# PRACTICAL 5

**AIM:** TCP/UDP connectivity using NETCAT.

**Software used: -** Ubuntu, Terminal, NETCAT

**Theory: -**

NETCAT performs a narrow function with a broad application to hacking and network debugging: it reads and writes data for TCP and UDP connections. NETCAT interacts directly with a TCP or UDP service. NTCAT provides the network connection and you provide the protocol. Its greatest utility comes from piping the input and output of other commands over the network. The Netcat commands on modern OS's have been rewritten and updated from the original version written by a hacker named Hobbit1995.

TELNET is important compile-time options in NETCAT. TELNET Enable this option to give Netcat better interaction with a telnet client. The telnet protocol exchanges several options between the client and the server when a connection is established. Without this option enabled, you won't be able to interact with a telnet service very well.

**NETCAT command options: -**

The basic command line for Netcat is nc [options] host ports, where host is the hostname or IP address to connect to and ports is either a single port, a port range (specified "mon"), or individual ports separated by spaces, depending on the desired behavior.

These are the most useful of the command-line options:

**-l** Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host. It is an error to use this option in conjunctionwith the -p, -s, or- options. Additionally, any timeouts specified with the Woption are ignored.

**-n** Do not do any DNS or service lookups on any specified addresses, hostnames orports.

**-v** Controls how much Netcat tells you about what it's doing. Without-v, Netcatonly reports the data it receives. A single -V will let you know what address it'sconnecting or binding to and if any problems occur. For the original Netcat, addingsecond v option to the command line lets you know how much data was sent andreceived at the end of the connection.

**-z** Specifies that nc should just scan for listening daemons, without sending any data to them. It is an error to use this option in conjunction with the –l option

**Command lines: -**

**Message transfer using NETCAT:**

Sender: - nc -1 4446

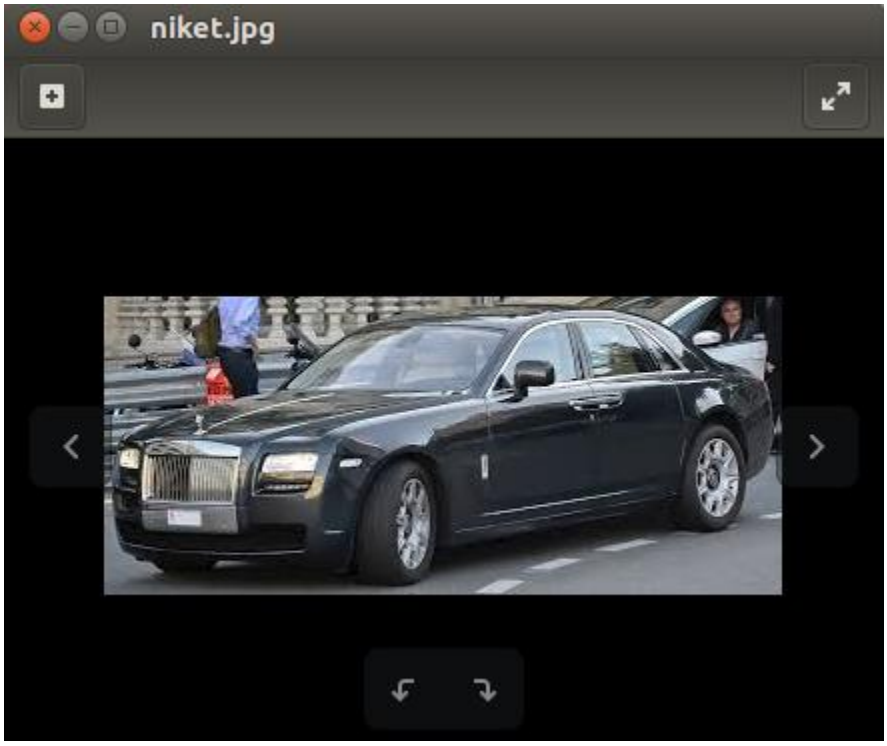
Receiver: - nc 172.16.5.58 4446


**File transfer using NETCAT:**

Sender: - nc–l -v 4445 < niket.jpg

Receiver: **-** nc -v 172.16.5.58 4445 > niket.jpg

```
administrator@ubuntu:~$ nc -v 172.16.5.13 4445 > niket.jpg
Connection to 172.16.5.13 4445 port [tcp/*] succeeded!
administrator@ubuntu:~$
```




Conclusion: -

Hence using NETCAT we can establish connection between two or more hosts and we have learnt about TCP/UDP connectivity.