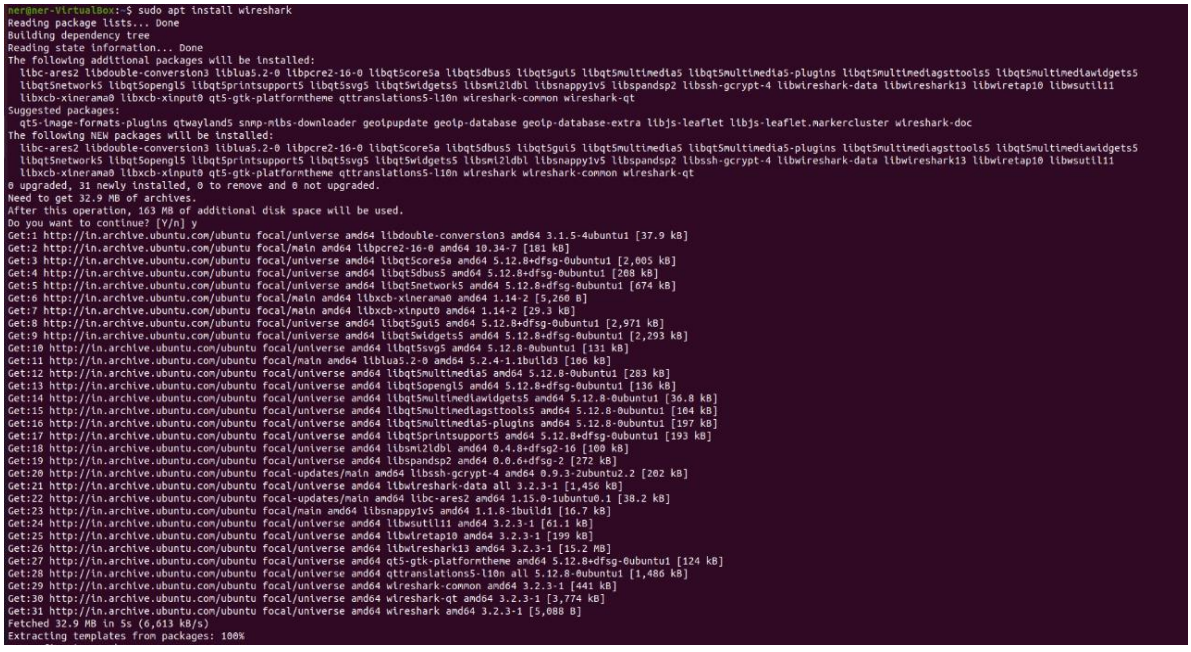
Step 2: Install wireshark on the system

sudo apt-get install wireshark

Step 3: Check the version

wireshark –version

OUTPUT



To capture network packet streams type,

wireshark

then copy the ip address