OFFSEC - Hash

Created	@October 15, 2025 12:15 PM
Tags	
Site	

https://tryhackme.com/room/offsecfcil

Introdução

A sala consiste em quebrar cinco hashes:

1. 482c811da5d5b4bc6d497ffa98491e38
2. 861c4f67e887dec85292d36ab05cd7a1a7275228
3. 4149c5cc4c378444d116d65ad5ba4099
4. cdeb746ec095149627348b61d4140fc58b745875 (Salt: satech)
5. 362fda2183b7ac73400a83f6ab2c359451e48adf6c3d46a2963ee2abdf852912

Primeiro Hash

Usando o hashid, sabemos que o algoritmo utilizado foi uma das seguintes opções:

```
┌──(kvothe㉿Viper)-[~]
└─$ hashid -m hash.txt
--File 'hash.txt'--
Analyzing '482c811da5d5b4bc6d497ffa98491e38'
[+] MD2
[+] MD5 [Hashcat Mode: 0]
[+] MD4 [Hashcat Mode: 900]
[+] Double MD5 [Hashcat Mode: 2600]
[+] LM [Hashcat Mode: 3000]
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5 [Hashcat Mode: 8600]
[+] Skype [Hashcat Mode: 23]
[+] Snefru-128
[+] NTLM [Hashcat Mode: 1000]
[+] Domain Cached Credentials [Hashcat Mode: 1100]
[+] Domain Cached Credentials 2 [Hashcat Mode: 2100]
[+] DNSSEC(NSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900]
--End of file 'hash.txt'--
```

Dessa forma, o comando

```
hashcat -a 0 -m 0 hash.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule
```

foi usado para executar um ataque de dicionário com a wordlist rockyou com o ruleset best64, obtendo a senha `password123`.

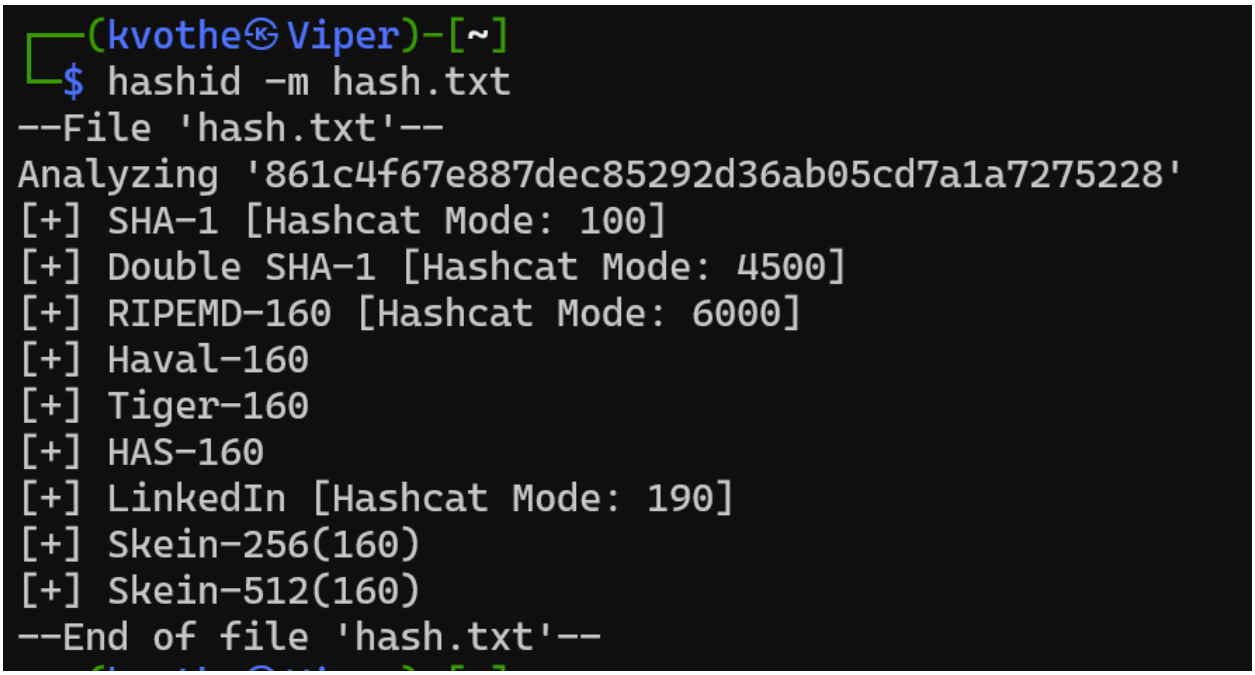
```
482c811da5d5b4bc6d497ffa98491e38:password123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 482c811da5d5b4bc6d497ffa98491e38
Time.Started.....: Wed Oct 15 12:21:21 2025 (0 secs)
Time.Estimated...: Wed Oct 15 12:21:21 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 39876.6 kH/s (4.87ms) @ Accel:256 Loops:77 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 315392/1104517645 (0.03%)
Rejected.........: 0/315392 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> oooooo
Hardware.Mon.#1..: Util: 10%

Started: Wed Oct 15 12:21:20 2025
Stopped: Wed Oct 15 12:21:23 2025
```

