Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Crack the Hash – Tryhackme

|  |  |
| --- | --- |
| Informações do documento | |
| Referência | Crack the Hash – Artur Adam de Oliveira |
| N° Revisão | 1 |
| Data de publicação | 21/09/2025 |
| Link | <https://tryhackme.com/room/crackthehash> |

|  |  |  |
| --- | --- | --- |
| Redação | Artur Adam de Oliveira | Estudante |
| Revisão | Alexandre Gualiume Coruquieri | Coordenador |
| Aprovação | Alexandre Gualiume Coruquieri | Coordenador |

|  |  |  |
| --- | --- | --- |
| Histórico de revisões | | |
| N° | Entregas | Descrição |
| 0 | 20/09/2025 | Produção |
| 1 | 30/10/2025 | Revisão |
| 2 | 31/10/2025 | Aprovação |

|  |  |
| --- | --- |
| Informações do CTF | |
| Nível de Dificuldade | Fácil |
| Tipo de acesso | Gratuito |
| Conceitos envolvidos | Hash, HashCat |
| Plataforma | Tryhackme |
| Área | Red |

Sumário

[Sumário 2](#_Toc212736289)

[Contextualização 2](#_Toc212736290)

[Desenvolvimento 3](#_Toc212736291)

[Level 1 3](#_Toc212736292)

[Level 2 8](#_Toc212736293)

[Conclusão 14](#_Toc212736294)

[Referências 14](#_Toc212736295)

Contextualização

Crack the Hash é um CTF extremamente simples que pode ser amplamente utilizado para o aprendizado e compreensão de Hashes e como quebrá-los. Sendo separado em dois níveis, o primeiro para hashes simples e o segundo para hashes que podem requerer a utilização de softwares como HashCat.

