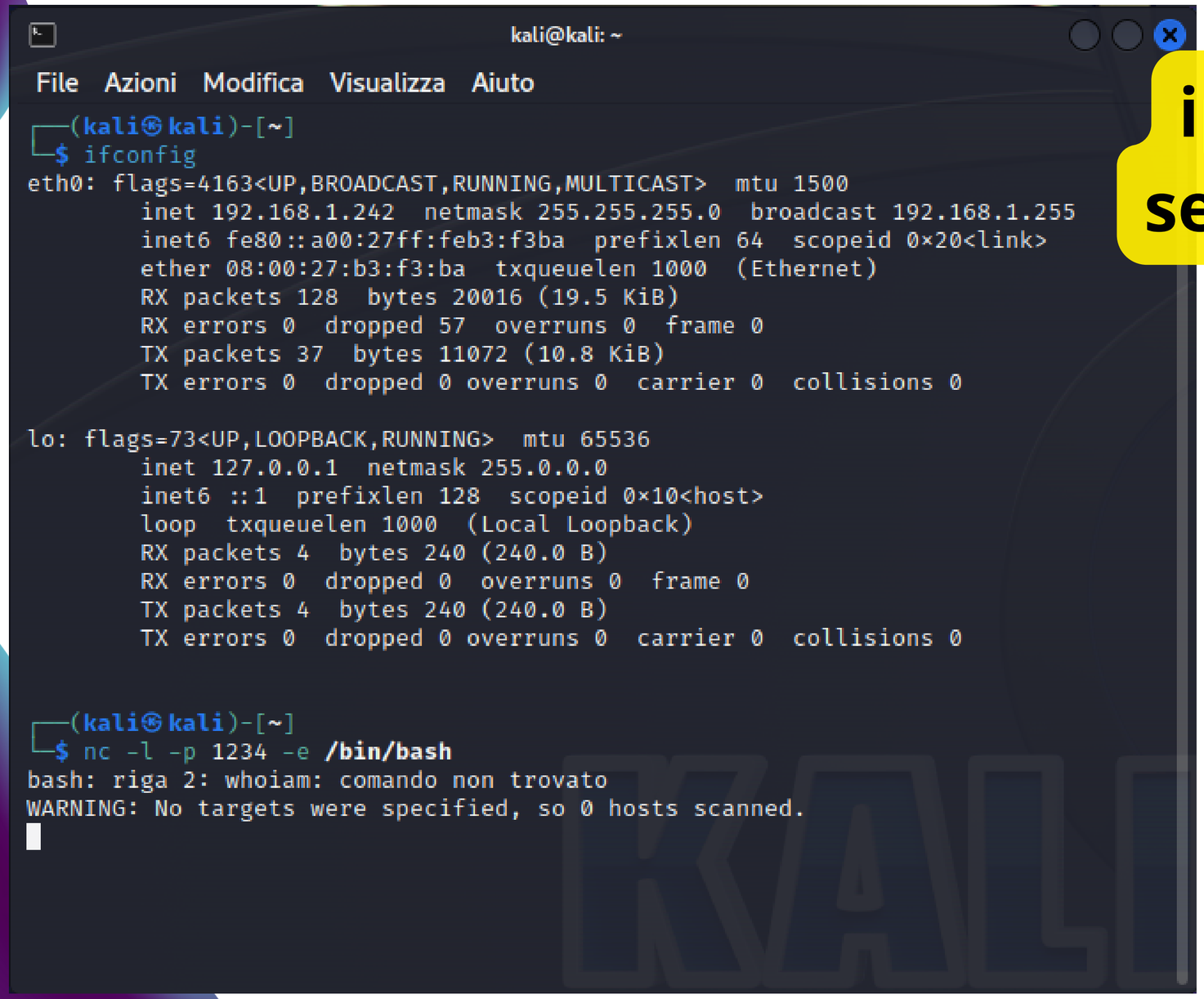
