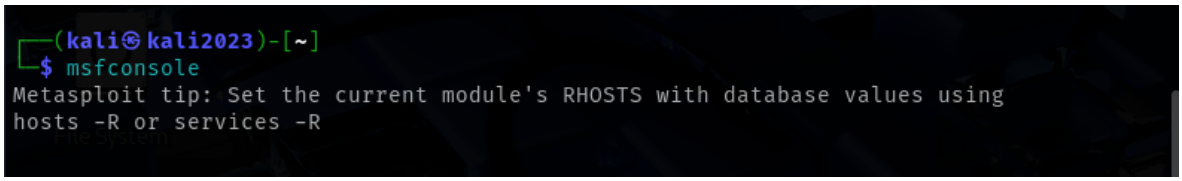
Report di Penetrazione su PostgreSQL in Metasploitable 2

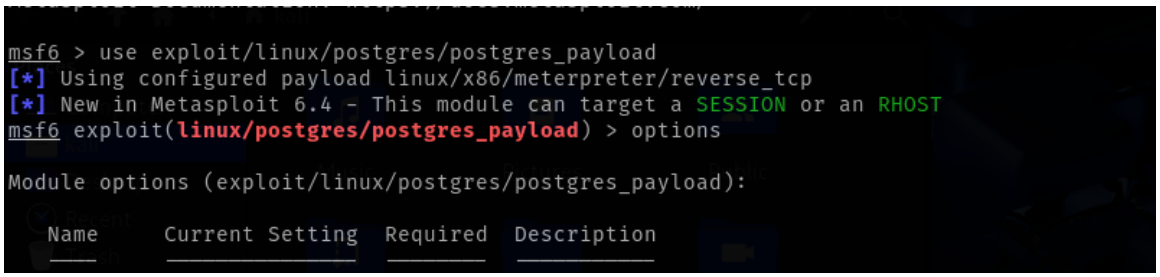
1. Introduzione
Questo report documenta lo sfruttamento di una vulnerabilità nel servizio PostgreSQL su Metasploitable 2 utilizzando il modulo `exploit/linux/postgres/postgres_payload` in Metasploit Framework (msfconsole). Successivamente, viene eseguita un'escalation di privilegi per ottenere i diritti di root sul sistema target. Infine, è stata installata una backdoor per verificare un accesso persistente al sistema compromesso.

2. Configurazione dell'Ambiente
- **Attaccante:**Kali Linux
- **Target:** Metasploitable 2
- **Modulo exploit usato:** “exploit/linux/postgres/postgres_payload”
- **Strumento:** Metasploit Framework (msfconsole)

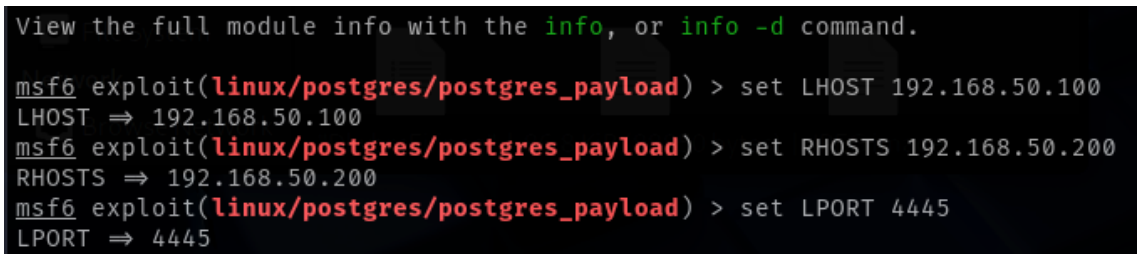
3. Sfruttamento della vulnerabilità in PostgreSQL
1. Avviare Metasploit:



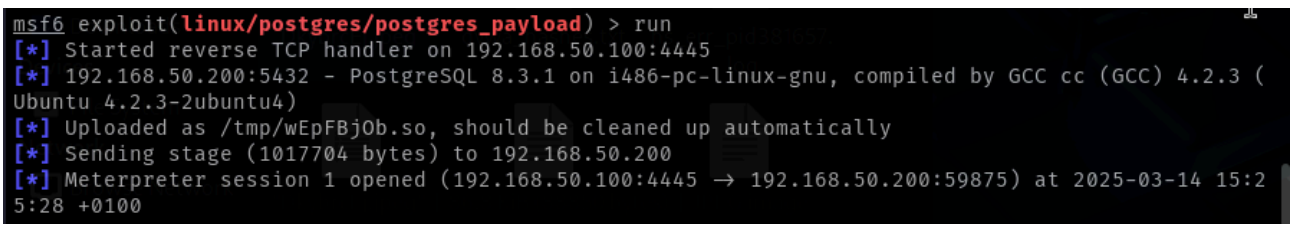
2. Selezionare il modulo di exploit:



3. Configurare i parametri necessari:



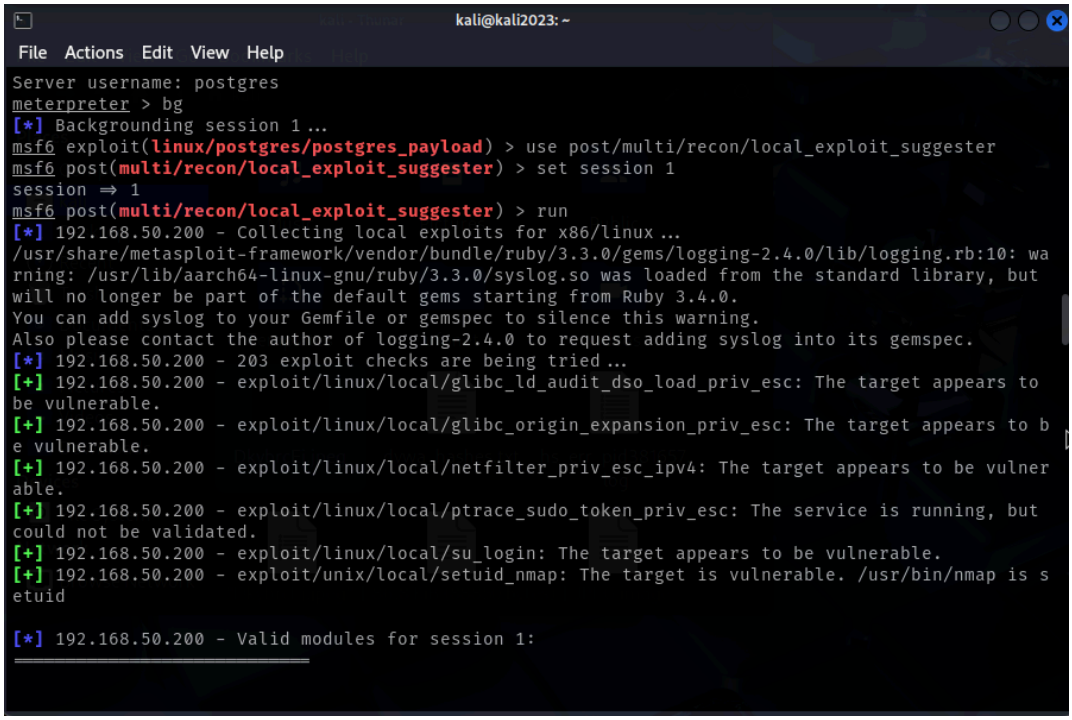
4. Eseguire l'exploit



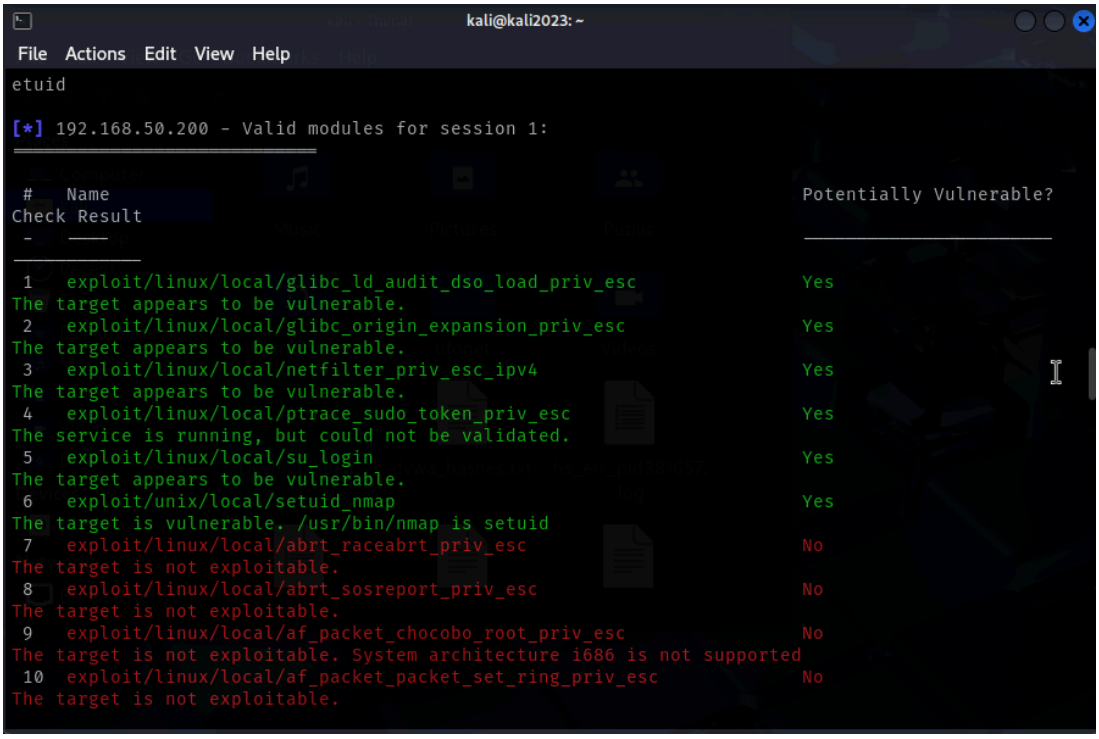
4. Verifica dell'utente attuale
