BENCHMARK MODULO 4

Java RMI exploit privilege escalation

Ottenimento di una sessione Meterpreter con privilegi root in una macchina metasploitable2.

Procedura

Cambio degli Indirizzi IP di Kali Linux e Metasploitable 2
Configurazione di Metasploitable 2: Per cambiare l'indirizzo IP di Kali Linux, ho modificato il file di configurazione dell'interfaccia di rete usando il seguente comando:
sudo nano /etc/network/interfaces
Ho modificato l'indirizzo IP dell'interfaccia di rete desiderata per corrispondere all'indirizzo IP richiesto (192.168.11.112)

Sfruttamento della Vulnerabilità Java RMI con Metasploit

Si inizia con una scansione nmap per individuare contro che target abbiamo a che fare e quali servizi sono attivi e con quale versione (e su quale porta sono eventualmente attivi)
Nmap -sV -p 1-1200 192.168.11.112

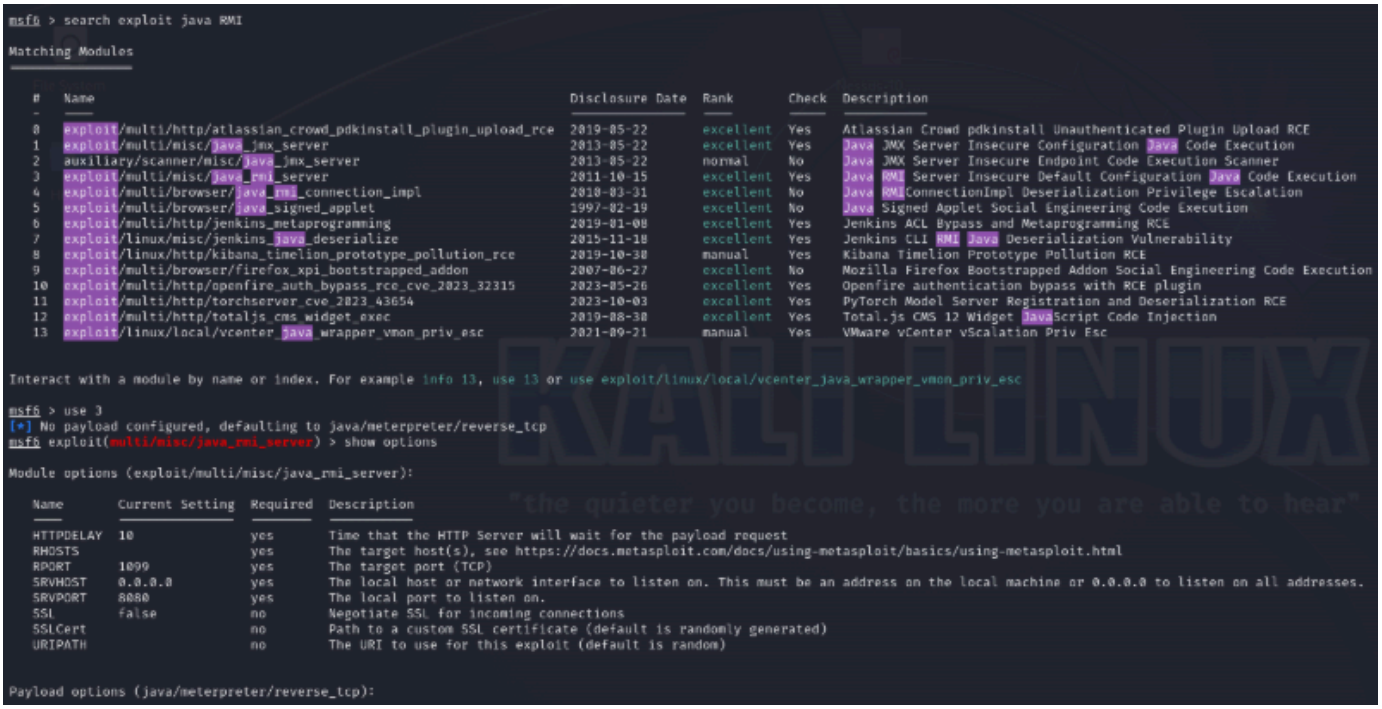
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 1-1200 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 08:57 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.11.112
Host is up (0.00014s latency).
Not shown: 1187 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
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 24.30 seconds
```

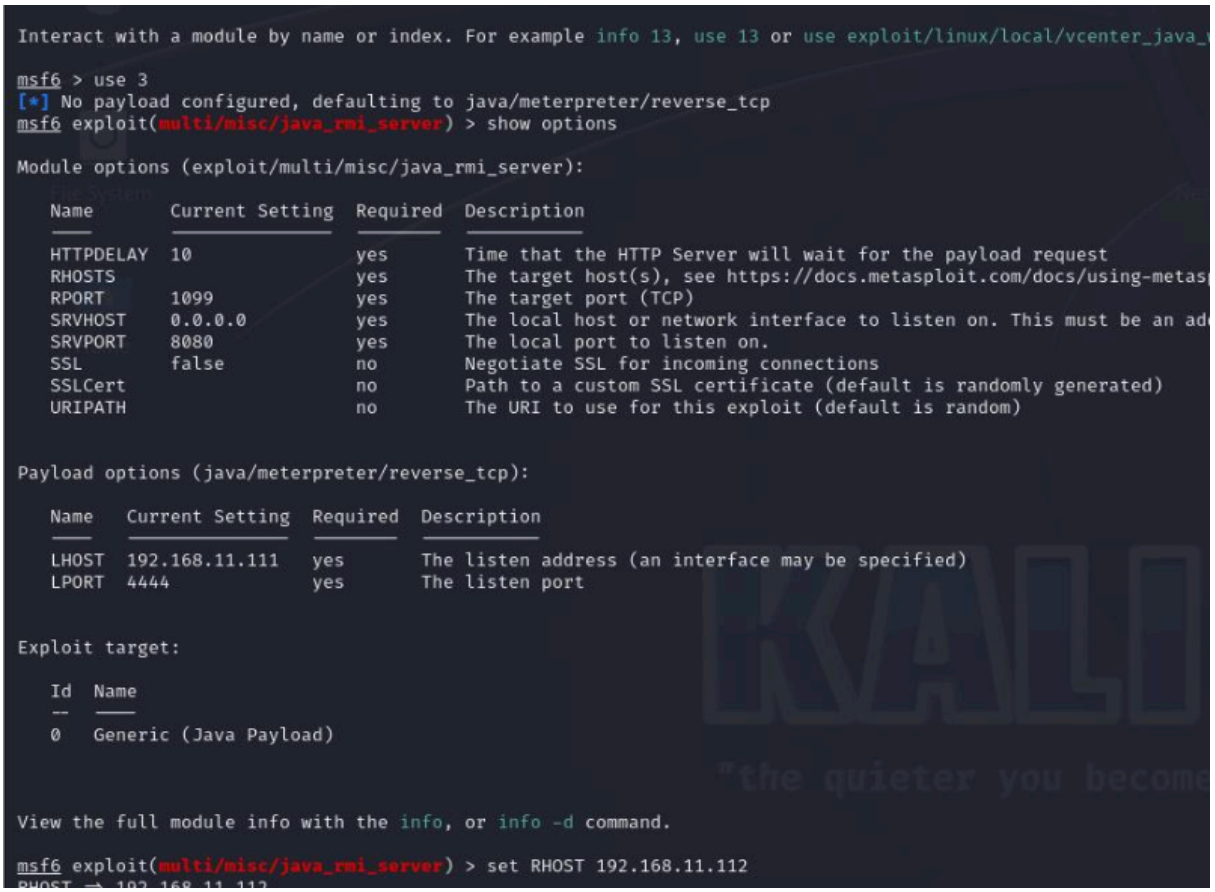
La scansione rivela che la porta 1099 accetta connessioni e ha un servizio “Java-rmi” attivo in ascolto.
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability riguarda diversi prodotti Java che implementano il server RMI (Remote Method Invocation). Questa vulnerabilità può permettere a un attaccante remoto non autenticato di eseguire codice arbitrario su un sistema bersaglio con privilegi elevati.

