

Forum:[Hack Forums](#)

Thread: [Netcat Cheat Sheet](#)

Clumsy - October 9, 2024, 3:54 pm

Code Netcat cheatsheet

Netcat listening on port 567/TCP:

```
$ nc -l 567
```

Connecting to that port from another machine:

```
$ nc 1.2.3.4 5676
```

To pipe a text file to the listener:

```
$ cat infile | nc 1.2.3.4 567 -q 10
```

To have the listener save a received text file:

```
$ nc -l -p 567 > textfile
```

To transfer a directory, first at the receiving end set up:

```
$ nc -l -p 678 | tar xvpz
```

Then send the directory:

```
$ tar zcfp - /path/to/directory | nc -w 3 1.2.3.4 678
```

To send a message to your syslog server (the <0> means emerg):

```
$ echo '<0>message' | nc -w 1 -u sysloger 514
```

Setting up a remote shell listener:

```
$ nc -v -e '/bin/bash' -l -p 1234 -t
```

or

```
$ nc -l -p 1234 -e "c:\windows\system32\cmd.exe"
```

Then telnet to port 1234 from elsewhere to get the shell.

Using netcat to make an HTTP request:

```
$ echo -e "GET http://www.google.com HTTP/1.0\n\n" | nc -w 5 www.google.com 80
```

Making a one-page webserver; this will feed homepage.txt to all comers:

```
$ cat homepage.txt | nc -v -l -p 80
```

Create an tty for made an text communication by tty share:

```
$ cat /dev/tty | nc LISTENER_IP 4444
```

```
$ nc -v -l -p 4444
```