Segundo Hash

Usando o hashid para identificar o algoritmo:



Comando usado para realizar um ataque de dicionário:

```
hashcat -a 0 -m 100 hash.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule
```

Resultado do ataque do ataque de dicionário:

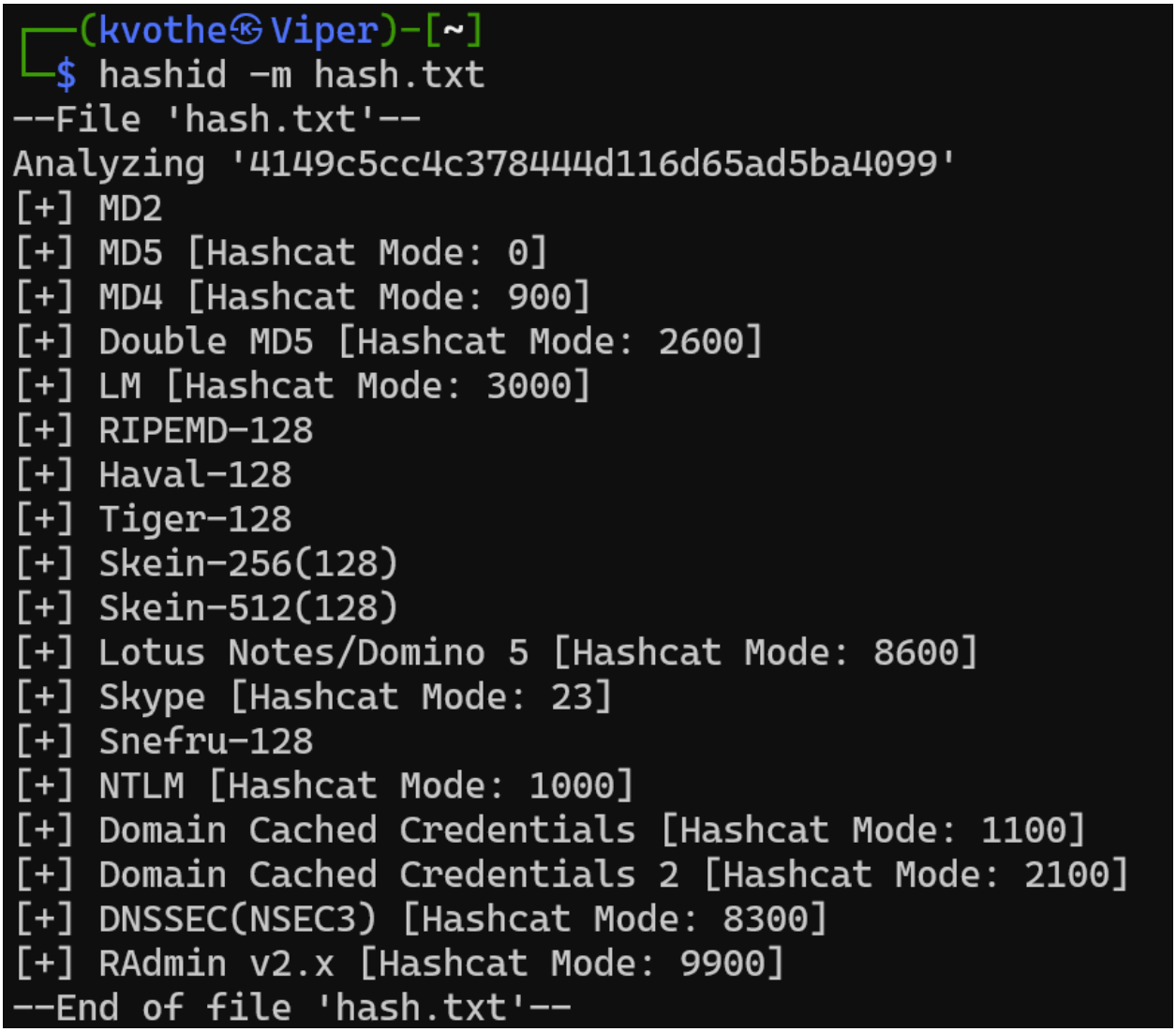
```
861c4f67e887dec85292d36ab05cd7a1a7275228:easy

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 100 (SHA1)
Hash.Target......: 861c4f67e887dec85292d36ab05cd7a1a7275228
Time.Started.....: Wed Oct 15 12:24:57 2025 (0 secs)
Time.Estimated...: Wed Oct 15 12:24:57 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 31840.3 kH/s (3.08ms) @ Accel:128 Loops:77 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 473088/1104517645 (0.04%)
Rejected.........: 0/473088 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: newzealand -> ityoui
Hardware.Mon.#1..: Util:  9%

Started: Wed Oct 15 12:24:56 2025
Stopped: Wed Oct 15 12:24:59 2025
```

