



OFFSEC Hash Write-up: Clara

Sinopse

Quebrando hashes, criado pela OFFSEC para a SATECH/UFSC. Dentro deste CTF, o objetivo é identificar o tipo de hash e realizar a sua quebra com hashcat, obtendo, ao final, o link do próximo desafio;

1 Quebra das Hashes

1.1 Hash: 482c811da5d5b4bc6d497ffa98491e38

Utilizando a ferramenta hashid, descobrimos que a hash utilizou a criptografia MD5, dessa forma com o seguinte comando, achamos a resposta desejada.

```
> hashcat -a 0 -m 0 hash.txt /usr/share/wordlists/rockyou.txt
```

```
482c811da5d5b4bc6d497ffa98491e38:password123
Session.....: hashcat
```

Figure 1: Resultado.

1.2 Hash: 861c4f67e887dec85292d36ab05cd7a1a7275228

Utilizando a ferramenta hashid, descobrimos que a hash utilizou a criptografia SHA-1, dessa forma com o seguinte comando, achamos a resposta desejada.

```
> hashcat -a 0 -m 100 hash.txt /usr/share/wordlists/rockyou.txt
```

```
* Bytes.....: 139921507
* Keyspace .. : 14344385
861c4f67e887dec85292d36ab05cd7a1a7275228:easy
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 100 (SHA1)
```

Figure 2: Resultado.

1.3 Hash: 4149c5cc4c378444d116d65ad5ba4099

Utilizando a ferramenta hashid, descobrimos que a hash utilizou a criptografia MD4, porém, diferente das hashes anteriores, temos que usar o modo de brute force para quebra-lá.

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

```
4149c5cc4c378444d116d65ad5ba4099:0ff53c
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 900 (MD4)
Hash.Target.....: 4149c5cc4c378444d116d65ad5ba4099
Time.Started.....: Wed Oct 1 21:41:51 2025 (4 mins, 20 secs)
Time.Estimated...: Wed Oct 1 21:46:11 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Mask.....: ?1?1?1?1?1 [6]
Guess.Charset....: -1 ?l?d?u, -2 N/A, -3 N/A, -4 N/A, -5 N/A, -6 N/A, -7 N/A, -8 N/A
Guess.Queue.....: 1/1 (100.00%)
Speed.#01.....: 41115.8 kH/s (17.65ms) @ Accel:379 Loops:1024 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 11365185184/56800235584 (20.01%)
Rejected.....: 0/11365185184 (0.00%)
Restore.Point....: 2956200/14776336 (20.01%)
Restore.Sub.#01..: Salt:0 Amplifier:1024-2048 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#01...: MZSH9c → m6P2hm
Hardware.Mon.#01.: Util: 77%
```

Figure 3: Resultado.

1.4 Hash: cdeb746ec095149627348b61d4140fc58b745875

Utilizando a ferramenta hashid, descobrimos que a hash utilizou a criptografia HMAC-SHA1, dessa forma com o seguinte comando, achamos a resposta desejada.

```
> hashcat -a 0 -m 150 hash.txt /usr/share/wordlists/rockyou.txt
```

```
$ hashcat -a 0 -m 150 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v7.1.2) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #01: cpu-penryn-11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 2224/4448 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimum salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.
For more information, see https://hashcat.net/faq/potfile

Started: Wed Oct 1 21:57:49 2025
Stopped: Wed Oct 1 21:57:49 2025

(kali@kali)-[~/Downloads]
$ hashcat --show -m 150 hash.txt
cdeb746ec095149627348b61d4140fc58b745875:satech:ovelha
```

Figure 4: Resultado.

1.5 Hash: 362fda2183b7ac73400a83f6ab2c359451e48adf6c3d46a2963ee2abdf852912

Utilizando a ferramenta hashid, descobrimos que a hash utilizou a criptografia SHA2-256, porém, diferente das hashes anteriores, temos que usar o modo de brute force para quebra-lá.

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

```
1310 sha224($pass.$salt) 0cf361904f4b0234c4ade8496d8c11c04e5982db967603e82f22b2f8945246646022084
362fda2183b7ac73400a83f6ab2c359451e48adf6c3d46a2963ee2abdf852912:sawctf
1320 sha224($salt.$pass) 4258a61d3d0d5a5b6796f0ab02d081e998fe657d55d22091d3b51409:36669207
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target.....: 362fda2183b7ac73400a83f6ab2c359451e48adf6c3d46a2963ee2abdf852912
Time.Started.....: Wed Oct 1 22:00:44 2025 (2 mins, 47 secs)
Time.Estimated...: Wed Oct 1 22:03:31 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Mask.....: ?1?1?1?1?1?1
Guess.Charset....: -1 ?l?d -2 N/A, -3 N/A, -4 N/A, -5 N/A, -6 N/A, -7 N/A, -8 N/A
Guess.Queue.....: 1/1 (100.00%)
Speed.#01.....: 9730.14kH/sW (10.89ms) @ Accel:86 Loops:1024 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1710802816/2176782336 (78.59%)
Rejected.....: 0/1710802816 (0.00%)
Restore.Point....: 1319928/1679616 (78.59%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1024 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#01...: sa4noz hvbjkf
Hardware.Mon.#01.: Util: 94%
1710 sha512($pass.$salt) e5c3ede3e49fb86592fb03f471c35ba13e8d89b8ab65142c9a8fda1b635fa2223c24e5558f
Started: Wed Oct 1 22:00:25 2025
Stopped: Wed Oct 1 22:03:31 2025
1730 sha512(utf16le($pass).$salt) 13070359002b6fbb3d28e50fba55efcd3d7cc115fe6e3f6c98bf0e3210f1c6923427a1e1a31
```

Figure 5: Resultado.

Dessa forma, achamos o link para o próximo ctf. E assim termina o OFFSEC Hash do CTF da satech 2025.