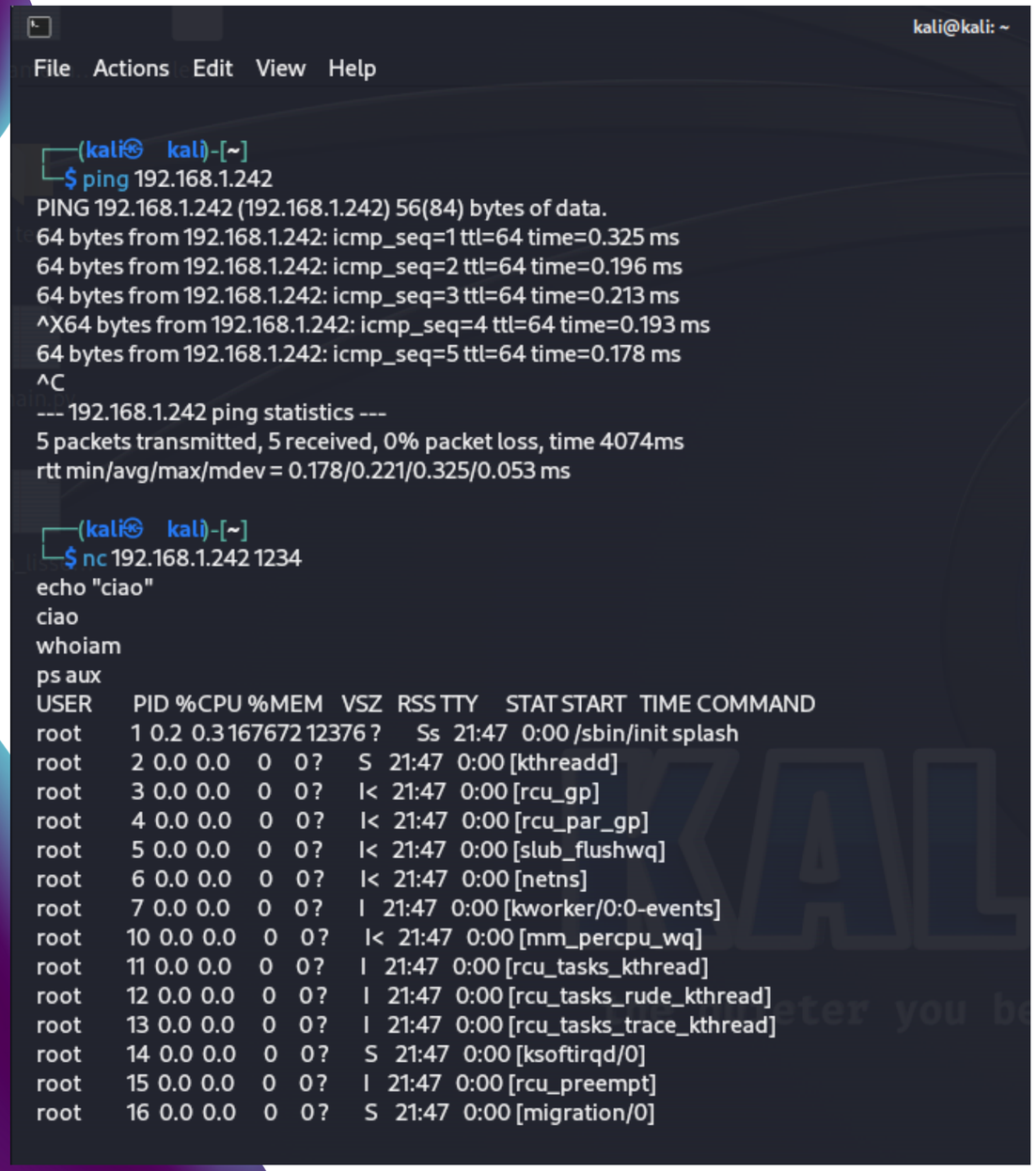
# ESERCITAZIONE n°W9D1 - Pratica (1)

