Esercizio W14D1

Traccia:

Traccia: password cracking Esercizio Traccia Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema. Se guardiamo meglio le 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 con John the Ripper per recuperare la loro versione in chiaro.

Redatto da: Pandolfi Luciano

Data: 05/12/24

Dettagli dell'Ambiente:

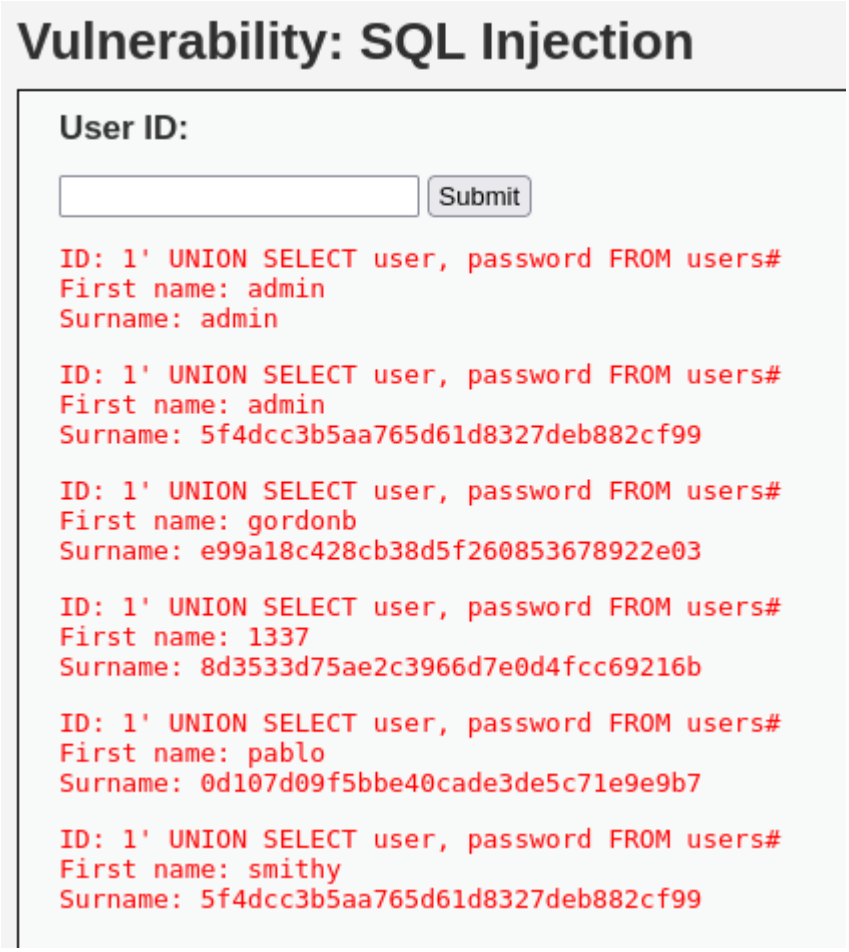
- **ATTANCANTE**: Kali Linux
  - **Indirizzo IP**: 192.168.1.18
- **TARGET:** Metasploitable2 (DVWA)
  - **Indirizzo IP**: 192.168.1.35

Obiettivo del Report:

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

Le password da craccare sono le seguenti:

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

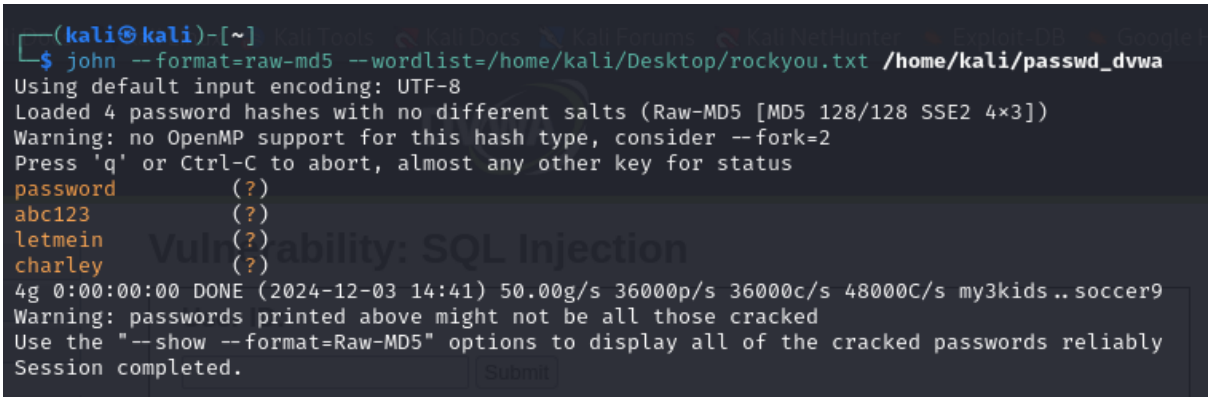


Per craccare gli hash delle password MD5 utilizziamo JtR John the Ripper).

La prima cosa da fare è creare un file **passwd_dvwa** dove andiamo ad inserire tutti gli hash delle password.

Sono andato poi ad eseguire il comando seguente utilizzando JtR per craccare gli hash delle password, specificando il dizionario da utilizzare ed il percorso del file rockyou.txt per confrontare hash delle password con password in chiaro.

- Screen:



Vi mostro in seguito le password craccate da JtR una volta terminata la sessione di cracking con il comando **“ john –show –format=Raw-MD5 passwd_dvwa “**.

- Screen: