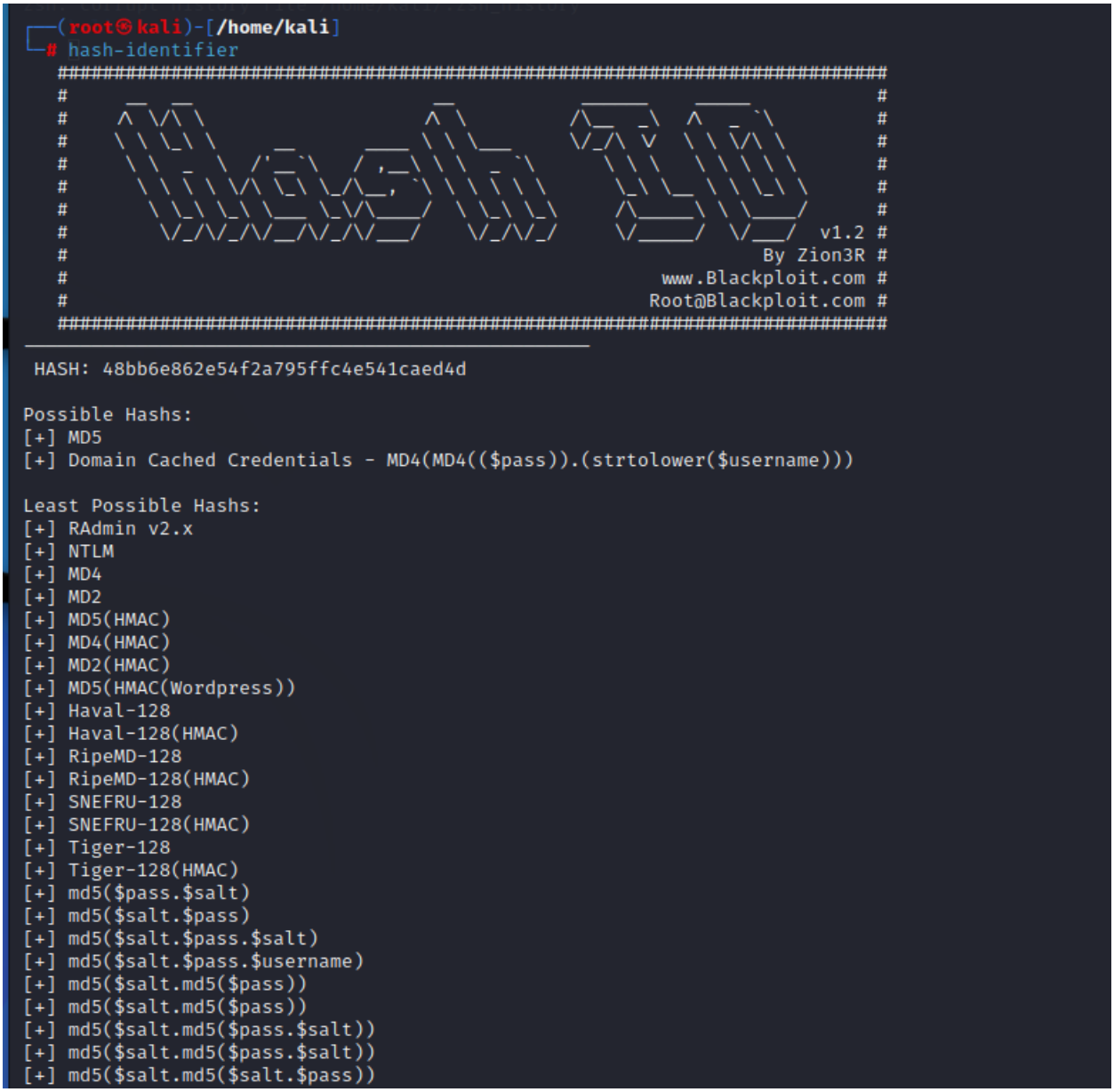
[Crack the Hash walkthrough on TryHackMe | j.info Cybersecurity Blog (j-info.github.io)]

[Hash Type Identifier - Identify unknown hashes]

