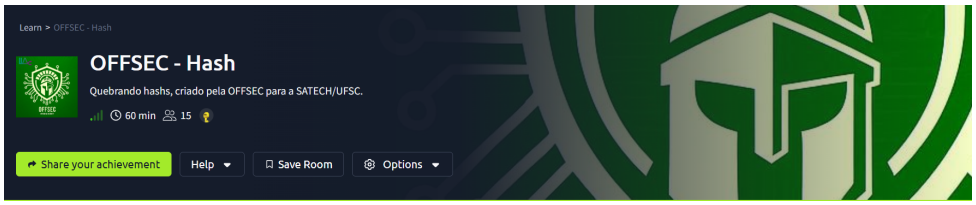

OFFSEC Hash Write-up: Clara

Sinopse

Quebrando hashs, 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
```

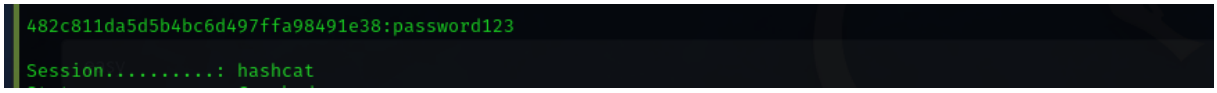

Figure 1: Resultado.

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
```

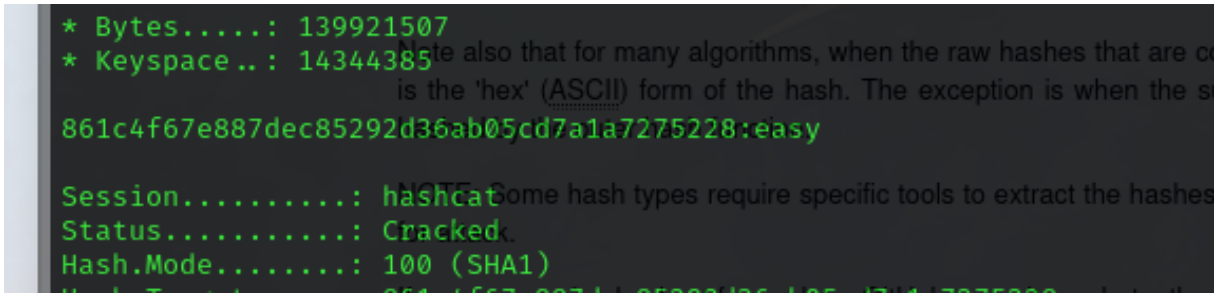

Figure 2: Resultado.

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
```

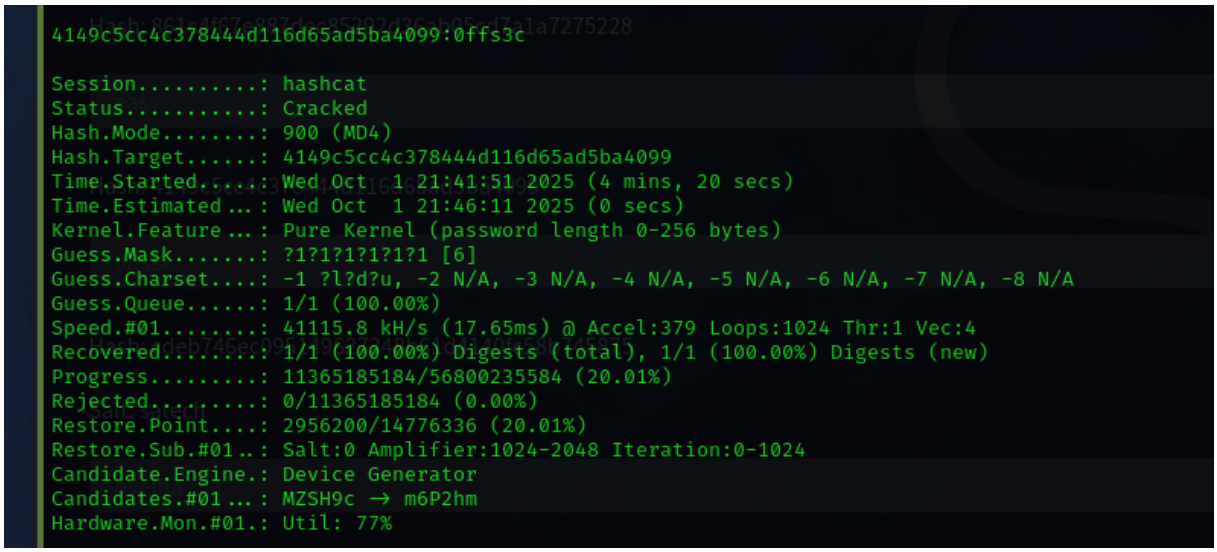

Figure 3: Resultado.

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
```

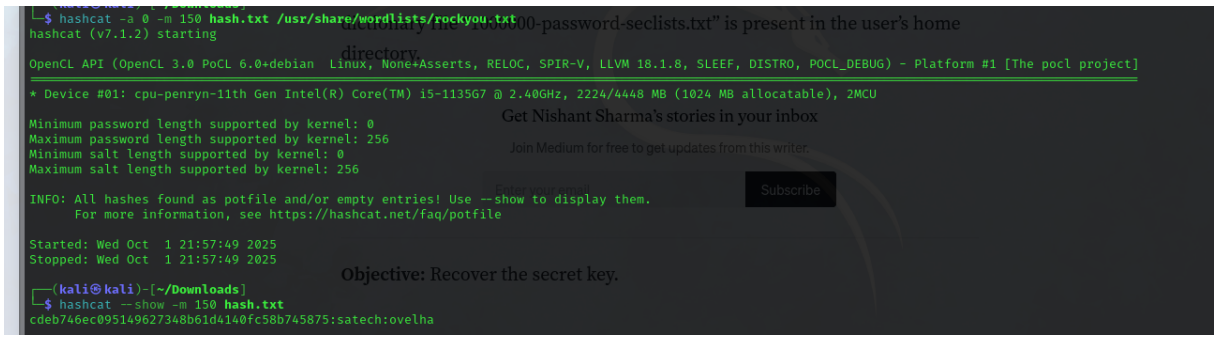

Figure 4: Resultado.

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
```

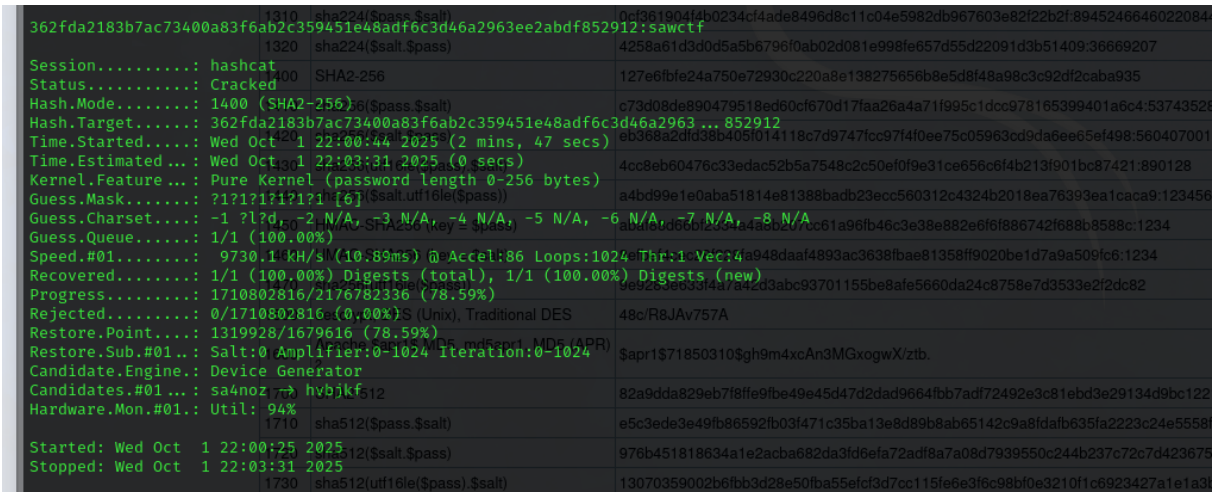

Figure 5: Resultado.

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