Terceiro Hash

Resultado do hashid:



Como na descrição da sala está escrito que cada hash foi feito com diferentes algoritmos, não testamos com o MD5. Primeiramente, realizamos um ataque de dicionário com as palavras da wordlist rockyou com 6 caracteres. Porém, não obtivemos sucesso com nenhum dos algoritmos acima. Então, decidimos fazer um ataque de bruteforce com o comando:

```
hashcat -a 3 -m 900 -1 ?l?u?d hash.txt ?1?1?1?1?1?1
```

quebrando assim o hash:

```
4149c5cc4c378444d116d65ad5ba4099:0ffs3c

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 900 (MD4)
Hash.Target......: 4149c5cc4c378444d116d65ad5ba4099
Time.Started.....: Wed Oct 15 08:44:41 2025 (28 secs)
Time.Estimated...: Wed Oct 15 08:45:09 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?1?1?1?1?1 [6]
Guess.Charset....: -1 ?l?u?d, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   387.3 MH/s (4.42ms) @ Accel:512 Loops:256 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 11351097344/56800235584 (19.98%)
Rejected.........: 0/11351097344 (0.00%)
Restore.Point....: 2949120/14776336 (19.96%)
Restore.Sub.#1...: Salt:0 Amplifier:1536-1792 Iteration:0-256
Candidate.Engine.: Device Generator
Candidates.#1....: GY6mgn -> VDNLZ4
Hardware.Mon.#1..: Util: 75%

Started: Wed Oct 15 08:44:17 2025
Stopped: Wed Oct 15 08:45:11 2025
```

Quarto Hash

Resultado do hashid:

```
┌──(kvothe㉿Viper)-[~]
└─$ hashid -m -e hash.txt
--File 'hash.txt'--
Analyzing 'cdeb746ec095149627348b61d4140fc58b745875:satech'
[+] SHA-1 [Hashcat Mode: 100]
[+] Double SHA-1 [Hashcat Mode: 4500]
[+] RIPEMD-160 [Hashcat Mode: 6000]
[+] Haval-160
[+] Tiger-160
[+] HAS-160
[+] LinkedIn [Hashcat Mode: 190]
[+] Skein-256(160)
[+] Skein-512(160)
[+] MangosWeb Enhanced CMS
[+] sha1(sha1(sha1($pass))) [Hashcat Mode: 4600]
[+] sha1(md5($pass)) [Hashcat Mode: 4700]
[+] sha1($pass.$salt) [Hashcat Mode: 110]
[+] sha1($salt.$pass) [Hashcat Mode: 120]
[+] sha1(unicode($pass).$salt) [Hashcat Mode: 130]
[+] sha1($salt.unicode($pass)) [Hashcat Mode: 140]
[+] HMAC-SHA1 (key = $pass) [Hashcat Mode: 150]
[+] HMAC-SHA1 (key = $salt) [Hashcat Mode: 160]
[+] sha1($salt.$pass.$salt) [Hashcat Mode: 4710]
[+] SMF ≥ v1.1 [Hashcat Mode: 121]
--End of file 'hash.txt'--
```