Task 1 Level 1



```
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.$salt)
[+] md5($salt.$pass.$username)
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass.$salt))
[+] md5($salt.md5($pass.$salt))
[+] md5($salt.md5($salt.$pass))
[+] md5($salt.md5(md5($pass).$salt))
[+] md5($username.0.$pass)
[+] md5($username.LF.$pass)
[+] md5($username.md5($pass).$salt)
[+] md5(md5($pass))
[+] md5(md5($pass).$salt)
[+] md5(md5($pass).md5($salt))
[+] md5(md5($salt).$pass)
[+] md5(md5($salt).md5($pass))
[+] md5(md5($username.$pass).$salt)
[+] md5(md5(md5($pass)))
[+] md5(md5(md5(md5($pass))))
[+] md5(md5(md5(md5(md5($pass)))))
[+] md5(sha1($pass))
[+] md5(sha1(md5($pass)))
[+] md5(sha1(md5(sha1($pass))))
[+] md5(strtoupper(md5($pass)))
--------------------------------------------------

HASH:
```

```
┌──(root㉿kali)-[/home/kali]
└─# hashcat --help
hashcat (v6.2.6) starting in help mode

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long          | Type | Description                                          | Example
═══
 -m, --hash-type               | Num  | Hash-type, references below (otherwise autodetect)   | -m 1000
 -a, --attack-mode             | Num  | Attack-mode, see references below                    | -a 3
 -V, --version                 |      | Print version                                        |
 -h, --help                    |      | Print help                                           |
     --quiet                   |      | Suppress output                                      |
     --hex-charset             |      | Assume charset is given in hex                       |
     --hex-salt                |      | Assume salt is given in hex                          |
     --hex-wordlist            |      | Assume words in wordlist are given in hex            |
     --force                   |      | Ignore warnings                                      |
     --deprecated-check-disable |      | Enable deprecated plugins                            |
     --status                  |      | Enable automatic update of the status screen         |
     --status-json             |      | Enable JSON format for status output                 |
     --status-timer            | Num  | Sets seconds between status screen updates to X      | --status-timer=1
     --stdin-timeout-abort     | Num  | Abort if there is no input from stdin for X seconds  | --stdin-timeout-abo
rt=300
```

```
═══=+═══════════════════════════════════════════════════=+═══════════
  900 | MD4                                               | Raw Hash
    0 | MD5                                               | Raw Hash
  100 | SHA1                                              | Raw Hash
 1300 | SHA2-224                                          | Raw Hash
 1400 | SHA2-256                                          | Raw Hash
10800 | SHA2-384                                          | Raw Hash
 1700 | SHA2-512                                          | Raw Hash
17300 | SHA3-224                                          | Raw Hash
17400 | SHA3-256                                          | Raw Hash
17500 | SHA3-384                                          | Raw Hash
17600 | SHA3-512                                          | Raw Hash
 6000 | RIPEMD-160                                        | Raw Hash
  600 | BLAKE2b-512                                       | Raw Hash
11700 | GOST R 34.11-2012 (Streebog) 256-bit, big-endian  | Raw Hash
11800 | GOST R 34.11-2012 (Streebog) 512-bit, big-endian  | Raw Hash
 6900 | GOST R 34.11-94                                   | Raw Hash
17010 | GPG (AES-128/AES-256 (SHA-1($pass)))              | Raw Hash
 5100 | Half MD5                                          | Raw Hash
17700 | Keccak-224                                        | Raw Hash
17800 | Keccak-256                                        | Raw Hash
17900 | Keccak-384                                        | Raw Hash
18000 | Keccak-512                                        | Raw Hash
 6100 | Whirlpool                                         | Raw Hash
10100 | SipHash                                           | Raw Hash
   70 | md5(utf16le($pass))                               | Raw Hash
  170 | sha1(utf16le($pass))                              | Raw Hash
 1470 | sha256(utf16le($pass))                            | Raw Hash
```