Avvio di Metasploit:
Per iniziare, ho avviato Metasploit dalla mia macchina attaccante, utilizzando il comando msfconsole. Questo ha aperto l'interfaccia della console Metasploit, pronta per l'uso dopo l’inserimento della password di root.

Selezione del Modulo di Sfruttamento:
Una volta aperto Metasploit, ho utilizzato il comando search per cercare moduli di sfruttamento relativi a Java RMI. Questo comando permette di cercare all'interno del vasto database di Metasploit per trovare moduli pertinenti a una specifica vulnerabilità o servizio. Nella nostra ricerca, abbiamo individuato il modulo "exploit/multi/misc/java_rmi_server" come adatto per la vulnerabilità Java RMI sulla porta 1099.



Selezione del Modulo e Impostazione delle Opzioni:
Dopo aver individuato il modulo appropriato, ho utilizzato il comando use 3 per selezionarlo all'interno di Metasploit. Una volta selezionato, ho impostato l'indirizzo IP della macchina Metasploitable come target utilizzando il comando set RHOST. Questo passaggio è essenziale per configurare correttamente il target da colpire con il nostro exploit.

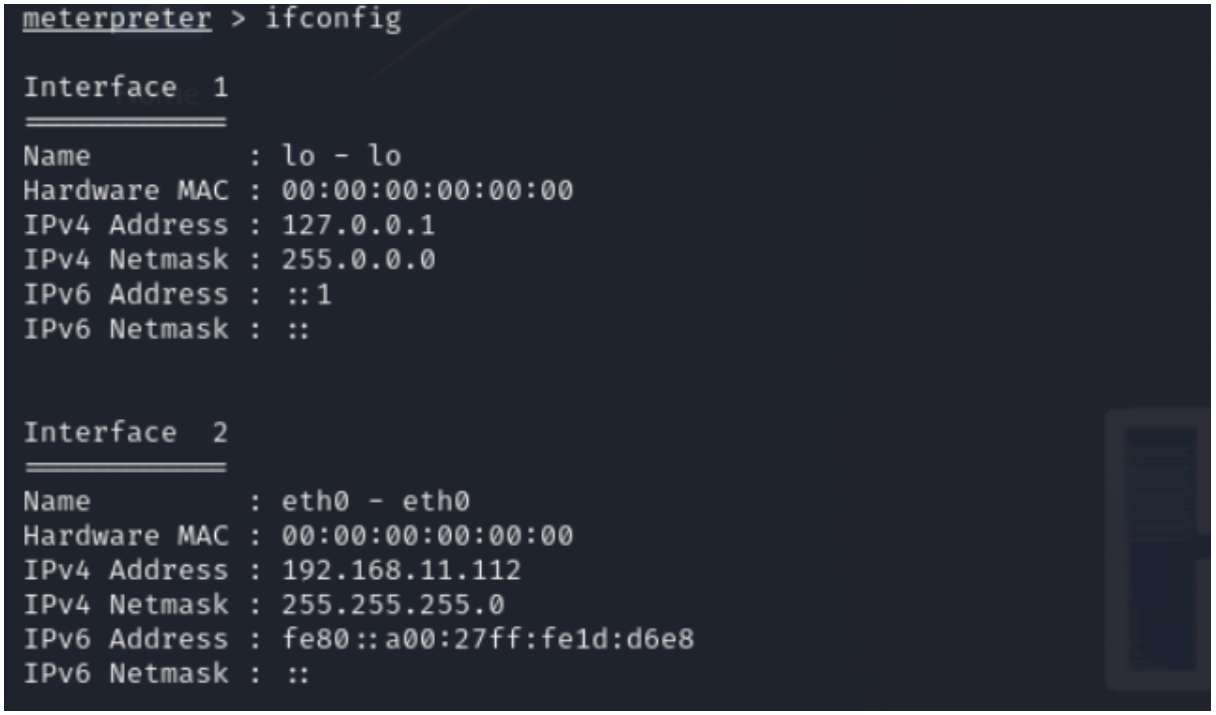


Esecuzione dell'Exploit:
Una volta configurato il modulo con l'indirizzo IP della macchina vittima, ho eseguito l'exploit utilizzando il comando exploit. Questo comando ha avviato l'azione di sfruttamento della vulnerabilità Java RMI sulla macchina Metasploitable. Metasploit ha automatizzato il processo di sfruttamento della vulnerabilità, cercando di ottenere un accesso non autorizzato alla macchina vittima.

