Data:21/01/2026 Cristiano Samuel Vanvitelli

Exploit telnet con Metasploit

Introduzione

Il documento riporta un attacco contro una macchina target **Metasploitable** per testarne le vulnerabilità. Il processo si articola in tre fasi:

- Ottenimento di un accesso sfruttando il database **PostgreSQL**
- **Escalation di privilegi** per acquisire comandi di utente **root**
- **Creazione Backdoor** nel sistema target

Quest'ultima permette di accedere al sistema anche dopo il riavvio della macchina target o la chiusura della sessione.

Obiettivo

L'obiettivo è ottenere una sessione **Meterpreter** sul sistema target, eseguire un'escalation di privilegi, creare una backdoor

---

Strumenti

- **Metasploitable:** macchina target
- **Metasploit:** piattaforma di attacco

Fase 1 esecuzione modulo meterpreter

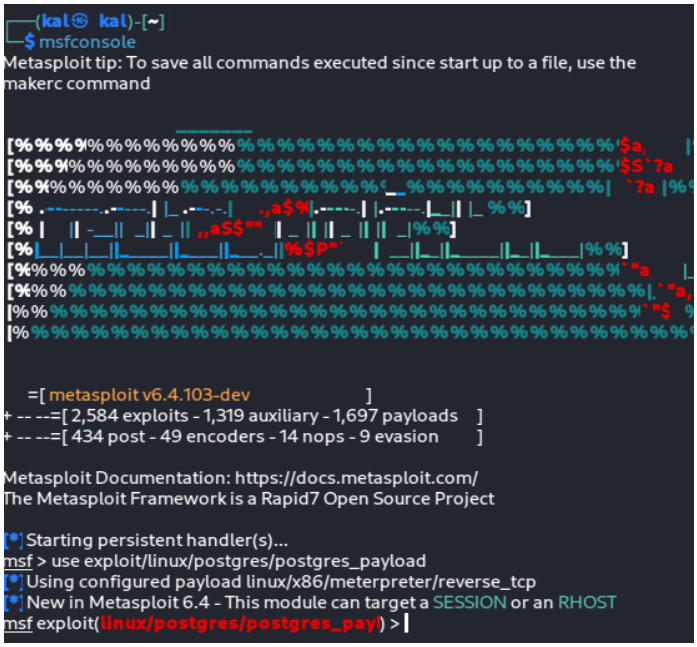

Fig.1 Accesso Metasploit e Ricerca modulo

Fig.2 Configurazione modulo

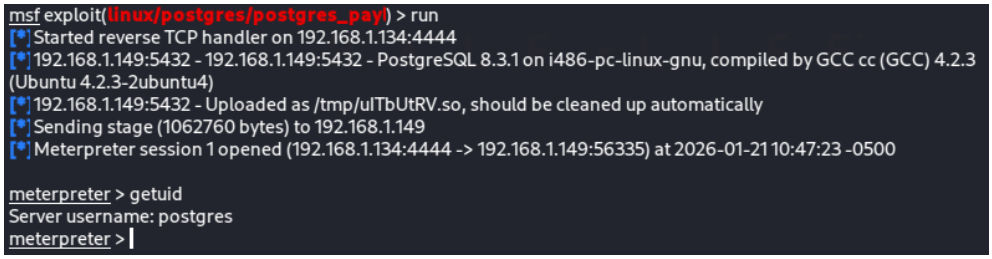

Fig.3 Esecuzione e verifica exploit

Per creare una sessione meterpreter con la macchina target,è stato utilizzato il modulo ***exploit/linux/postgres/postgres_payload*** e configurato con:

- **RHOST:** IP Metasploitable (192.168.1.149)
- **LHOST:** IP Kali (192.168.1.134)

Lanciato l'exploit, Metasploit ha avviato una sessione meterpreter con la Metasploitable ottenendo l'accesso come utente **postgres.**

Questa sessione viene inoltre messa in **background** per i prossimi step.

Fase 2 Escalation privilegi

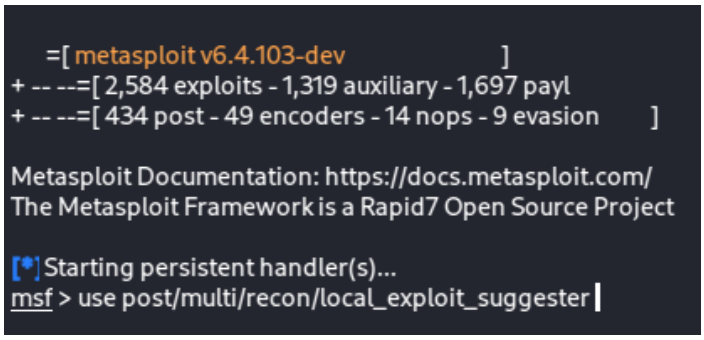

*Fig.4 Ricerca modulo

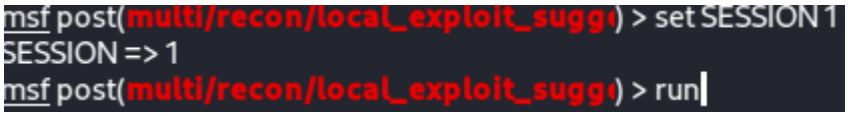

*Fig.5 Configurazione modulo

*Fig.6 Risultato modulo

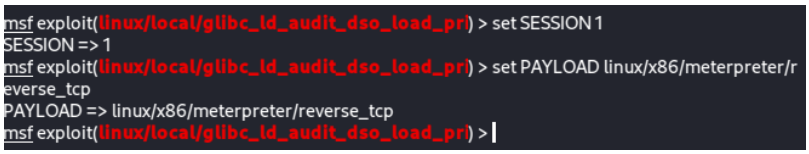

*Fig.7 Configurazione modulo scelto

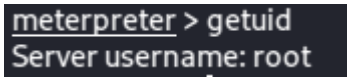

*Fig.8 Lancio e verifica exploit

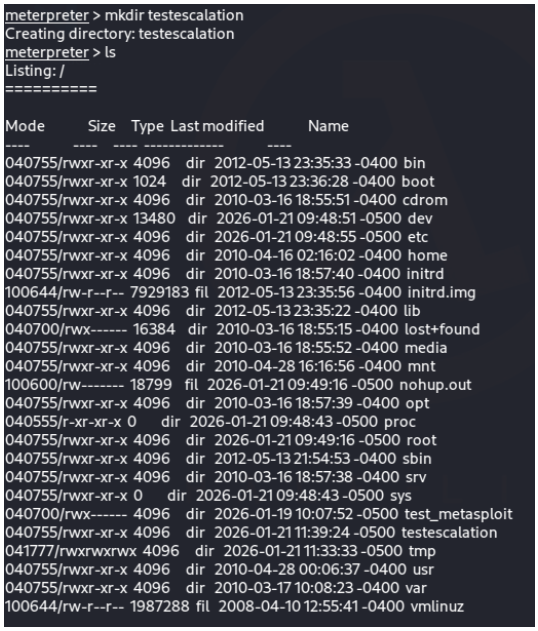

*Fig.9 Creazione lista in (/)

Dato che l'utente postgres ha privilegi limitatisi procede con **l'escalation di permessi** fino ad arrivare all'utente **root.**

Si cerca il modulo ***post/multi/recon/local_exploit_suggester*** che analizza il sistema compromesso per individuare e suggerire gli exploit specifici in base alla sessione creata.

La sua configurazione comprende:

- **SESSION:** ID sessione meterpreter attiva (1)

Come risultato darà una lista di tutti gli exploit locali che permetteranno di ottenere privilegi root.

Il modulo scelto è ***exploit/linux/local/glibc_ld_audit_dso_load_priv_esc*** e la sua configurazione è:

- **SESSION: 1**
- **PAYLOAD:** linux/x86/meterpreter/reverse_tcp

Il payload durante la configurazione è stato modificato per corrispondere **all'architettura** della macchina target **(x64 ----> x86)** e per evitare errori durante l'esecuzione del comando.

Viene aperta una nuova sessione ottenendo l'accesso come utente **root** e come verifica,si è proseguito con la creazione di una cartella ***testescalation*** all'interno della directory **(/)**

Fase 3 Accesso backdoor

```
useradd -m -s /bin/bash backup_service
passwd backup_service
```

*Fig.10 Creazione utente

```
Enter new UNIX password: backup_service
Retype new UNIX password: backup_service
passwd: password updated successfully
```

*Fig.11 Creazione password

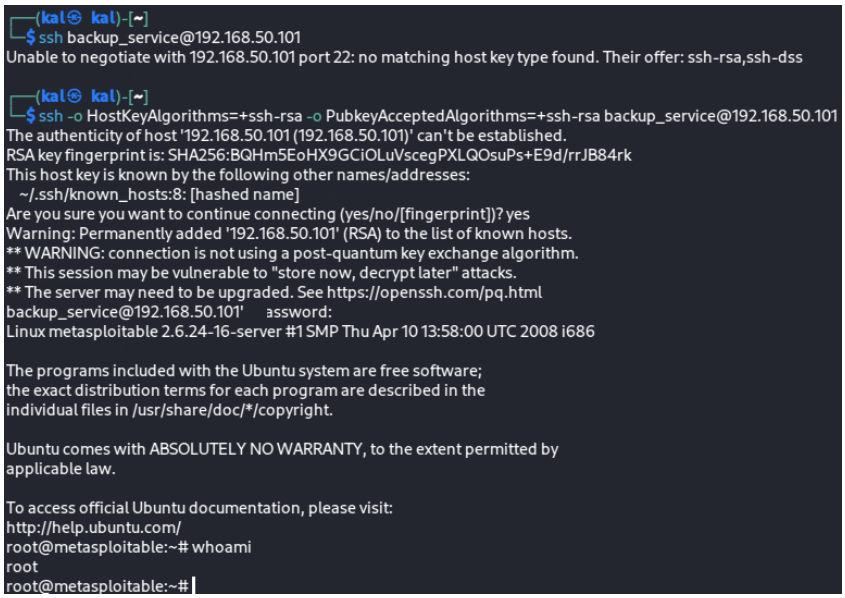

*Fig.12 Verifica backdoor

Come backdoor è stato scelto di creare un utente chiamato **backup_service** all'interno della Metasploitable dandogli i permessi root.

Per effettuare la connessione da terminale, la kali è stata forzata ad accettare algoritmi di cifratura obsoleti per permettere di comunicare con sistemi datati.

Come risultato finale si ha un accesso al sistema con comandi root per il controllo totale della macchina target.

Conclusione

L’analisi ha dimostrato come la presenza di versione di servizi obsoleti, come **PostgreSQL 8.3.1**, rappresenti un punto di ingresso critico che può portare alla completa compromissione del sistema.

Attraverso la lista di moduli locali, è stato permesso il passaggio da un utente limitato al controllo totale del server come **root**.

Inoltre, la creazione della backdoor ha permesso all’utente di entrare nuovamente nel sistema con l’utente avente permessi root.

Per mitigare questi attacchi:

- Aggiornare regolarmente i servizi all'ultima versione stabile per correggere le vulnerabilità note sfruttate dai moduli.
- Limitare l'accesso alla porta **5432** tramite **firewall**, consentendo connessioni solo da indirizzi IP autorizzati.
- Implementare **il principio del minimo privilegio** per garantire ulteriore sicurezza del sistema