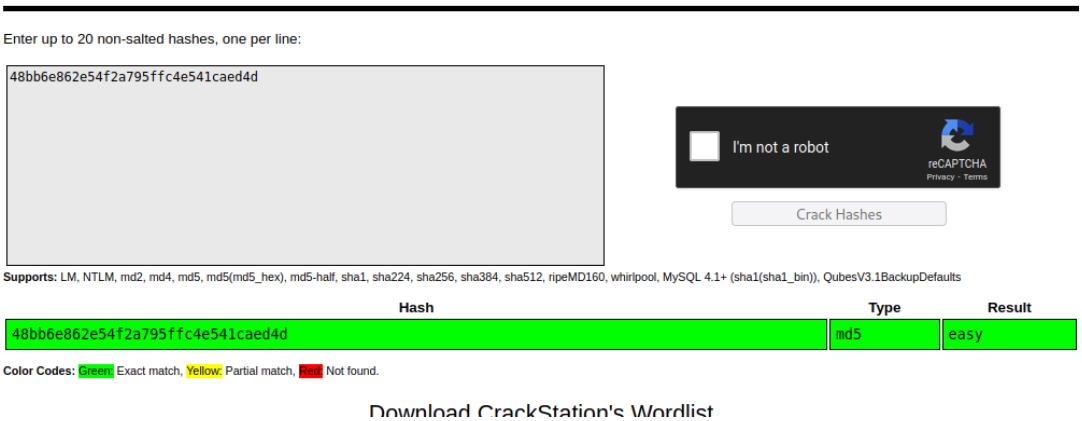
Can you complete the level 1 tasks by cracking the hashes?

Answer the questions below

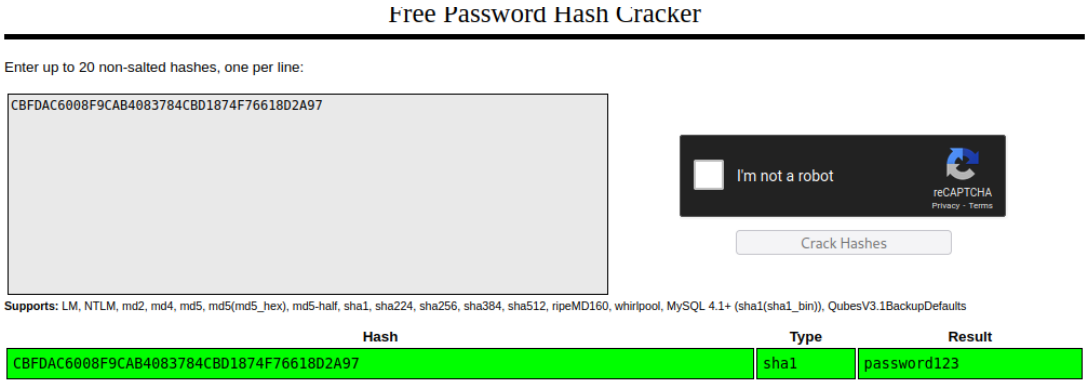
48bb6e862e54f2a795ffc4e541caed4d

```
┌──(root㉿kali)-[/home/kali/crackthehash]
└─# echo "48bb6e862e54f2a795ffc4e541caed4d"> pass.txt
```

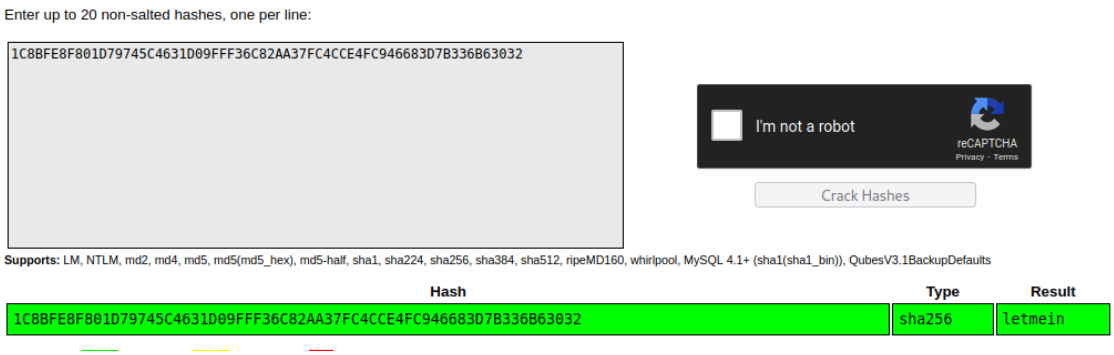
Hash :md5 ->



CBFDAC6008F9CAB4083784CBD1874F76618D2A97



1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032



$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom

```
┌──(root㉿kali)-[/home/kali/crackthehash]
└─# hashcat -m 3200 "\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom" /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, 1438/2940 MB (512 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385
```

