Password Cracking su Database DVWA

1. Introduzione

L'obiettivo di questo esercizio è simulare uno scenario di post-compromissione in cui un attaccante ha ottenuto l'accesso al database di un'applicazione vulnerabile in questo caso la DVWA.

Dopo gli argomenti spiegati in classe devo distinguere due tipi di attacchi alle password:

- Attacchi Online (Hydra): si usano contro form di login attivi (tentare di indovinare la password via SSH o pagina web).
- Attacchi Offline (John the Ripper): si usano quando abbiamo già "rubato" gli hash e vogliamo lavorarci con calma sul nostro computer per scoprirne il testo in chiaro.

Visto che l'esercizio chiede di recuperare le password hashate dal database e poi craccarle, eseguiro un Attacco Offline. Per questo motivo lo strumento principale che utilizzò sarà John the Ripper, mentre l'enumerazione ci serve per individuare i punti di accesso.

2. Strumenti Utilizzati

Per lo svolgimento dell'esercizio all'interno del laboratorio virtuale utilizzerò i seguenti strumenti:

- Kali Linux: La macchina attaccante.
- DVWA (su Metasploitable): La macchina target contenente il database MySQL.
- MySQL Client: Per connettermi al database ed estrarre i dati.
- Hash-Identifier: Per confermare la natura dell'algoritmo di hashing (MD5).
- John the Ripper: Lo strumento di password cracking offline studiato oggi. Utilizzerò la modalità dizionario (wordlist).

- Wordlist (rockyou.txt): Il dizionario standard contenente milioni di password comuni.

3.Svolgimento dell'Esercizio

Recupero delle Password dal Database

In questa fase accedo al servizio MySQL della macchina target per leggere la tabella users.

- Apro il terminale sulla Kali.

- Accedo al database MySQL, sulla macchina Metasploitable il comando è:

```
msfadmin@metasploitable:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Per la password ho premuto invio lasciando vuoto perchè di solito le password possono essere owaspbwa o può non esserci quindi invio.

- Una volta dentro la shell MySQL, visualizzo i database:

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

mysql>
```

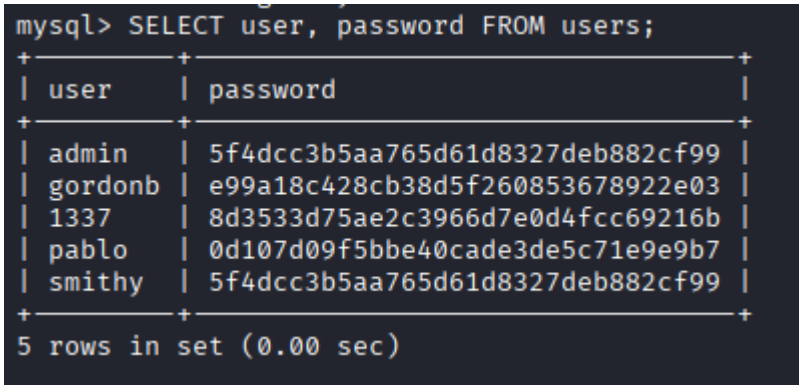
- Seleziono il database DVWA:

```
mysql> use dvwa
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

- Estraggo utenti e password con la query:

```
mysql> show tables;
+-----------------+
| Tables_in_dvwa  |
+-----------------+
| guestbook       |
| users           |
+-----------------+
2 rows in set (0.00 sec)
```



```
mysql> SELECT user, password FROM users;
+----------+----------------------------------+
| user     | password                         |
+----------+----------------------------------+
| admin    | 5f4dcc3b5aa765d61d8327deb882cf99 |
| gordonb  | e99a18c428cb38d5f260853678922e03 |
| 1337     | 8d3533d75ae2c3966d7e0d4fcc69216b |
| pablo    | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| smithy   | 5f4dcc3b5aa765d61d8327deb882cf99 |
+----------+----------------------------------+
5 rows in set (0.00 sec)
```

Identificazione dell'Hash

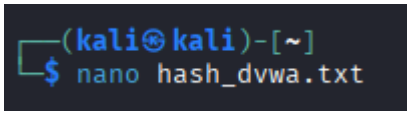
Prima di procedere all'attacco verifico l'algoritmo di hashing utilizzato. Prelevando una stringa hash (quella dell'utente admin) e analizzandola con il tool hash-identifier ho confermato che si tratta di algoritmo MD5.

Esecuzione del Cracking con John the Ripper

Questa è la fase critica dell'esercizio, per eseguire l'attacco offline sono stati seguiti i seguenti sottopassaggi sulla macchina Kali Linux:

Creazione del File degli Hash

Per permettere a John the Ripper di analizzare i dati ho creato manualmente un file di testo contenente gli hash estratti



Inserimento i dati recuperati nel formato utente:hash, questo è cio che ho inserito:

```
┌──(kali㉿kali)-[~]
└─$ cat hash_dvwa.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Preparazione della Wordlist

Ho verificat la presenza del dizionario rockyou.txt dentro /usr/share/wordlists/ e il risultato è stato positivo.

Avvio dell'Attacco

Con il file degli hash e il dizionario pronti ho lanciato l'attacco specificando il formato Raw-MD5

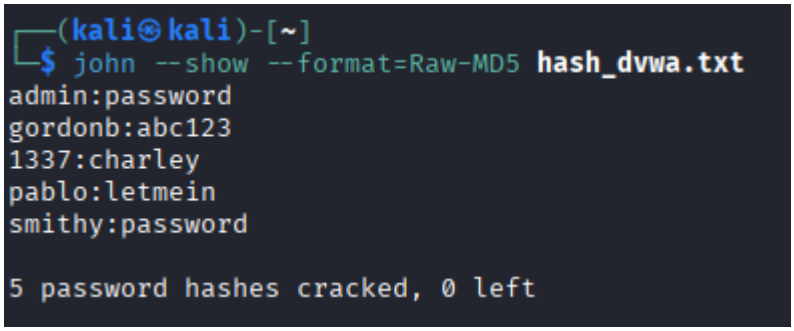
```
┌──(kali㉿kali)-[~]
└─$ rm ~/.john/john.pot

┌──(kali㉿kali)-[~]
└─$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash_dvwa.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2026-01-15 12:41) 400.0g/s 307200p/s 307200c/s 460800C/s my3kids..dangerous
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.
```

Il tool ha iniziato a comparare gli hash calcolati dalle parole del dizionario con quelli presenti nel file hash_dvwa.txt mostrando a schermo le corrispondenze trovate in tempo reale.

Verifica dei Risultati

Al termine dell'elaborazione per visualizzare un riepilogo pulito e completo delle credenziali recuperate in chiaro ho utilizzato il comando di visualizzazione:



4. Conclusione

L'esercitazione ha dimostrato l'efficacia degli attacchi a dizionario contro algoritmi di hashing deboli come MD5. Con l'uso di John the Ripper e una wordlist comune (rockyou.txt) sono stato in grado di recuperare in pochi secondi le password in chiaro partendo dai soli hash del database.

Le evidenze emerse sottolineano due gravi vulnerabilità nella configurazione della DVWA:

1. L'uso di MD5 senza "salt" rende gli hash estremamente facili da invertire.
2. Gli utenti utilizzavano password presenti nei dizionari comuni (come: "password", "abc123"), rendendo l'attacco immediato.

Come contromisura ho pensato all'uso di algoritmi robusti e l'obbligo di password complesse.