EXPLOIT JAVA-RMI

REPORTED BY

BENEDETTA FORESTIERI

INTRODUCTION

L'obiettivo del progetto è sfruttare una vulnerabilità relativa ad un servizio sulla porta 1099, specificamente Java RMI, utilizzando Metasploit. Il fine ultimo è ottenere una sessione di Meterpreter sulla macchina remota.

Java RMI, abbreviazione di Remote Method Invocation, consente a processi Java di interagire tra loro attraverso una rete.

La presenza della vulnerabilità è causata da una configurazione di default non corretta, la quale consente a un possibile attaccante di inserire del codice arbitrario.

Se la vulnerabilità viene sfruttata con successo**, l'attaccante può ottenere accesso amministrativo completo alla macchina di destinazione**, eseguire codice dannoso, raccogliere informazioni sensibili o interrompere i servizi sulla macchina remota.

Il primo passo consiste nell'eseguire una scansione con nmap al fine di ottenere informazioni dettagliate sui servizi in esecuzione su Metasploitale.

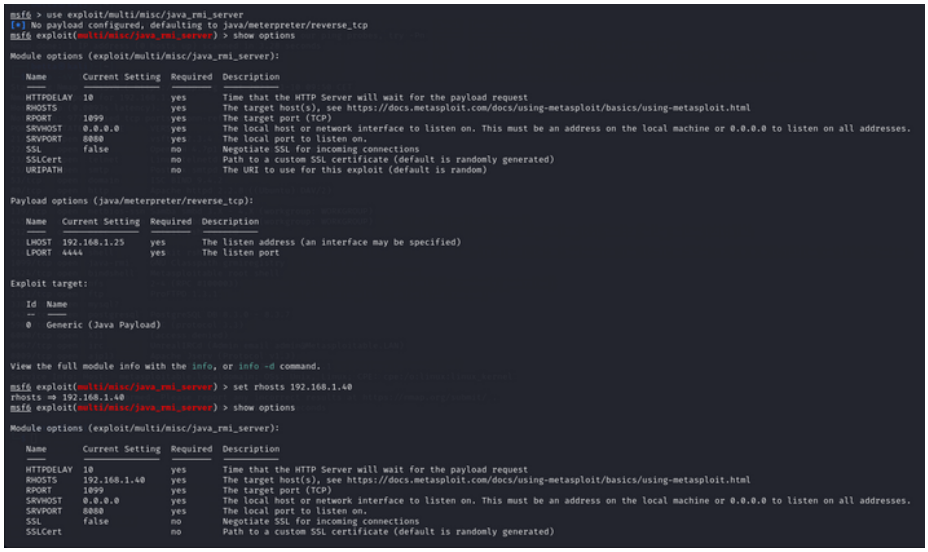
```
┌──(betta㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-10 09:50 CET
Nmap scan report for 192.168.1.40
Host is up (0.0093s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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?
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?
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 (Admin email admin@Metasploitable.LAN)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host:  metasploitable.localdomain; 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 187.26 seconds
```

PRELIMINARY PHASE

Avviando Metasploit su Kali, ho cercato gli exploit e ne sono emersi 4. Quello più interessante è il primo, con la descrizione "default configuration code execution", indicando la possibilità di sfruttare una configurazione predefinita per eseguire codice.

Eseguito il comando per la scelta dell'exploit, Metasploit assegna automaticamente il "payload" (codice eseguibile inviato alla macchina bersaglio dopo lo sfruttamento di una vulnerabilità). Il payload **java/meterpreter/reverse_tcp**, progettato per Java, permette a Metasploit di stabilire una connessione inversa sulla macchina bersaglio, creando una sessione Meterpreter per l'interazione con il sistema remoto.

In seguito, verifico le opzioni disponibili tramite il comando "show options" e procedo a configurare il parametro RHOSTS inserendo l'indirizzo IP della macchina vittima. Mi assicuro che nell'opzione LHOST sia presente l'indirizzo della macchina attaccante.

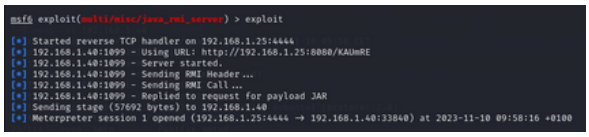


EXPLOIT

Un **attacco exploit** è un'azione mirata che sfrutta vulnerabilità nei sistemi per ottenere accesso non autorizzato o compromettere la sicurezza del sistema.

Successivamente alla definizione di tutte le configurazioni e parametri, possiamo avviare l'attacco.

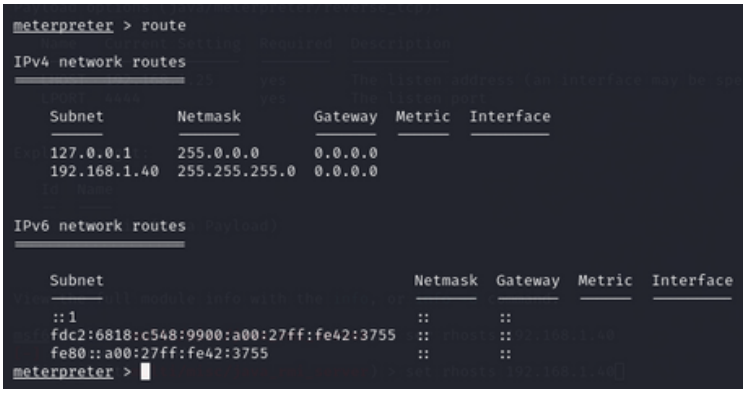
L'attacco è stato eseguito con successo ed ho ottenuto una shell di Meterpreter.



Dopo aver acquisito una sessione remota Meterpreter, conduco due test:

1) analisi della configurazione di rete;
2) ottenimento di informazioni sulla tabella di routing della macchina vittima.

L'utilizzo del comando "ifconfig" rivela la **configurazione di rete** della macchina, confermando la presenza dell'indirizzo IP 192.168.1.40 (Metasploitable). Questa evidenza è sufficiente per concludere che l'attacco sia riuscito con successo e che la vulnerabilità "Java_RMI code execution" sia stata sfruttata correttamente, garantendo l'accesso alla macchina bersaglio.



Mediante l'esecuzione del comando "route", posso esplorare le **impostazioni di routing della macchina bersaglio,** rilevando gli indirizzi IP.