->bleh

279412f945939ba78ce0758d3fd83daa

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

279412f945939ba78ce0758d3fd83daa

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
279412f945939ba78ce0758d3fd83daa	md4	Eternity22

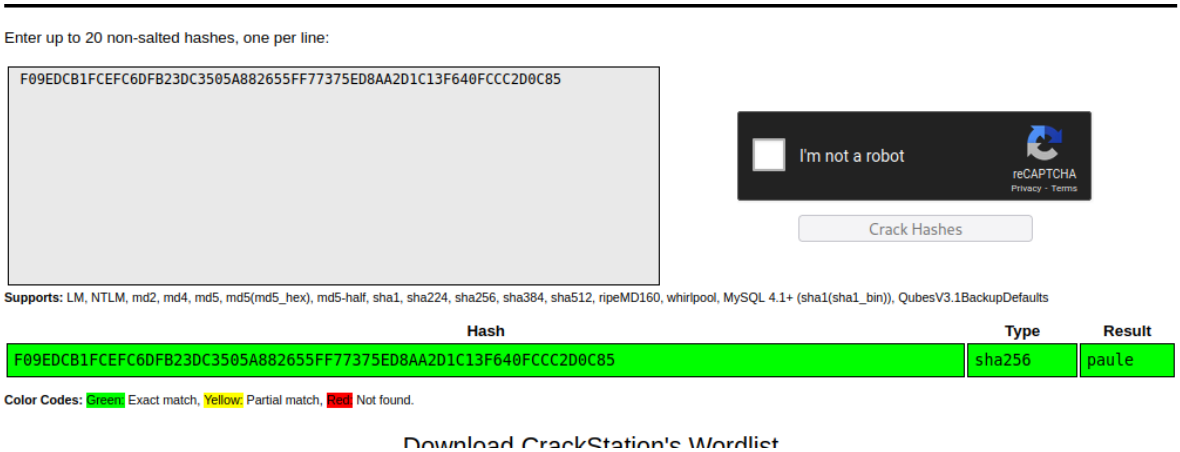
Task 2 Level 2

This task increases the difficulty. All of the answers will be in the classic rock you password list.

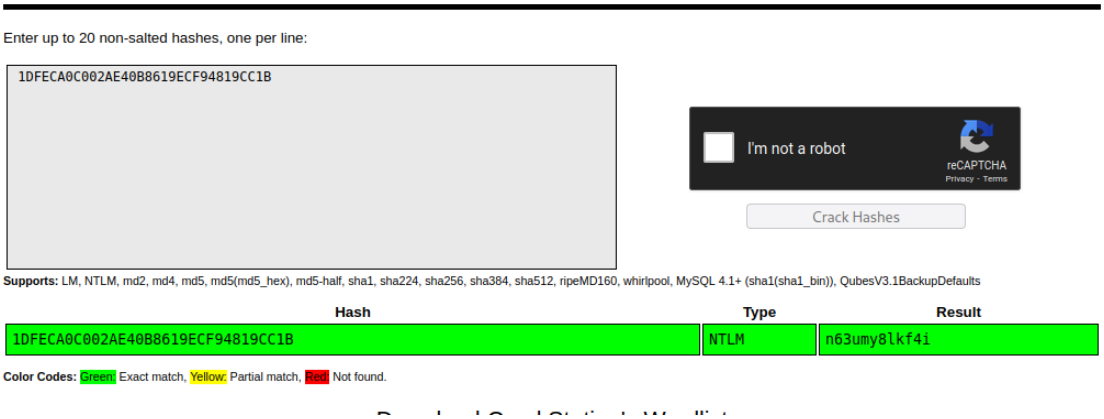
You might have to start using hashcat here and not online tools. It might also be handy to look at some example hashes on hashcats page.

