PASSWORD CRACKING

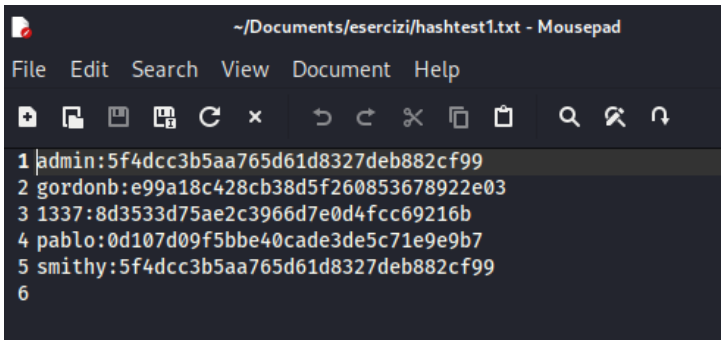
1. Hash di password (MD5) recuperate tramite SQL injection e relativi nomi utenti

2. Tecnica utilizzata

Per recuperare le password in chiaro utilizzerò la tecnica cosidetta *password cracking a dizionario* ovvero si confrontano gli hash di password comuni presenti in una lista con quelli recuperati tramite SQL injection. Al fine di ottenere le password mi avvarrò di un tool per automatizzare la ricerca ovvero JohnTheRipper e come dizionario utilizzerò una wordlist già presente nella nostra macchina ovvero *rockyou.txt* .

3. Esecuzione dell'hash cracking

Prepariamo il file da analizzare con JohnTheRipper abbinando nomi utenti e password così da facilitare la lettura del risultato del cracking.



Lo screenshot successivo mostra il risultato del cracking.