Ottenimento della Sessione Meterpreter:
Dopo aver eseguito con successo l'exploit, Metasploit ha sfruttato la vulnerabilità Java RMI sulla macchina Metasploitable e ha ottenuto una sessione Meterpreter. Questo tipo di sessione fornisce all'attaccante un elevato livello di controllo sulla macchina remota, consentendo di eseguire una vasta gamma di comandi e azioni.

Raccolta di Evidenze dalla Macchina Remota

Configurazione di Rete:
Una volta ottenuta una sessione remota Meterpreter sulla macchina vittima, è importante raccogliere informazioni sulla configurazione di rete della macchina remota. Questo può includere dettagli come l'indirizzo IP, il gateway predefinito, il subnet mask e altri parametri di rete pertinenti. Utilizzando i comandi appropriati all'interno di Meterpreter, è possibile estrarre queste informazioni per comprendere meglio l'ambiente di rete della macchina vittima.
Tramite il comando ifconfig otterremo dettagli sulla configurazione network della macchina.



Informazioni sulla Tabella di Routing della Macchina Vittima:
Oltre alla configurazione di rete, è essenziale raccogliere informazioni sulla tabella di routing della macchina vittima. La tabella di routing contiene dettagli su come il traffico di rete viene instradato all'interno della rete della macchina vittima. Questo può essere cruciale per comprendere il percorso che il traffico di rete prende attraverso la rete, identificare eventuali gateway o rotte specifiche e valutare la topologia di rete complessiva.