Answer the questions below

Hash:
F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85

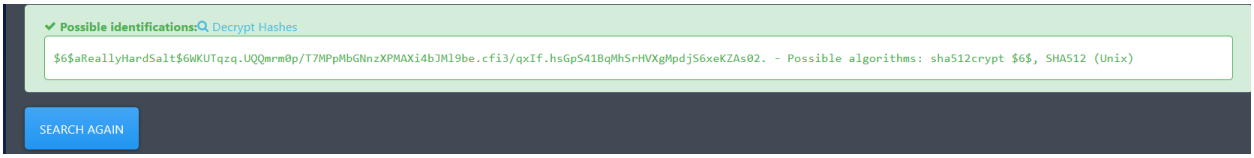


Hash: 1DFECA0C002AE40B8619ECF94819CC1B



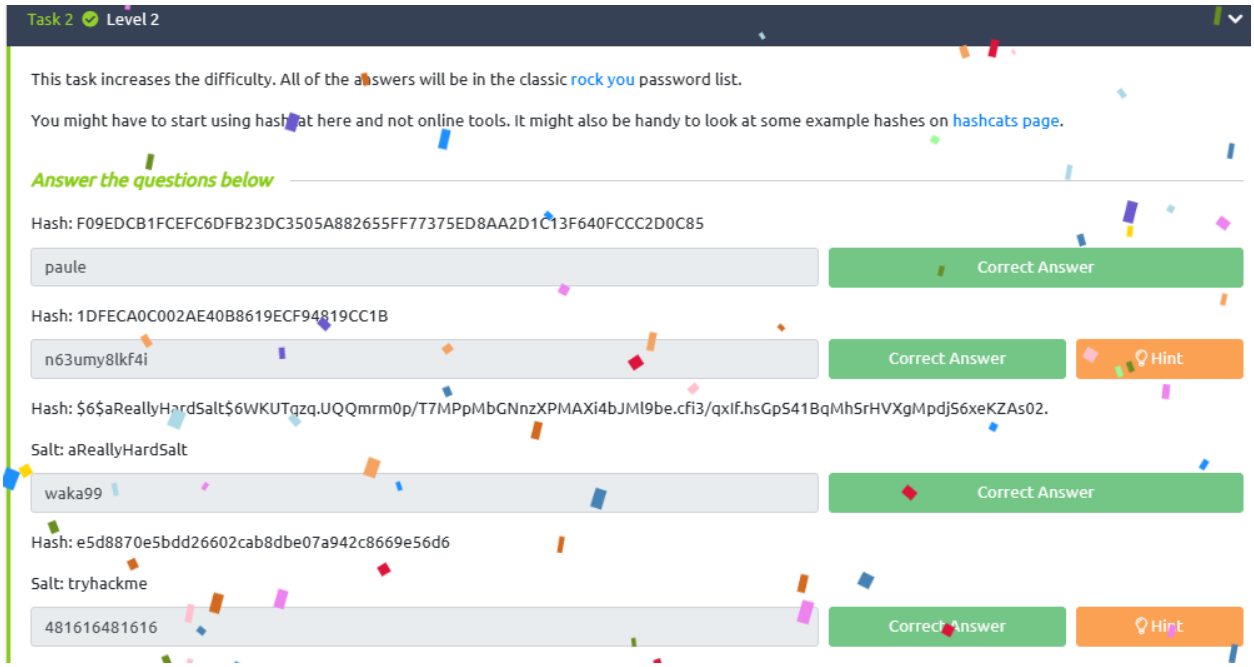
Hash: 6aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.

Salt: aReallyHardSalt



Hash: e5d8870e5bdd26602cab8dbe07a942c8669e56d6

Salt: tryhackme


Task 2 Level 2
This task increases the difficulty. All of the answers will be in the classic rock you password list.
You might have to start using hashcat here and not online tools. It might also be handy to look at some example hashes on hashcats page.
Answer the questions below
Hash: F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85
paule
Correct Answer
Hash: 1DFECA0C002AE40B8619ECF94819CC1B
n63umy8lkf4i
Correct Answer
Hint
Hash: 6aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.
Salt: aReallyHardSalt
waka99
Correct Answer
Hash: e5d8870e5bdd26602cab8dbe07a942c8669e56d6
Salt: tryhackme
481616481616
Correct Answer
Hint