Como esse hash tem salt, precisamos testar algumas das opções antes de conseguir quebrá-lo. Abaixo, segue o comando usado e o resultado do comando.

```
hashcat -a 0 -m 160 hash.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule
```

```
cdeb746ec095149627348b61d4140fc58b745875:satech:ovelha

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 160 (HMAC-SHA1 (key = $salt))
Hash.Target......: cdeb746ec095149627348b61d4140fc58b745875:satech
Time.Started.....: Wed Oct 15 08:54:36 2025 (1 sec)
Time.Estimated...: Wed Oct 15 08:54:37 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 16554.2 kH/s (2.21ms) @ Accel:128 Loops:38 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 7804928/1104517645 (0.71%)
Rejected.........: 0/7804928 (0.00%)
Restore.Point....: 100352/14344385 (0.70%)
Restore.Sub.#1...: Salt:0 Amplifier:0-38 Iteration:0-38
Candidate.Engine.: Device Generator
Candidates.#1....: p0pcorn -> bi123
Hardware.Mon.#1..: Util: 18%

Started: Wed Oct 15 08:54:34 2025
Stopped: Wed Oct 15 08:54:38 2025
```

Quinto Hash

Resultado do hashid:

```
┌──(kvothe㉿Viper)-[~]
└─$ hashid -m -e hash.txt
--File 'hash.txt'--
Analyzing '362fda2183b7ac73400a83f6ab2c359451e48adf6c3d46a2963ee2abdf852912'
[+] Snefru-256
[+] SHA-256 [Hashcat Mode: 1400]
[+] RIPEMD-256
[+] Haval-256
[+] GOST R 34.11-94 [Hashcat Mode: 6900]
[+] GOST CryptoPro S-Box
[+] SHA3-256 [Hashcat Mode: 5000]
[+] Skein-256
[+] Skein-512(256)
[+] Ventrilo
[+] sha256($pass.$salt) [Hashcat Mode: 1410]
[+] sha256($salt.$pass) [Hashcat Mode: 1420]
[+] sha256(unicode($pass).$salt) [Hashcat Mode: 1430]
[+] sha256($salt.unicode($pass)) [Hashcat Mode: 1440]
[+] HMAC-SHA256 (key = $pass) [Hashcat Mode: 1450]
[+] HMAC-SHA256 (key = $salt) [Hashcat Mode: 1460]
[+] Cisco Type 7
[+] BigCrypt
--End of file 'hash.txt'--
```

Tentamos realizar um ataque de dicionário com a wordlist rockyou, porém não deu certo. Então, decidimos fazer um ataque de bruteforce similar ao do terceiro hash. Segue abaixo o comando e o resultado da execução do comando.

```
hashcat -a 3 -m 1400 -1 ?l?u?d hash.txt ?1?1?1?1?1?1
```

```
362fda2183b7ac73400a83f6ab2c359451e48adf6c3d46a2963ee2abdf852912:sawctf

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: 362fda2183b7ac73400a83f6ab2c359451e48adf6c3d46a2963...852912
Time.Started.....: Wed Oct 15 08:59:34 2025 (5 mins, 42 secs)
Time.Estimated...: Wed Oct 15 09:05:16 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?1?1?1?1?1 [6]
Guess.Charset....: -1 ?l?u?d, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 70628.7 kH/s (6.00ms) @ Accel:256 Loops:128 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 25790873600/56800235584 (45.41%)
Rejected.........: 0/25790873600 (0.00%)
Restore.Point....: 6709248/14776336 (45.41%)
Restore.Sub.#1...: Salt:0 Amplifier:0-128 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: saO26i -> coq0p8
Hardware.Mon.#1..: Util: 75%

Started: Wed Oct 15 08:59:08 2025
Stopped: Wed Oct 15 09:05:18 2025
```

Dessa forma, seguimos para a próxima sala pelo link: https://tryhackme.com/jr/sawctf.

Respostas

1. 482c811da5d5b4bc6d497ffa98491e38 → `password123`
2. 861c4f67e887dec85292d36ab05cd7a1a7275228 → `easy`
3. 4149c5cc4c378444d116d65ad5ba4099 → `0ffs3c`
4. cdeb746ec095149627348b61d4140fc58b745875 (Salt: satech) → `ovelha`
5. 362fda2183b7ac73400a83f6ab2c359451e48adf6c3d46a2963ee2abdf852912 → `sawctf`