Report Cracking Password

Per crackare delle password cryptate possiamo andare a utilizzare vari tool già preimpostati su kali, oggi abbiamo utilizzato Jack the Ripper per decryptare le password trovate nel database del dvwa di metasploitable. Le password erano cryptate in HASH e quello che abbiamo fatto è:

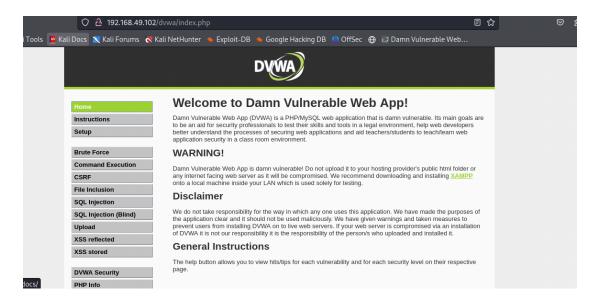
```
john -- format=raw-MD5 /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed
for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
                 (smithy)
abc123
                 (gordonb)
letmein
                (pablo)
Proceeding with incremental:ASCII
charley
                 (1337)
5g 0:00:00:00 DONE 3/3 (2024-02-28 08:58) 13.51g/s 492610p/s 492610c/s 539097
C/s stevy13..candake
Use the "---show ---format=Raw-MD5" options to display all of the cracked passw
ords reliably
```

Creare prima di tutto un file "hash.txt" con all'interno tutte le password in formato hash con il corrispondente nome utente, (user:password). Successivamente andiamo a utilizzare un comando che ci consente di decryptarle per averle in chiaro, il comando è john --format=raw-MD5 dove MD5 è il formato di decryptazione che utilizziamo.

Come possiamo vedere tutte e 5 le password sono state trovate e adesso proviamo ad accedere al DVWA di metasploitable usando un altro account con la password che abbiamo appena trovato, e come vediamo:



Username	
pablo	
Password	
letmein	
	Login



E siamo dentro!