Report: Exploitation e Privilege Escalation

Data: 22 Gennaio 2026

Target: Metasploitable 2 (Linux)

Obiettivo: Ottenere accesso root partendo dal servizio PostgreSQL.

---

1. Sintesi Esecutiva

L'attività ha simulato un attacco mirato a un database PostgreSQL vulnerabile. Attraverso l'uso del framework **Metasploit**, è stato possibile ottenere una shell iniziale con privilegi limitati, successivamente elevata a privilegi di amministratore di sistema (**root**) sfruttando una vulnerabilità del kernel locale.

---

2. Fase 1: Accesso Iniziale (Exploitation)

La prima fase ha riguardato lo sfruttamento del servizio PostgreSQL (porta 5432) per l'esecuzione di codice remoto.

- **Modulo utilizzato:** `exploit/linux/postgres/postgres_payload`
- **Vulnerabilità sfruttata:** Il modulo sfrutta la capacità dell'utente database `postgres` (con credenziali di default `postgres:postgres`) di scrivere file nel file system e caricarli come librerie condivise (.so) per eseguire codice arbitrario.
- **Risultato:** Apertura di una sessione **Meterpreter** con l'utente di sistema `postgres`.
- **Verifica identità:** Il comando `getuid` ha confermato l'identità dell'utente come `postgres (uid=106)`.

---

3. Fase 2: Post-Exploitation e Ricognizione Locale

Una volta ottenuto l'accesso come utente a bassi privilegi, è stata avviata una fase di analisi per identificare vettori di attacco interni.

- **Strumento:** `post/multi/recon/local_exploit_suggester`

- **Analisi:** Lo strumento ha scansionato il sistema target alla ricerca di vulnerabilità note non patchate nel kernel Linux di Metasploitable 2.
- **Identificazione:** È stata identificata la vulnerabilità `udev_netlink` come potenziale vettore critico per la scalata dei privilegi.

---

4. Fase 3: Escalation di Privilegi

Per passare da un utente limitato al controllo totale del sistema, è stato eseguito un exploit locale.

- **Modulo utilizzato:** `exploit/linux/local/udev_netlink`
- **Dettagli tecnici:** Questa vulnerabilità (CVE-2009-1185) risiede nel demone `udev`. Esso non verifica correttamente l'origine dei messaggi NETLINK inviati dal "user space". Un utente locale può inviare un messaggio malformato per istruire `udev` a eseguire un file binario con privilegi di **root**.
- **Procedura:**
    1. Impostazione della sessione target (`SET SESSION 1`).
    2. Configurazione di un nuovo `LPORT` (4445) per evitare conflitti con la sessione precedente.
    3. Esecuzione dell'exploit.

---

5. Risultati Finali e Conclusioni

L'attacco ha avuto successo. Al termine della procedura, è stata aperta una seconda sessione Meterpreter.

- **Verifica finale:** Il comando `getuid` ha restituito **`Server username: root (0)`**.
- **Stato del sistema:** Compromissione totale (Full System Compromise). L'attaccante ha ora pieno accesso a file di sistema, hash delle password (`/etc/shadow`) e configurazioni di rete.

---

6. Misure di Mitigazione Consigliate

Per prevenire questo tipo di attacchi, si raccomandano le seguenti azioni:

1. **Hardening del Database:** Cambiare le password di default di PostgreSQL e limitare i permessi dell'utente `postgres` affinché non possa scrivere in directory di sistema.
2. **Patch Management:** Aggiornare il kernel Linux e il demone `udev` a versioni non vulnerabili.
3. **Network Segregation:** Limitare l'accesso alla porta 5432 solo a host fidati tramite firewall