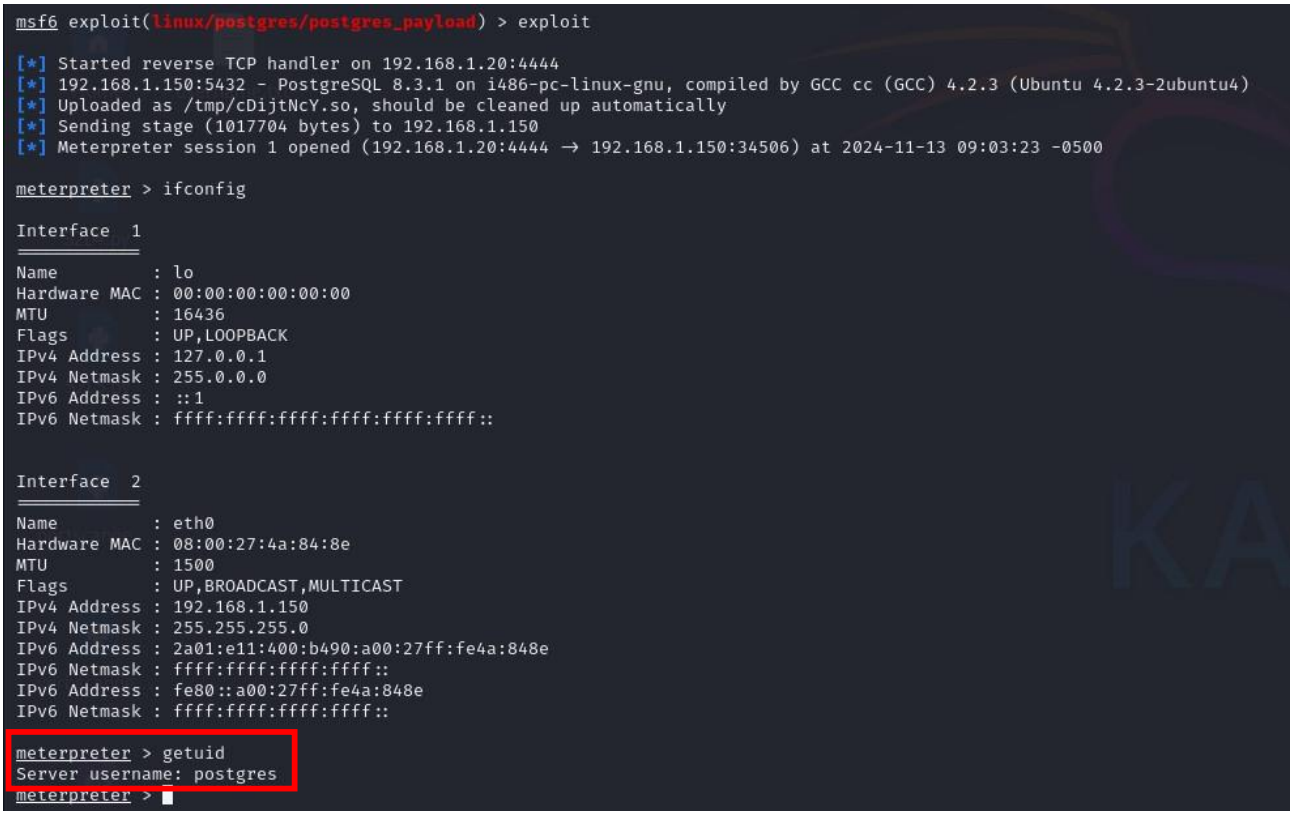
Esercizio S7 L3 del 13/11/24 ***Daniele Paolone***

