Pratica S6L4

Durante questo esercizio mi sono occupato di recuperare le password hashate che si trovano nel database di DVWA (Damn Vulnerable Web Application) e, successivamente, di decifrarle per ottenere la loro versione in chiaro. L'attività mi ha permesso di mettere in pratica alcune tecniche fondamentali di cybersecurity utilizzando strumenti specifici e simulando un ambiente di test realistico con macchine virtuali.

Gli strumenti che ho usato

Per completare l'esercizio ho usato:

1. **DVWA:** una piattaforma pensata apposta per esercitarsi con vulnerabilità di sicurezza.
2. **Mozilla Firefox:** il browser utilizzato per accedere alla DVWA sulla macchina Metasploitable.
3. **Rockyou.txt:** una wordlist molto famosa che contiene una lunga lista di password comuni.
4. **John the Ripper:** un programma per decifrare gli hash delle password.
5. **Kali Linux:** il sistema operativo host utilizzato per eseguire gli strumenti di analisi e cracking.
6. **Metasploitable:** una macchina virtuale vulnerabile configurata sulla stessa rete statica della macchina Kali Linux.

Passaggi seguiti

1. Configurazione dell'Ambiente

Ho configurato due macchine virtuali:

- **Kali Linux (host):** utilizzata per controllare e attaccare.
- **Metasploitable:** macchina vulnerabile dove è installata la DVWA.

Entrambe le macchine sono state collegate alla stessa rete statica per garantire la comunicazione tra di loro. Dal browser Mozilla Firefox sulla macchina Kali, ho acceduto all'interfaccia web della DVWA presente su Metasploitable inserendo l'indirizzo IP della macchina vulnerabile.

2. Accesso e Configurazione della DVWA

Una volta entrato nella DVWA, ho impostato il livello di sicurezza su **Low**, per consentire la vulnerabilità necessaria al test. Successivamente, ho utilizzato la vulnerabilità SQL Injection presente nella schermata di login per estrarre i dati delle password hashate dal database.

3. Recupero delle Password Hashate

Ho utilizzato un payload di SQL Injection per ottenere username e password hashate. Ad esempio, ho inserito il seguente comando nel campo username della pagina di login:

' OR '1'='1' --

Questo comando ha bypassato il controllo di autenticazione e restituito i dati degli utenti, comprese le password hashate, che ho copiato in un file di testo chiamato `hashes.txt` per l'analisi successiva.

4. Identificazione degli Hash

Prima di procedere con il cracking, ho verificato che le password fossero effettivamente hashate con l'algoritmo MD5. Questo si capisce dalla loro lunghezza (32 caratteri) e dal formato esadecimale. Per conferma, ho usato John the Ripper per elencare i formati supportati, assicurandomi che quello corretto fosse `raw-md5`.

5. Cracking delle Password

A questo punto ho avviato la fase di cracking. Ecco cosa ho fatto:

- Ho caricato il file `hashes.txt` contenente gli hash estratti.
- Ho selezionato la wordlist `rockyou.txt` per avere il maggior numero possibile di tentativi di confronto.
- Ho avviato il cracking con questo comando:

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

John the Ripper ha trovato le seguenti password:

- `password`
- `abc123`
- `letmein`
- `charley`

6. Verifica

Alla fine ho controllato che le password trovate fossero corrette e corrispondessero agli hash forniti. Tutto ha funzionato come previsto.

Conclusioni

Questo esercizio mi ha fatto capire quanto sia importante evitare l'utilizzo di algoritmi di hashing obsoleti come MD5. Strumenti come John the Ripper dimostrano quanto sia semplice decifrare password con questo tipo di protezione, specialmente se si utilizza una wordlist ampia come `rockyou.txt`.

Risultato dell’esercizio