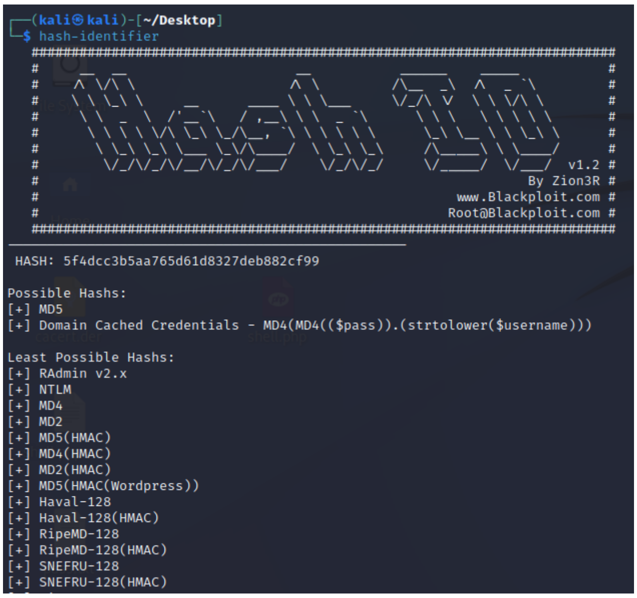
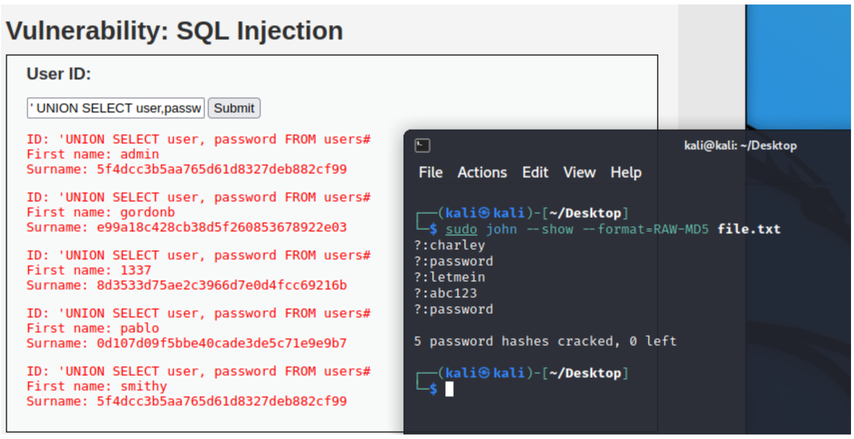
Offline password cracking

3-1-2023

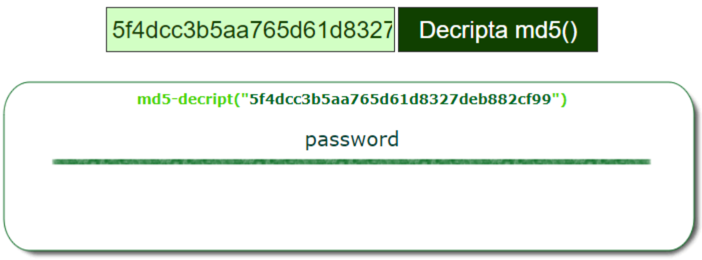


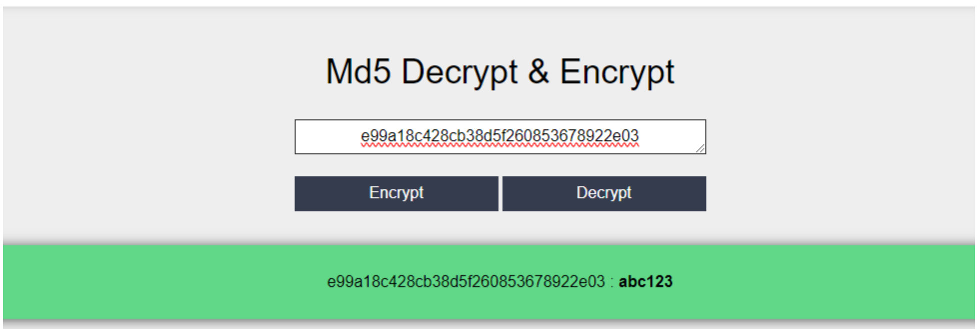
Dopo aver ottenuto i codici hash ne inserisco uno nel programma per capire di che tipo di criptazione si tratta poi procedo all'attacco



Basandoci sull'attacco di tipo SQL injection fatto ieri, avvalendoci di un tool preinstallato nella macchina kali linux chiamato John the Ripper, possiamo provare una serie di combinazioni criptate nello stesso tipo di hash che stiamo cercando di scoprire, dato che la criptazione di tipo MD5 è irreversibile bisogna per forza avvalersi di questo tipo di ricerca "a dizionario" fino ad azzeccare la combinazione corretta.

Questo tipo di vulnerabilità del metodo di criptazione danneggia solo chi usa password deboli e scontate dato che come in un bruteforce più lunga e complessa la password è, meno sono le possibilità che un software di questo tipo abbia effetto, e se si usa una combinazione seguendo le best practice come una lunghezza superiore a 12 caratteri con numeri e simboli e un rinnovo a cadenza annuale l'efficacia dell'attacco viene annullata quasi completamente.





La pericolosità di usare password scontate come in questo caso è lampante dato che basta inserire i codici in un qualsiasi sito accessibile a tutti su internet per ottenere una corrispondenza in pochi secondi.