Practical: - 3

3. TCP / UDP connectivity using Netcat

What is Netcat?

Netcat is a featured networking utility which reads and writes data across network connections, using the TCP/IP protocol. Designed to be a reliable "back-end" tool, Netcat can be used directly with other programs and scripts to send files from a client to a server and back. At the same time, it is a feature-rich network debugging and exploration tool that can specify the network patameters while also establishing a connection to a remote host via a tunnel.

Syntax

nc [-options] hostname port[s] [ports]
nc -l -p port [-options] [hostname] [port]

Basic Parameters

- -1: Listen mode (default is client mode)
- -L: Listen harder (supported only on Windows version of Netcat). This option makes Netcat a persistent listener which starts listening again after a client disconnects
- -u: UDP mode (default is TCP)
- -p: Local port (In listen mode, this is port listened on. In client mode, this is source port for all packets sent)
- -e: Program to execute after connection occurs, connecting STDIN and STDOUT to the program
- -n: Don't perform DNS lookups on names of machines on the other side
- -z: Zero-I/O mode (Don't send any data, just emit a packet without payload)
- -wN: Timeout for connects, waits for N seconds after closure of STDIN. A Netcat client or listener with this option will wait for N seconds to make a connection. If the connection doesn't happen in that time, Netcat stops running.
- -v: Be verbose, printing out messages on Standard Error, such as when a connection occurs
- -vv: Be very verbose, printing even more details on Standard Error

Name: - 1. Bhalsod Aditya M. Enrollment No.:- 1. 175690693001

2. Sachin Parmar 2. 185693693016

Group No.: -6

Test your Netcat understanding as a client-server

Open two computer terminals, the first will act as the server and the second will be the client.

TCP client

With **Netcat** your PC can be converted in a server, you want to begin as a server that listens at port **4444**:

```
C:\WINDOWS\system32\cmd.exe-nc

Microsoft Windows [Version 10.0.17763.379]

(c) 2018 Microsoft Corporation. All rights reserved. hello.txt cammmd....

player

C:\Users\Aditya\cdot desktop

C:\Users\Aditya\Desktop\cd Aditya

C:\Users\Aditya\Desktop\Aditya\nc

Cmd line: -L -vv -p 4444

listening on [any] 4444 ...

connect to [169.254.132.62] from DESKTOP-RJS2DJ6 [169.254.18.105] 62963

hello

hiii panth Nox

vgm
```

In addition, we can use the server to connect to the port (4444) recently opened, from the client side:

```
Microsoft Windows [Version 10.0.16299.431]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Dell>cd desktop

C:\Users\Dell\Desktop>nc
Cmd line: 169.254.132.62 4444
hello
hiii parth
vgm
^C
C:\Users\Dell\Desktop>nc
Cmd line: -L -vv -p 4444
listening on [any] 4444 ...
connect to [169.254.18.105] from ADITYA [169.254.132.62] 63664
good moring parth
Very Good Morning Aditya
```

Name: - 1. Bhalsod Aditya M. Enrollment No.:- 1. 175690693001 2. Sachin Parmar 2. 185693693016

Group No.: - 6

File Transfer Using Netcat

Push a file from client to listener:

nc-l-p [LocalPort] > [outfile]

Listen on [LocalPort], Store results in [outfile]

\$ nc -w2 [TargetIpAddr] [port] < [infile]

Push [infile] to [TargeIPAddr] on [port]

Pull file form listener back to client

\$ nc -w3 [TargetIPaddr] [port] > [outfile]

Connect to [TargetIPaddr] on [port] and retrieve [outfile]

```
C:\WINDOWS\system32\cmd.exe-nc -v-w 30-p 4444-l

C:\Users\Dell\Desktop>nc -v -w 30 -p 4444 -l < demo.txt
listening on [any] 4444 ...

connect to [169.254.18.105] from ADITYA [169.254.132.62] 63668

hello
file already send
```

Name: - 1. Bhalsod Aditya M. Enrollment No.:- 1. 175690693001 2. Sachin Parmar 2. 185693693016

Success No. . C

Group No.: - 6