CRACKING HASHES USING HASHCAT

STEP 1

Same as before cracking the hash type we need to find the hash type or format using hash-identifier, you can also use tools from online

```
└─$ hash-identifier
   ##########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__  \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\  \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/   \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   ##########################################################################
--------------------------------------------------
 HASH: f03b919de2cb8a36e9e404e0ad494627

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$salt)
```

STEP 2

```
└─$ hashcat -m 0 -a 0 h2.txt rockyou.txt
hashcat (v6.2.6) starting
```

Using hashcat and using the MD5 module the famous rockyou.txt wordlist to crack the hash and get the password

STEP 3

The hashcat has been launched and its cracking the password. You can checkout the status. If you get exhausted it probably means the wordlist or the hash-type isn't appropriate so also try the least possible hashes mentioned by hashcat

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

f03b919de2cb8a36e9e404e0ad494627:INDIA

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: f03b919de2cb8a36e9e404e0ad494627
Time.Started.....: Sun Jul 21 18:34:50 2024 (1 sec)
Time.Estimated...: Sun Jul 21 18:34:51 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   402.3 kH/s (144115188075.96ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 163328/14344384 (1.14%)
Rejected.........: 0/163328 (0.00%)
Restore.Point....: 162816/14344384 (1.14%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: London1 -> 860412
Hardware.Mon.#1..: Util: 36%

Started: Sun Jul 21 18:34:49 2024
Stopped: Sun Jul 21 18:34:52 2024
```