Lab Activity - 11

-Networking & System Administration Lab

Submitted by,

Anjali C Abraham

Roll No : 18

S2 RMCA A

Submitted on :05-10-2021

# Analyzing network packet stream using nc and wireshark

- **sudo apt-get install wireshark**


```
anjali@anjali-VirtualBox:~$ sudo apt-get install wireshark
[sudo] password for anjali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0
  libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libspandsp2 libssh-gcrypt-4 libwireshark-data
  libwireshark14 libwiretap11 libwsutil12 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0
  libminizip1 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libqt5network5 libqt5printsupport5 libqt5svg5
  libqt5widgets5 libsmi2ldbl libspandsp2 libssh-gcrypt-4 libwireshark-data
  libwireshark14 libwiretap11 libwsutil12 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
  wireshark-qt
0 upgraded, 32 newly installed, 0 to remove and 247 not upgraded.
Need to get 34.0 MB of archives.
After this operation, 170 MB of additional disk space will be used.
```


Package configuration

┤ **Configuring wireshark-common** ├

Dumpcap can be installed in a way that allows members of the "wireshark" system group to capture packets. This is recommended over the alternative of running Wireshark/Tshark directly as root, because less of the code will run with elevated privileges.

For more detailed information please see /usr/share/doc/wireshark-common/README.Debian.gz once the package is installed.

Enabling this feature may be a security risk, so it is disabled by default. If in doubt, it is suggested to leave it disabled.

Should non-superusers be able to capture packets?

<Yes>   <No>

- **sudo dpkg-reconfigure wireshark-common**

```
anjali@anjali-VirtualBox:~$ sudo dpkg-reconfigure wireshark-common
```
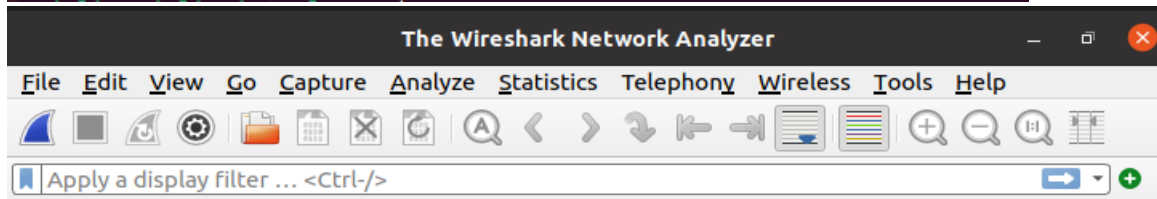

- **sudo adduser $USER wireshark**
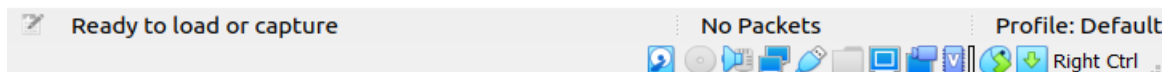
```
anjali@anjali-VirtualBox:~$ sudo adduser $USER wireshark
Adding user `anjali' to group `wireshark' ...
Adding user anjali to group wireshark
Done.
```

- **nc -z -c 10.0.2.255 20-80**

```
anjali@anjali-VirtualBox:~$ nc -z -v 10.0.2.255 20-80
nc: connect to 10.0.2.255 port 20 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 21 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 22 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 23 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 24 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 25 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 26 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 27 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 28 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 29 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 30 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 31 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 32 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 33 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 34 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 35 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 36 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 37 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 38 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 39 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 40 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 41 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 42 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 43 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 44 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 45 (tcp) failed: Network is unreachable
nc: connect to 10.0.2.255 port 46 (tcp) failed: Network is unreachable
```