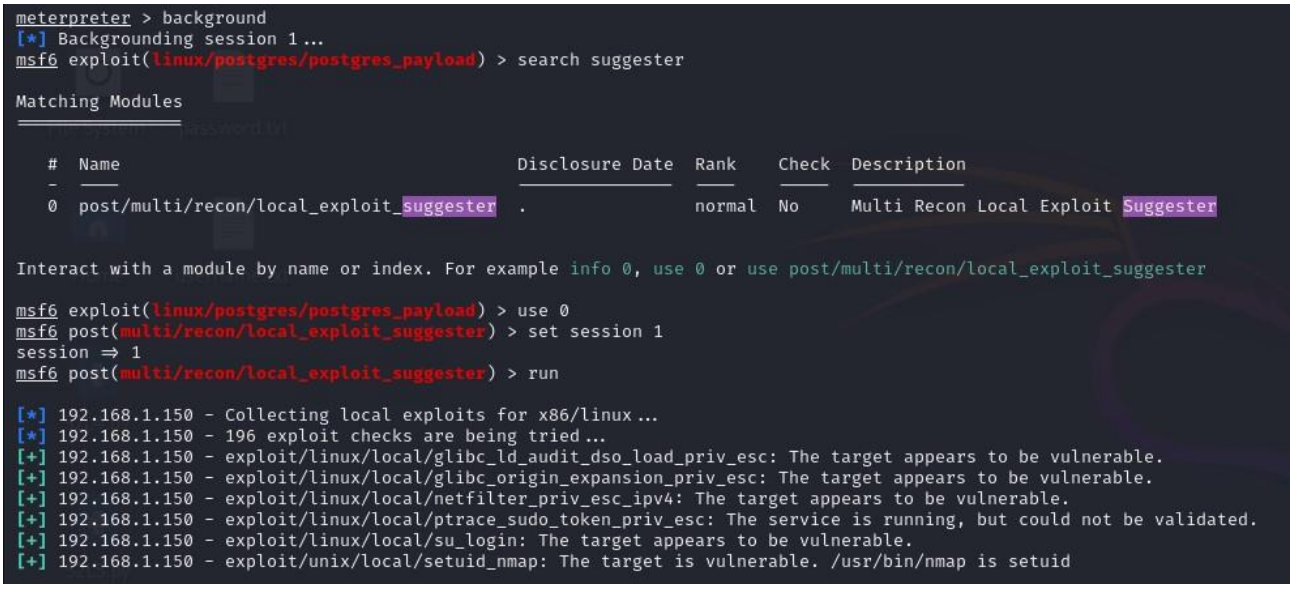
Sfruttare una vulnerabilità nel servizio PostgreSQL ed eseguire un'escalation di privilegi per passare da un utente limitato a root

Come primo passaggio, si deve ottenere una sessione di *Meterpreter*. Per questo motivo si utilizza l' exploit exploit/linux/postgres/postgres_payload.



Dopo essere riusciti nell' exploit, come si vede nell' immagine, si è ottenuta una sessione di meterpreter, ed inoltre, utilizzando il comando *getuid*, si può verificare quale tipologia di utente si ha avuto accesso, cioè *postgres.*

Giunti a questo punto, bisogna eseguire un altro exploit per passare da utente postgres ad utente root, quindi riuscire ad eseguire il privilege escalation. Per fare ciò va messa in pausa la sessione con il comando *background* ed eseguire un secondo comando *post/multi/recon/local_exploit_suggester*, che rilascerà una lista di exploit.



L' exploit da eseguire è *exploit/linux/local/glibc_ld_audit_dso_load_priv_esc*, che a sua volta rilascerà una lista di payloads. Quello interessato è *payload/linux/x86/meterpreter/reverse_tcp*.
Successivamente si settano la sessione che avevamo messo in pausa e anche il target. Quest' ultimo perché metasploitable2 è settato con x86 e non con x64, come lo esegue il payload in automatico.

Inseriti questi parametri si può procedere con l' esecuzione dell' exploit che effettuerà il privilege escalation, permettendo di accedere all' utente root. Eseguendo il comando getuid, si può verificare il cambio di utente.