esercitazione di discovering
usando netcat da kali a kali



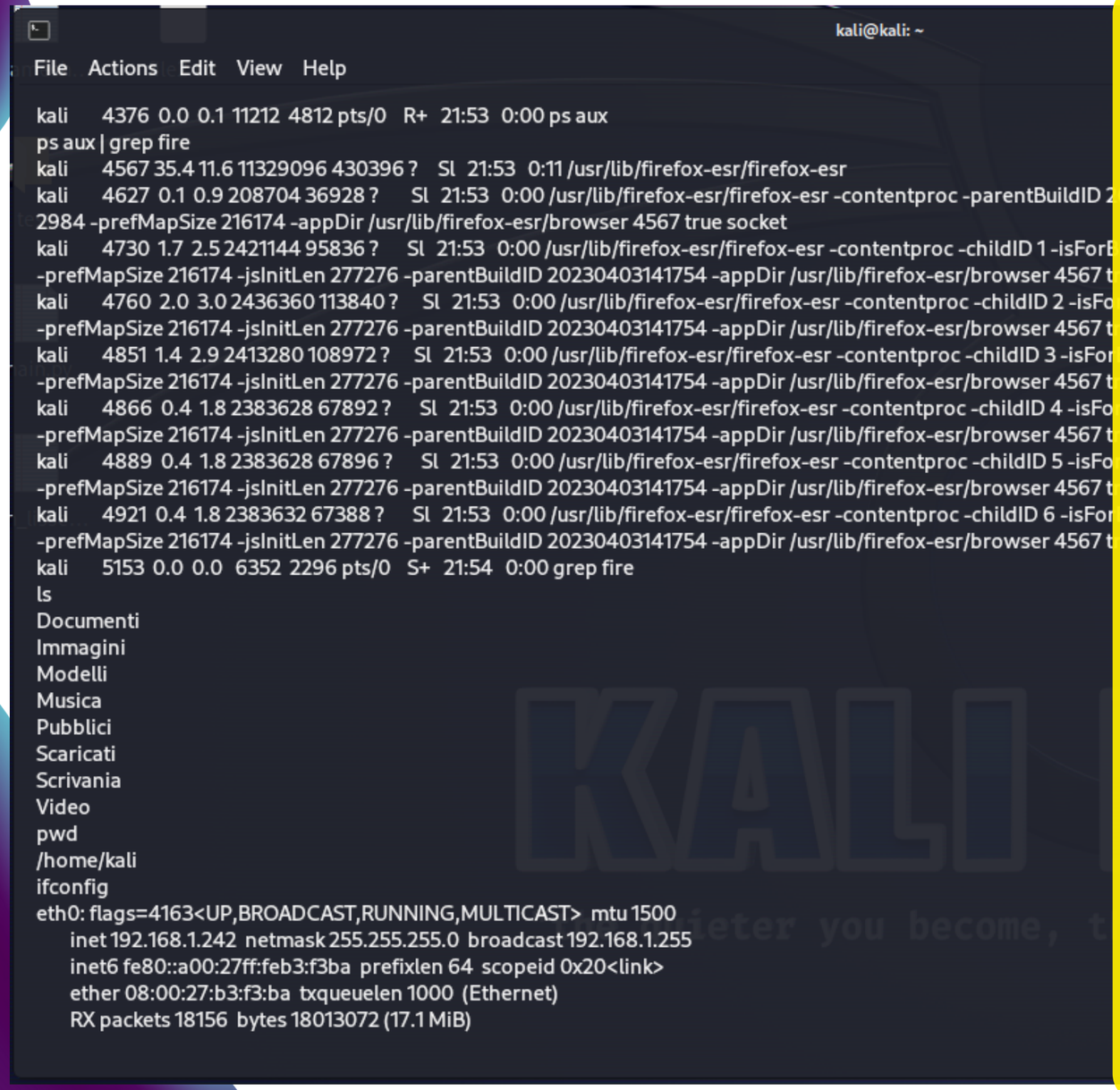

**ip kali: 192.168.1.242**
**server su cui lanciamo il listen**




**ip kali: 192.168.1.67**
**client da cui ci colleghiamo alla shel lanciata sul server.**
**esecuzione del comando ps aux in modo da visualizzare tuti i processi avviati da ogni utente sulla macchina**

```
ls -la
totale 180
drwx------ 16 kali kali  4096  5 gen 21.53 .
drwxr-xr-x  3 root root  4096 19 dic 21.39 ..
-rw-r--r--  1 kali kali   220 19 dic 21.39 .bash_logout
-rw-r--r--  1 kali kali  5551 19 dic 21.39 .bashrc
-rw-r--r--  1 kali kali  3526 19 dic 21.39 .bashrc.original
drwxr-xr-x  8 kali kali  4096  5 gen 21.53 .cache
drwxr-xr-x 12 kali kali  4096 20 dic 19.29 .config
-rw-r--r--  1 kali kali    35 19 dic 21.43 .dmrc
drwxr-xr-x  2 kali kali  4096 19 dic 21.43 Documenti
-rw-r--r--  1 kali kali 11759 19 dic 21.39 .face
lrwxrwxrwx  1 kali kali     5 19 dic 21.39 .face.icon -> .face
drwx------  3 kali kali  4096 19 dic 21.43 .gnupg
-rw-------  1 kali kali     0 19 dic 21.43 .ICEauthority
drwxr-xr-x  2 kali kali  4096 19 dic 21.43 Immagini
drwxr-xr-x  3 kali kali  4096 19 dic 21.39 .java
drwxr-xr-x  4 kali kali  4096 19 dic 21.43 .local
drwxr-xr-x  2 kali kali  4096 19 dic 21.43 Modelli
drwx------  4 kali kali  4096  5 gen 21.53 .mozilla
drwxr-xr-x  2 kali kali  4096 19 dic 21.43 Musica
-rw-r--r--  1 kali kali   807 19 dic 21.39 .profile
drwxr-xr-x  2 kali kali  4096 19 dic 21.43 Pubblici
drwxr-xr-x  2 kali kali  4096 19 dic 21.43 Scaricati
drwxr-xr-x  2 kali kali  4096 19 dic 21.43 Scrivania
-rw-r-----  1 kali kali     4  5 gen 21.47 .vboxclient-clipboard-tty7-control.pid
-rw-r-----  1 kali kali     4  5 gen 21.47 .vboxclient-clipboard-tty7-service.pid
-rw-r-----  1 kali kali     5  5 gen 21.47 .vboxclient-display-svga-x11-tty7-control.pid
-rw-r-----  1 kali kali     5  5 gen 21.47 .vboxclient-display-svga-x11-tty7-service.pid
```

**col comando ls -la visualizziamo tutti i file e i relativi permessi**




usando “ps aux |grep fire” filtriamo i risultati cercando solo processi che contengono il nome fire

usando “ls” abbiamo una lista dei file nella posizione attuale

mentre “pwd” ci dice in che posizione siamo

“ifconfig” invece ci da le configurazioni di rete attualmente configurate sulla macchina