Una volta ottenuta la shell Meterpreter, eseguire il comando:

```
meterpreter > getuid
Server username: postgres
```

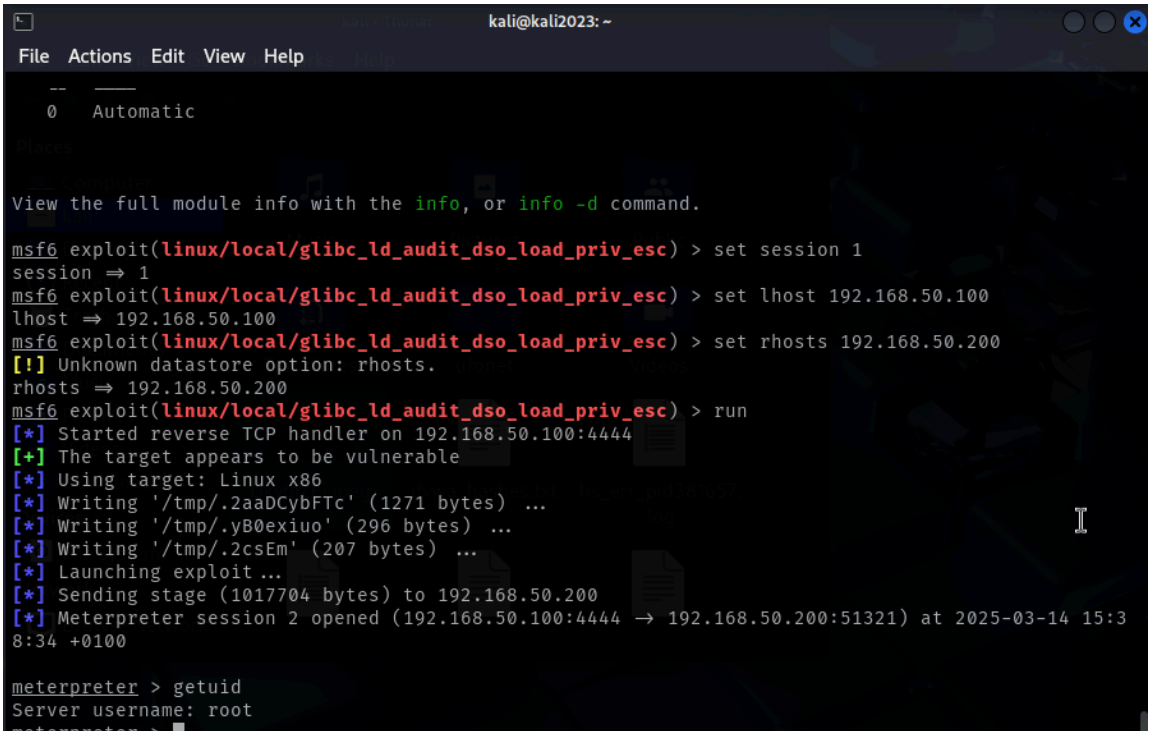
5. Escalation di privilegi
1. Utilizzare il modulo per identificare vulnerabilità locali:



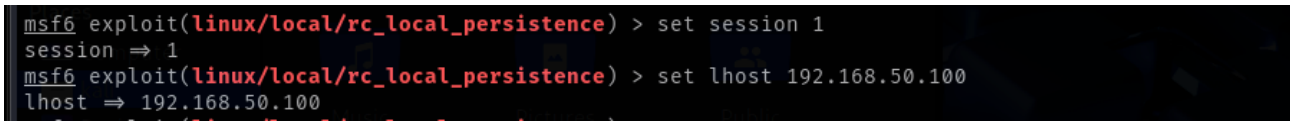
2. Identificare le vulnerabilità disponibili.



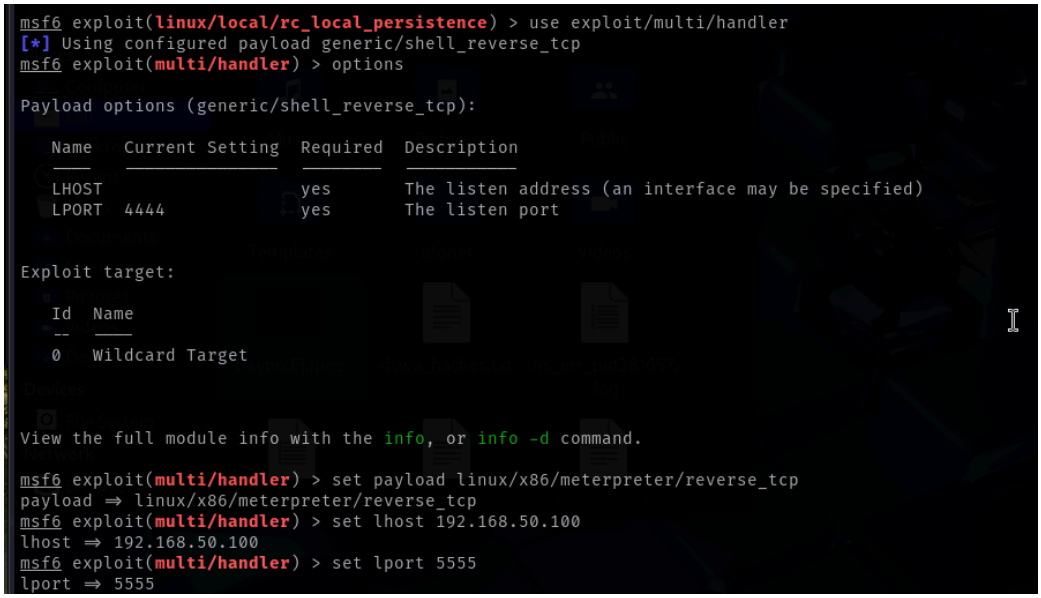
3. Verificare l'escalation di privilegi:



6. Installazione di una backdoor
1. Creare una persistenza sulla macchina target utilizzando il modulo `linux/local/rc_local_persistence`:



2. Chiudere la sessione e verificare l'accesso alla backdoor:



7. Conclusioni
In questo esercizio, abbiamo sfruttato una vulnerabilità nel servizio PostgreSQL per ottenere l'accesso al sistema target. Dopo aver ottenuto una shell Meterpreter, è stata effettuata un'escalation di privilegi per ottenere i permessi di root. Infine, è stata installata una backdoor persistente utilizzando il modulo `linux/local/rc_local_persistence` per garantire un accesso persistente al sistema compromesso.