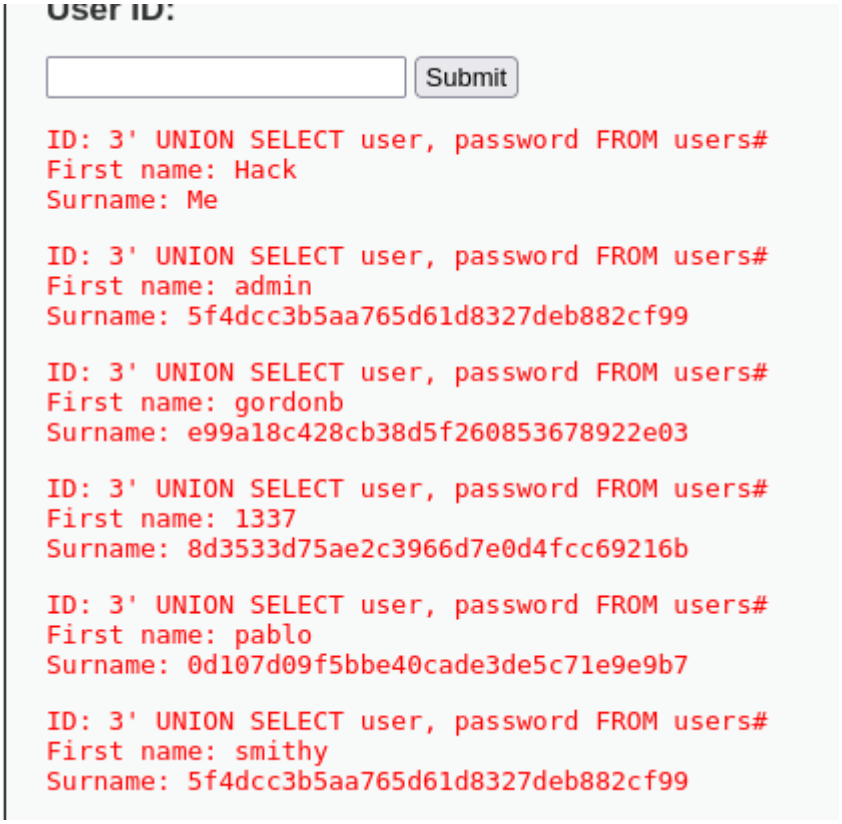
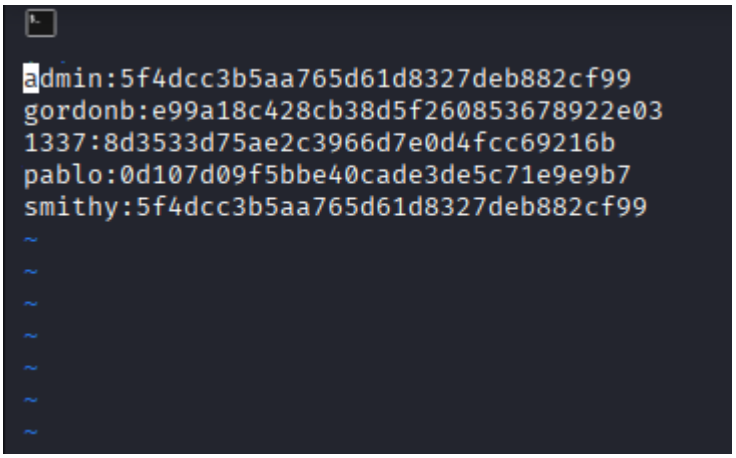
W14D1 - Password cracking e malware

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

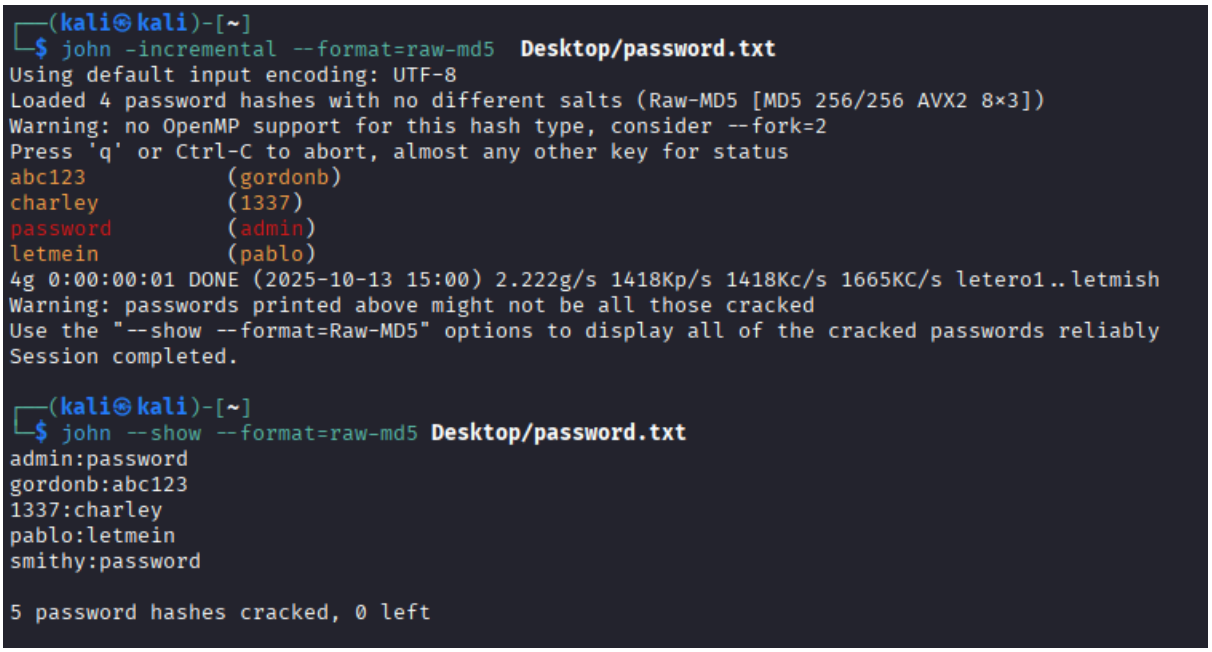


le credenziali le scriviamo su un file di testo come in figura sotto



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



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.