Attacchi su Java RMI e PostgreSQL sulla Metasploitable

Matteo Zerbi

12/07/2024

Introduzione

Questo report descrive in dettaglio gli attacchi exploit eseguiti su una macchina Metasploitable 2. Sono stati effettuati due attacchi principali: il primo utilizzando una vulnerabilità nel servizio Java RMI, e il secondo sfruttando una vulnerabilità nel servizio PostgreSQL. Inoltre, è stata inclusa una sezione bonus con azioni di post-exploitation.

Esercizio 1: Attacco su Java RMI

Traccia e Requisiti

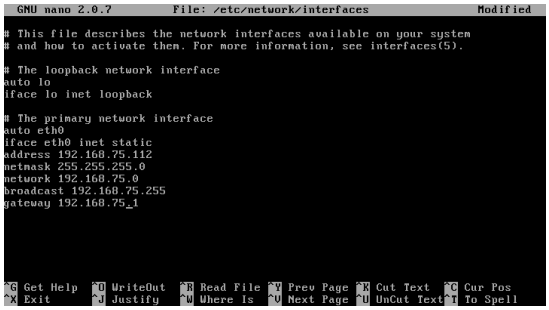
La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 - Java RMI. Si richiede di sfruttare la vulnerabilità con Metasploit per ottenere una sessione di Meterpreter sulla macchina remota.

- **Macchina attaccante (Kali)**: IP 192.168.75.111
- **Macchina vittima (Metasploitable)**: IP 192.168.75.112
- **Obiettivi**:
  - Ottenere la configurazione di rete
  - Ottenere informazioni sulla tabella di routing della macchina vittima

Passi Eseguiti

Configurazione della rete

Verifica della configurazione IP su entrambe le macchine. Ping tra le macchine per assicurarsi della raggiungibilità.



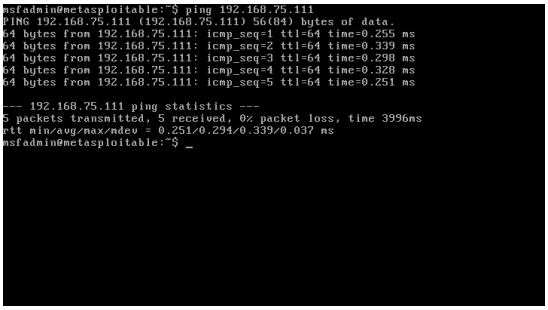


Figure 1: Configurazione Kali

Scansione delle porte

Utilizzo di `nmap` per verificare le porte aperte sulla macchina vittima e identificare la presenza del servizio Java RMI sulla porta 1099.

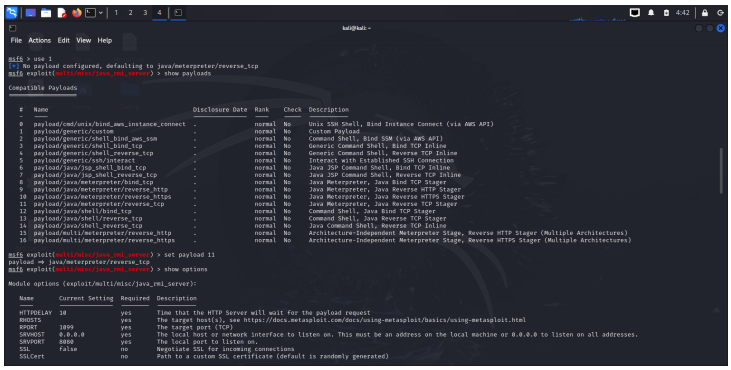
Figure 2: Scansione delle porte

Esecuzione dell'exploit

- Utilizzo di Metasploit per perfezionare l'exploit per Java RMI.

- Cercasi il giusto exploit da utilizzare e lo selezioniamo con il comando 'use'

- Cercasi payload, tramite 'show payloads' e settiarlo tramite 'set'

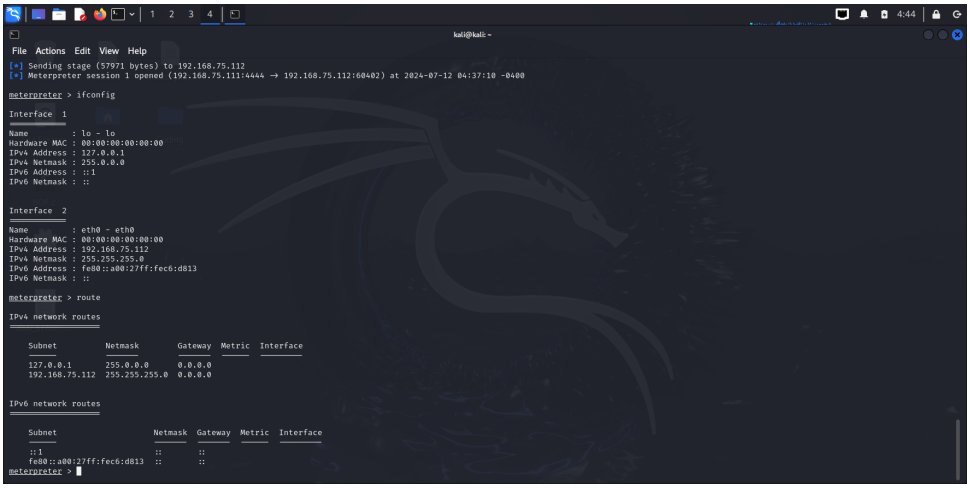


- Configuriamo gli IP della macchina vittima e della macchina attaccante

- Inviamo l'exploit.

