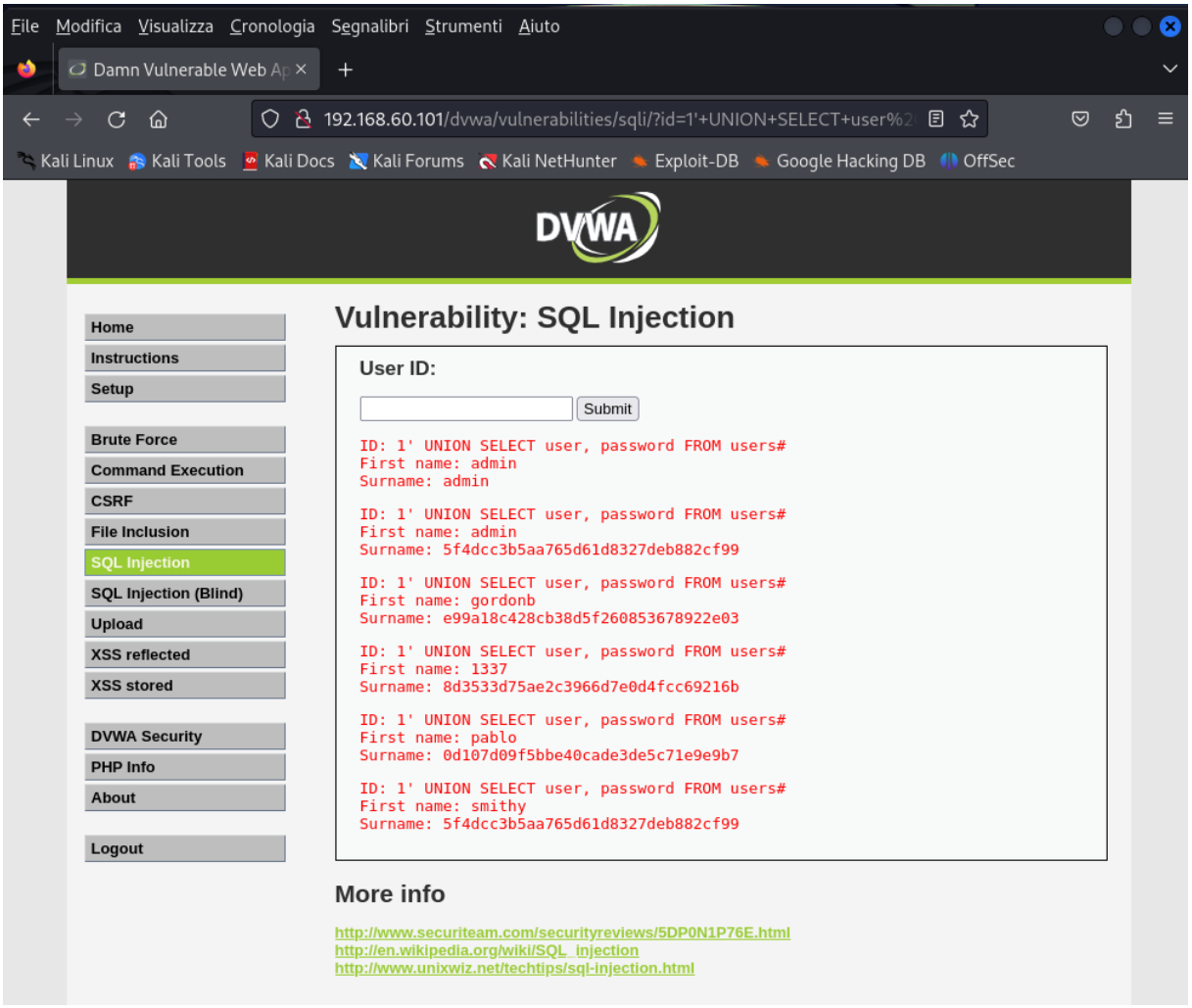
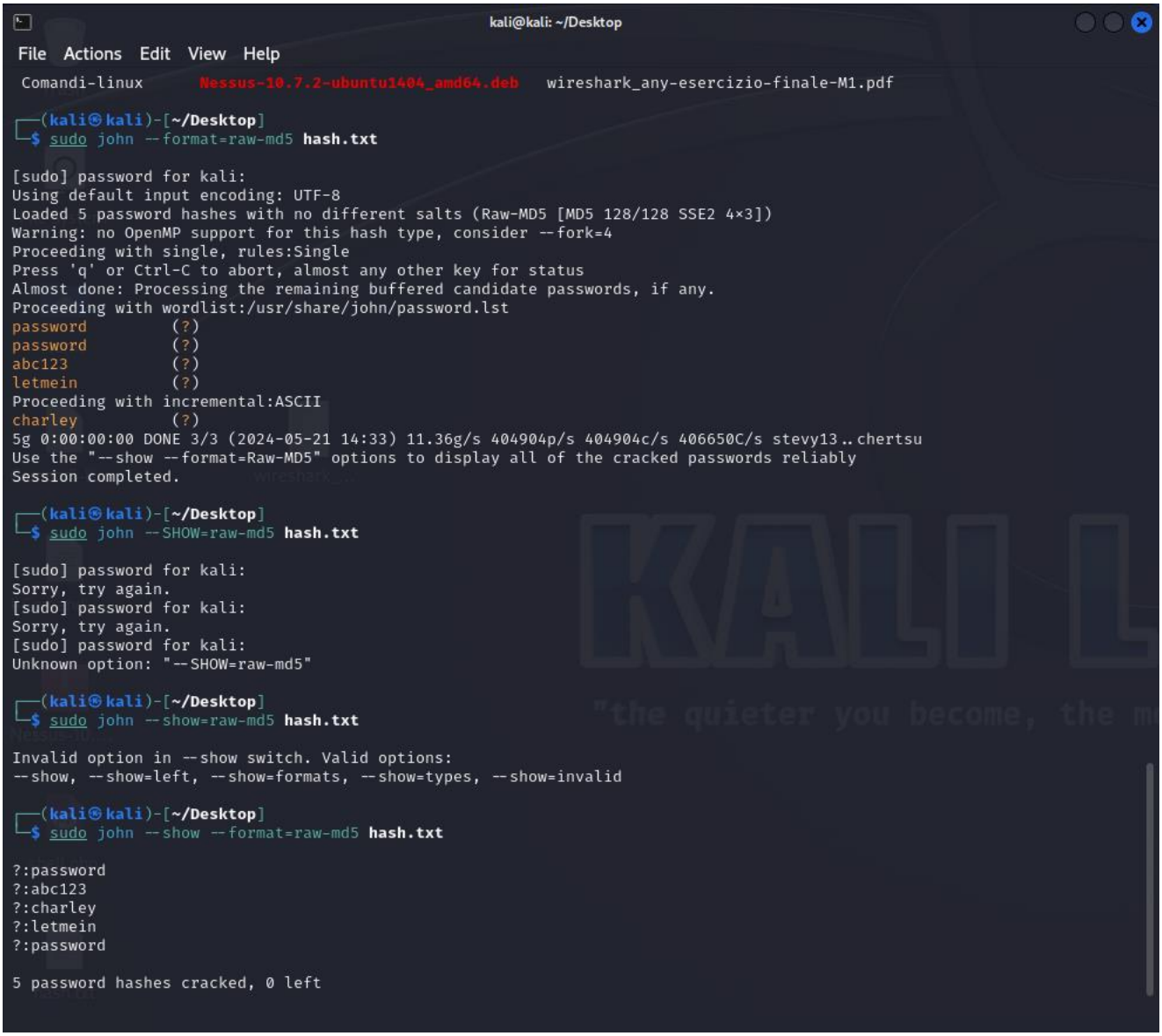
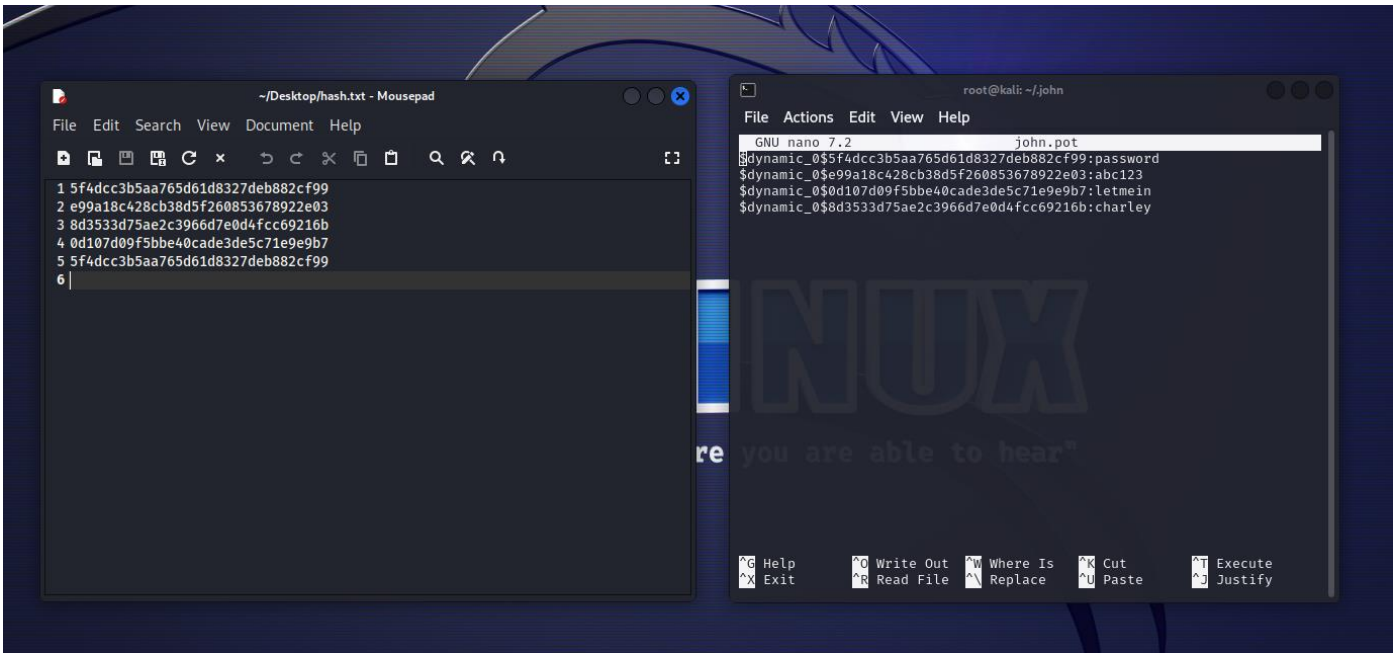


Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema, queste password però sono criptate e quello che vediamo nel surname è l'hash delle password e come ci suggerisce l'esercizio dovrebbero essere codificate con l'algoritmo MD5.

Anche se l'algoritmo in sé non è reversibile. Ciò non significa che crackare gli hash sia impossibile. Disponendo della versione con hash di una password e si conosce l'algoritmo di hashing, puoi utilizzare quell'algoritmo di hashing per eseguire l'hashing di un gran numero di parole, chiamato dizionario. Puoi quindi confrontare questi hash con