CRACKING HASHES WITH HASHCAT

STEP 1

First we need to identify the hash type. Using the hash-identifier we can check for the most to least possible hash types and work our way from there.

```
└─$ hash-identifier h1.txt
   ##########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \      __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \   /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \ /\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   ##########################################################################
--------------------------------------------------

 Not Found.
--------------------------------------------------
 HASH: 56901cf4584b7841ec3cdbe1dba23caa47a79eb1

Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))

Least Possible Hashs:
[+] Tiger-160
[+] Haval-160
[+] RipeMD-160
[+] SHA-1(HMAC)
[+] Tiger-160(HMAC)
[+] RipeMD-160(HMAC)
[+] Haval-160(HMAC)
[+] SHA-1(MaNGOS)
[+] SHA-1(MaNGOS2)
[+] sha1($pass.$salt)
[+] sha1($salt.$pass)
[+] sha1($salt.md5($pass))
[+] sha1($salt.md5($pass).$salt)
[+] sha1($salt.sha1($pass))
```

STEP 2

```
└─$ hashcat -m 100 h1.txt /usr/share/wordlists/sqlmap.txt
hashcat (v6.2.6) starting
```

Using the hashcat tool we use the SHA-1 hash type and check for possible hashes using the sqlmap wordlist.

STEP 3

```
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..: /usr/share/wordlists/sqlmap.txt
* Passwords.: 1633938
* Bytes.....: 14891958
* Keyspace..: 1633938

56901cf4584b7841ec3cdbe1dba23caa47a79eb1:flag1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 100 (SHA1)
Hash.Target......: 56901cf4584b7841ec3cdbe1dba23caa47a79eb1
Time.Started.....: Sun Jul 21 20:19:22 2024 (2 secs)
Time.Estimated...: Sun Jul 21 20:19:24 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/sqlmap.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   412.7 kH/s (144115188075.97ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 794624/1633938 (48.63%)
Rejected.........: 0/794624 (0.00%)
Restore.Point....: 794112/1633938 (48.60%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: fkj2003 -> flamaster
Hardware.Mon.#1..: Util: 32%

Started: Sun Jul 21 20:19:21 2024
Stopped: Sun Jul 21 20:19:26 2024
```

The hashcat has been launched and it has cracked the hash and found the password which is (flag 1) in this scenario.