Raccolta delle informazioni richieste

Una volta ottenuta la sessione Meterpreter, significa che l'attacco exploit e' andato a buon fine, e possiamo procedere con la raccolta della configurazione di rete e della tabella di routing della macchina vittima.



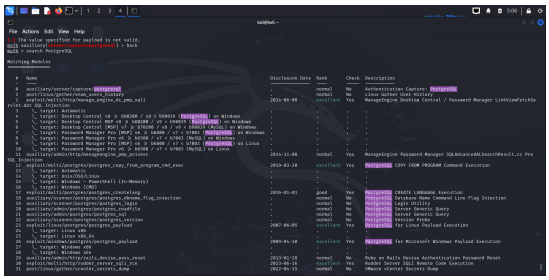
Esercizio 2: Attacco su PostgreSQL

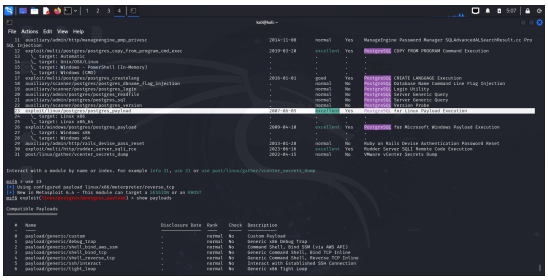
Traccia

Sfrutta la vulnerabilità nel servizio PostgreSQL di Metasploitable 2. Esegui l'exploit per ottenere una sessione Meterpreter sul sistema target.

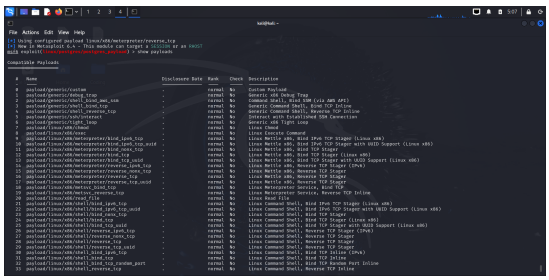
Esecuzione dell'exploit

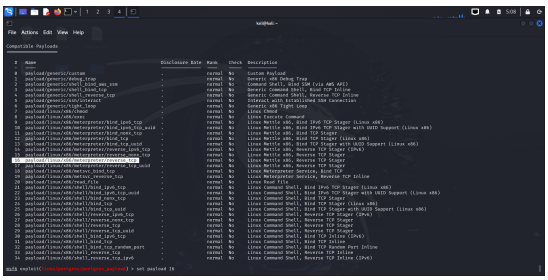
- Utilizzo di Metasploit per caricare l'exploit per PostgreSQL.





- Configurazione del payload





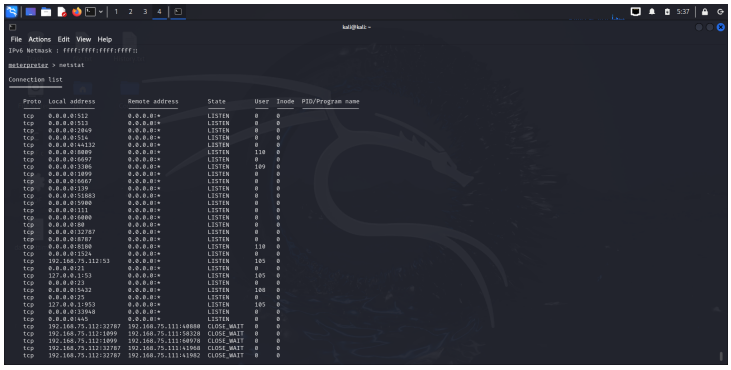
- Impostazione degli indirizzi IP

- Esecuzione dell'exploit per ottenere una sessione Meterpreter.

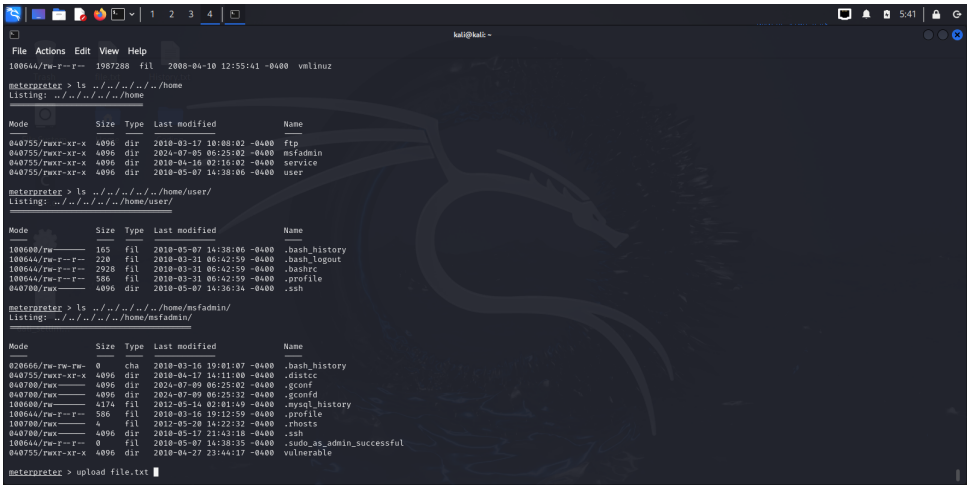
Parte Bonus: Attività Post-Exploitation

Una volta preso il possesso della macchina grazie all'exploit, possiamo fare veramente di tutto se si crea una conessione Meterpreter.
Vediamone alcune:

- Verifica delle connessioni attive con netstat



- Osservare i file presenti con ls



- Scaricare o caricare file nella macchina vittima