PASSWORD CRACKING

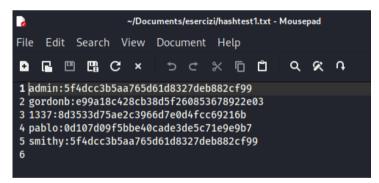
1. Hash di password (MD5) recuperate tramite SQL injection e relativi nomi utenti

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.

```
(kali⊗kali)-[/usr/share/wordlists]
 💲 john --wordlist=rockyou.txt --format=raw-md5 --verbosity=5 /home/kali/Documents/esercizi/hashtest1.txt
initUnicode(UNICODE, UTF-8/ISO-8859-1)
UTF-8 → UTF-8 → UTF-8
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider -- fork=2
Loaded 10 hashes with 1 different salts to test db from test vectors
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123
                 (pablo)
                (1337)
charley
4g 0:00:00:00 DONE (2023-09-06 17:45) 44.44g/s 34133p/s 34133c/s 51200C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```