quello che stai cercando di decifrare, per vedere se qualcuno di essi corrisponde. Se lo fanno, ora sai quale parola corrisponde a quell'hash.


kali@kali: ~/Desktop
File Actions Edit View Help
Comandi-linux Nessus-10.7.2-ubuntu1404_amd64.deb wireshark_any-esercizio-finale-M1.pdf
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --format=raw-md5 hash.txt
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2024-05-21 14:33) 11.36g/s 404904p/s 404904c/s 406650C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --SHOW=raw-md5 hash.txt
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Unknown option: "--SHOW=raw-md5"
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --show=raw-md5 hash.txt
Invalid option in --show switch. Valid options:
--show, --show=left, --show=formats, --show=types, --show=invalid
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --show --format=raw-md5 hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left


~/Desktop/hash.txt - Mousepad
File Edit Search View Document Help
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6
root@kali: ~/.john
File Actions Edit View Help
GNU nano 7.2 john.pot
$dynamic_0$5f4dcc3b5aa765d61d8327deb882cf99:password
$dynamic_0$e99a18c428cb38d5f260853678922e03:abc123
$dynamic_0$0d107d09f5bbe40cade3de5c71e9e9b7:letmein
$dynamic_0$8d3533d75ae2c3966d7e0d4fcc69216b:charley
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify