

# **Analyzing network packet stream using nc and wireshark**

**NIMISHA JAMES**

**RMCA-B S2**

**ROLL NO:11**

## Step1:

- **sudo apt-get install wireshark**

```
(root@kali)-[~]
# apt-get install wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (3.4.8-1).
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical liblua5.1-2 liblua5.1-common python3-qrcode
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 805 not upgraded.

(root@kali)-[~]
# dpkg-reconfigure wireshark-common

(root@kali)-[~]
#
```

## Step2:

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

```
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>
```

### Step3.

open wireshark from the applist

