# Consegna S7-L3

## Consegna: Escalation di privilegi con Metasploit

⚜️ **Tag:** #escalation_privilegi #metasploit #postgresql #meterpreter

### Obiettivo dell'Esercizio

Usare il modulo `exploit/linux/postgres/postgres_payload` per sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2 ed ottenere una sessione **Meterpreter** sul sistema target.

---

## Attività

1. **Preparazione dell'ambiente:**
   - Assicurarsi che l'indirizzo IP di Metasploitable sia configurato correttamente.
   - Verificare la comunicazione tra la macchina Kali e Metasploitable utilizzando comandi come `ping`.
2. **Esecuzione dell'exploit:**
   - Aprire msfconsole sulla macchina Kali.
   - Configurare il modulo `exploit/linux/postgres/postgres_payload` con i seguenti parametri:
     - `RHOSTS`: Indirizzo IP di Metasploitable.
     - `USERNAME`: Nome utente PostgreSQL (di default, "postgres").
     - `PASSWORD`: Password PostgreSQL (di default, "postgres").
   - Eseguire l'exploit per ottenere una sessione **Meterpreter**.
3. **Escalation di privilegi e backdoor:**
   - Verificare l'utente corrente eseguendo il comando `getuid`.

- Usare i moduli forniti da msfconsole per eseguire un'escalation di privilegi, con l'obiettivo di passare da un utente limitato a root.
- Installare una backdoor sulla macchina target per assicurare un accesso persistente.

4. **Verifica dell'accesso root:**
    - Eseguire nuovamente il comando `getuid` o qualsiasi altro comando che richieda privilegi root per verificare l'avvenuta escalation.

---

## Bonus

- Utilizzare i moduli **post** di msfconsole per identificare ulteriori vulnerabilità locali sfruttabili per escalation di privilegi.
- Documentare ogni passaggio, incluse le vulnerabilità identificate e gli exploit utilizzati.
- Testare ogni vulnerabilità e verificare i risultati con il comando `getuid` o con un comando privilegiato.

---

🔑 **Chiavi:**
[escalation_privilegi, metasploit, postgresql, meterpreter]