S7L3 Exploit di PostgreSQL ed Escalation di Privilegi

Introduzione e Obiettivi

L'obiettivo di questo esercizio è sfruttare una vulnerabilità nel servizio PostgreSQL di Metasploitable 2 per ottenere una sessione Meterpreter sul sistema target. Successivamente, si richiede di:

1. Eseguire un'escalation di privilegi per passare da un utente limitato (postgres) a root utilizzando solo i mezzi forniti da msfconsole.
2. Verificare l'identità dell'utente corrente tramite il comando getuid.

Metasploitable 2 è una macchina virtuale intenzionalmente vulnerabile progettata per testare tecniche di penetrazione. PostgreSQL, un database relazionale open-source, presenta una vulnerabilità che consente l'esecuzione di codice arbitrario, permettendo di ottenere accesso al sistema.

Descrizione dell'Esercizio

1. Configurazione e lancio dell'exploit per PostgreSQL

Abbiamo avviato Metasploit (msfconsole) e selezionato l'exploit specifico per PostgreSQL:

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

Successivamente, abbiamo configurato i parametri necessari:

- RHOSTS: Indirizzo IP della macchina target (192.168.50.101).
- LHOST: Indirizzo IP della nostra macchina Kali Linux (192.168.50.100).
- LPORT: Porta locale per la connessione inversa (4445).

Dopo aver impostato i parametri, abbiamo lanciato l'exploit:

```
run
```

L'exploit ha avuto successo, stabilendo una sessione Meterpreter sulla macchina target.

2. Verifica dell'utente corrente

Una volta ottenuta la sessione Meterpreter, abbiamo verificato l'identità dell'utente corrente utilizzando il comando:

```
getuid
```

Il risultato ha confermato che stavamo operando come utente postgres, un account con privilegi limitati.

3. Identificazione delle vulnerabilità locali
Per eseguire l'escalation di privilegi, abbiamo utilizzato il modulo post/multi/recon/local_exploit_suggester per identificare le vulnerabilità locali che potevano essere sfruttate:

use post/multi/recon/local_exploit_suggester

set session 1

run

Il modulo ha restituito una lista di potenziali exploit applicabili al sistema target.

4. Escalation di privilegi
Tra gli exploit suggeriti, abbiamo selezionato exploit/linux/local/glibc_ld_audit_dso_load_priv_esc, che consente di aumentare i privilegi a livello di root. Abbiamo configurato i parametri necessari:

- SESSION: Sessione Meterpreter attiva (sessione 1).
- LPORT: Nuova porta per la connessione inversa (4446).
- PAYLOAD: Payload linux/x86/meterpreter/reverse_tcp.

Dopo aver configurato i parametri, abbiamo lanciato l'exploit:

run

L'exploit ha avuto successo, ottenendo una nuova sessione Meterpreter con privilegi elevati. Abbiamo nuovamente verificato l'identità dell'utente corrente:

getuid

Il risultato ha confermato che ora stavamo operando come root.

Conclusioni

Questo esercizio ha dimostrato come sfruttare una vulnerabilità in PostgreSQL per ottenere una sessione Meterpreter su un sistema target. Successivamente, abbiamo utilizzato un modulo di escalation di privilegi per passare da un utente limitato (postgres) a root. Infine, abbiamo verificato l'identità dell'utente corrente in ogni fase del processo.
L'esercizio evidenzia l'importanza di patchare le vulnerabilità note nei servizi di rete e di adottare misure di sicurezza per prevenire l'escalation di privilegi. L'uso di strumenti come Metasploit può aiutare a identificare e mitigare tali minacce in un ambiente controllato.