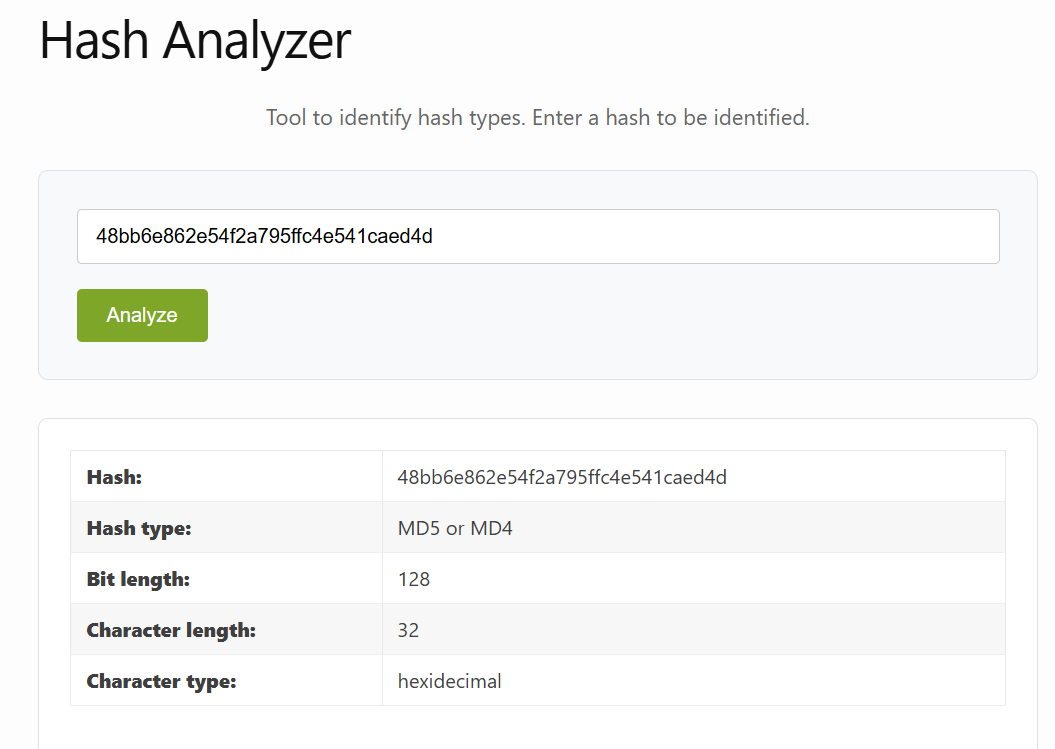
Desenvolvimento

Level 1

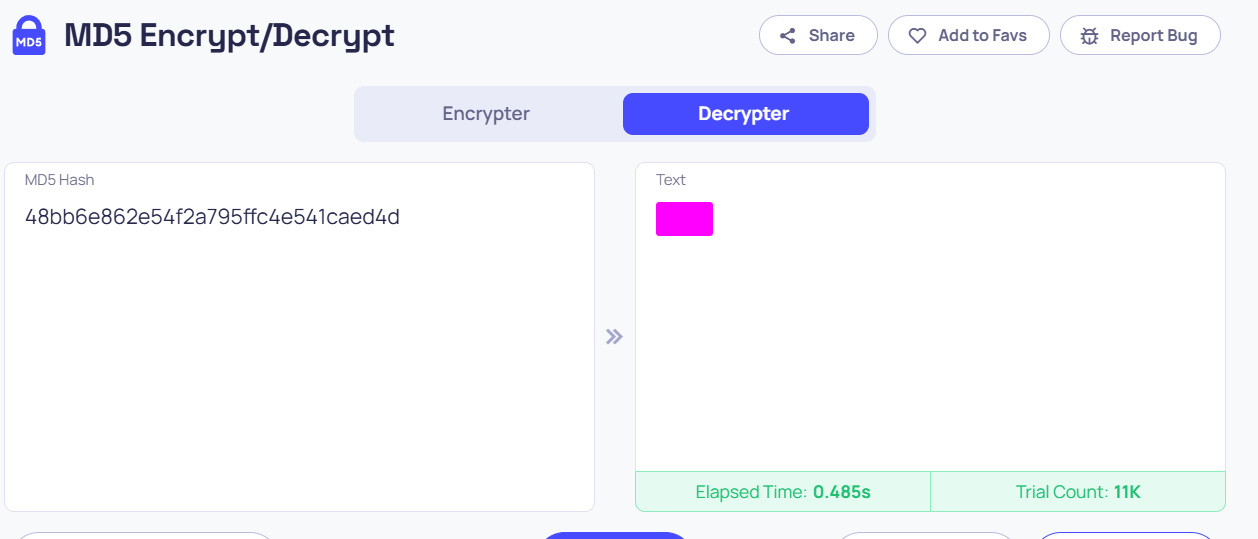
Para obter a solução de todos os hashes deste nível é necessário apenas verificar dois sites, o primeiro é o <https://www.tunnelsup.com/hash-analyzer> um site criado para identificar a tipagem de um Hash dentre os Hashes mais comuns. O segundo é <https://10015.io/tools/md5-encrypt-decrypt> que permite realizar a decifração de diversos tipos de hash.

**48bb6e862e54f2a795ffc4e541caed4d:**

Primeiramente coloque no site TunnelSup e descubra o tipo de hash:

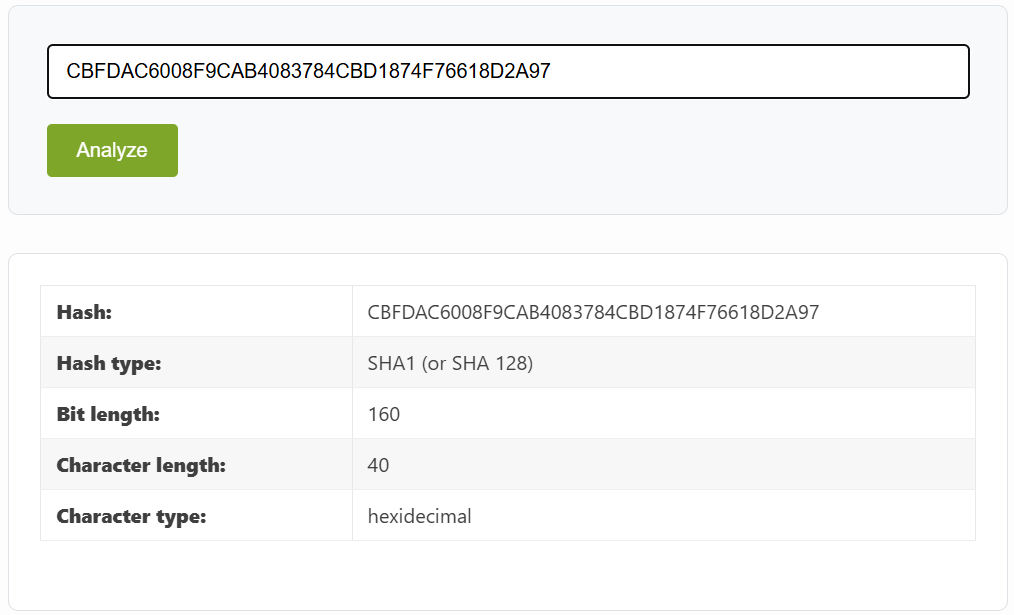


Após isso utilize o 1OOL5 para decifrar:

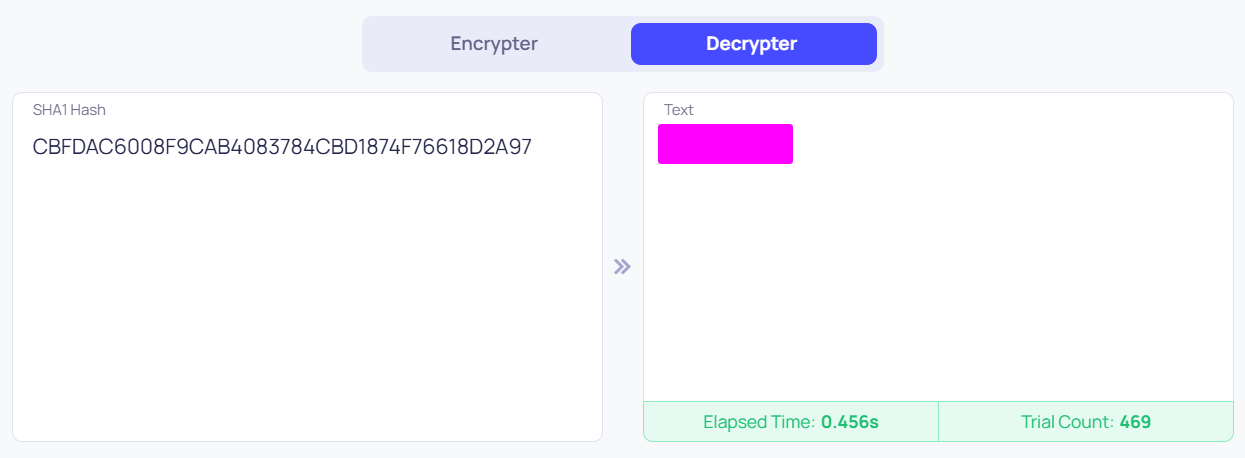


**CBFDAC6008F9CAB4083784CBD1874F76618D2A97:**

Primeiramente coloque no site TunnelSup e descubra o tipo de hash:

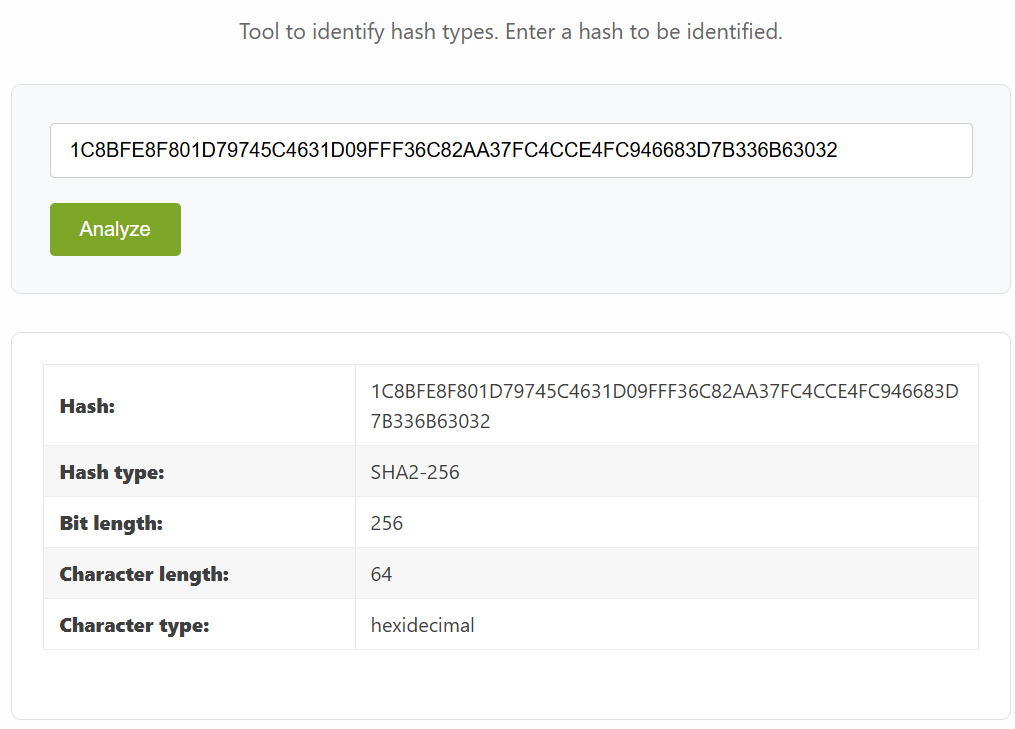


Após isso utilize o 1OOL5 para decifrar:

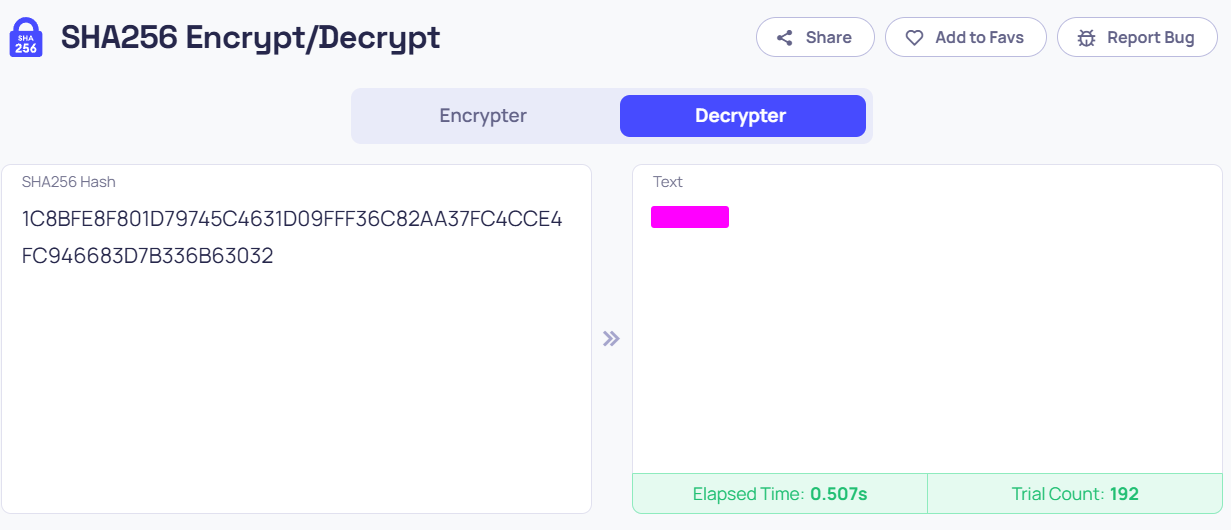


**1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032:**

Primeiramente coloque no site TunnelSup e descubra o tipo de hash:

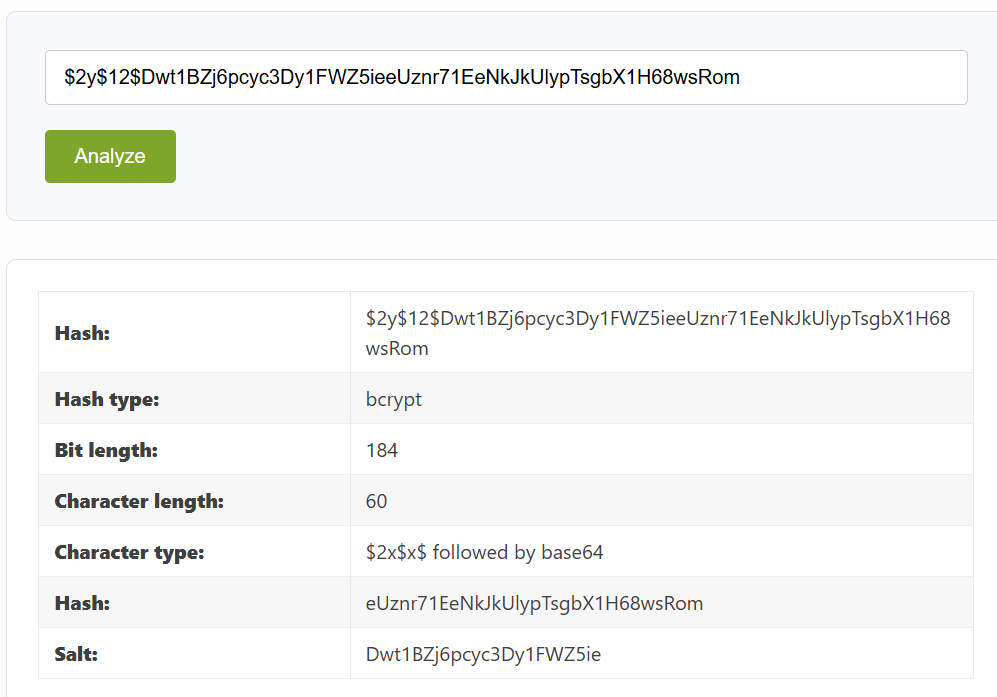


Após isso utilize o 1OOL5 para decifrar:

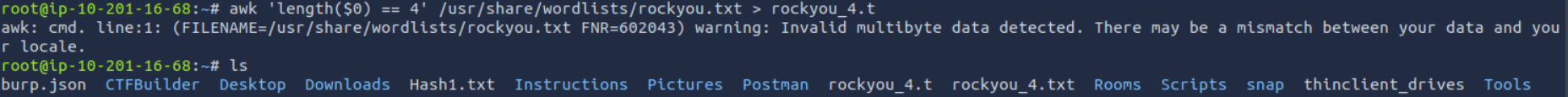


**$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom:**

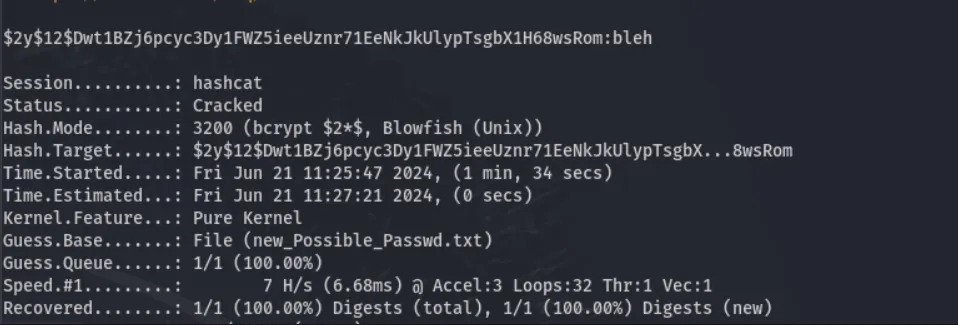
Primeiramente coloque no site TunnelSup e descubra o tipo de hash:



Este tipo de Hash não pode ser encontrado no site que tem sido utilizado até este momento para poder solucionar este Hash o transfira para um arquivo em sua máquina e encurte a lista “rockyou.txt” para que utilize apenas senhas de 4 caracteres com o comando **awk ‘length($0) == 4' rockyou.txt > [Nome\_do\_Arquivo\_Rock]**

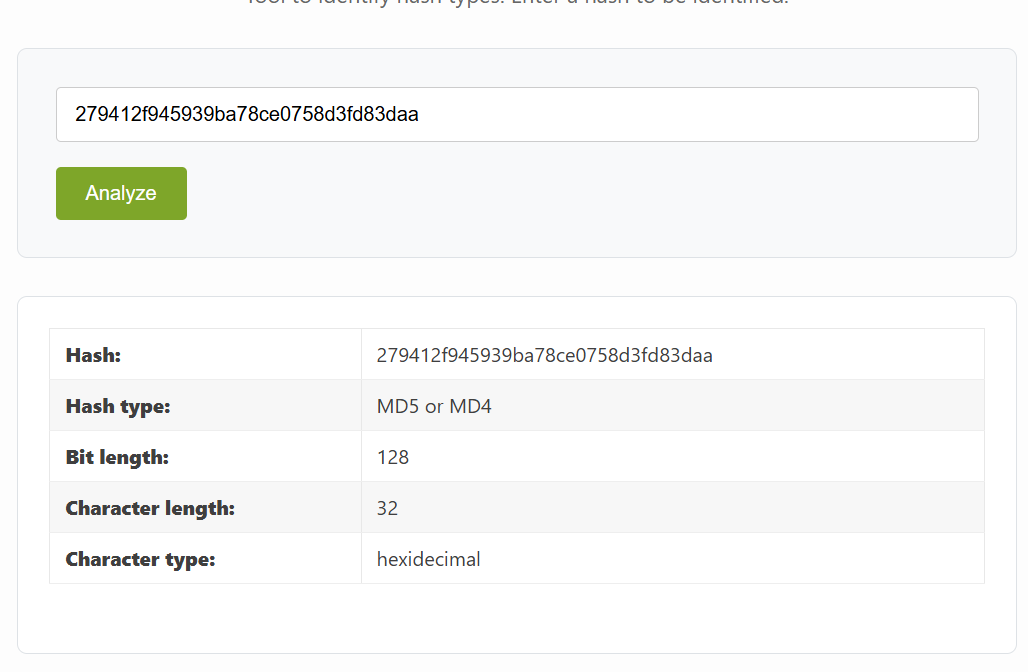


Agora utilize o seguinte comando de HashCat **hashcat -a 0 -m 3200 [Arquivo\_Hash] [Nome\_do\_Arquivo\_Rock] --force** que irá resultar na senha sendo devolvida.

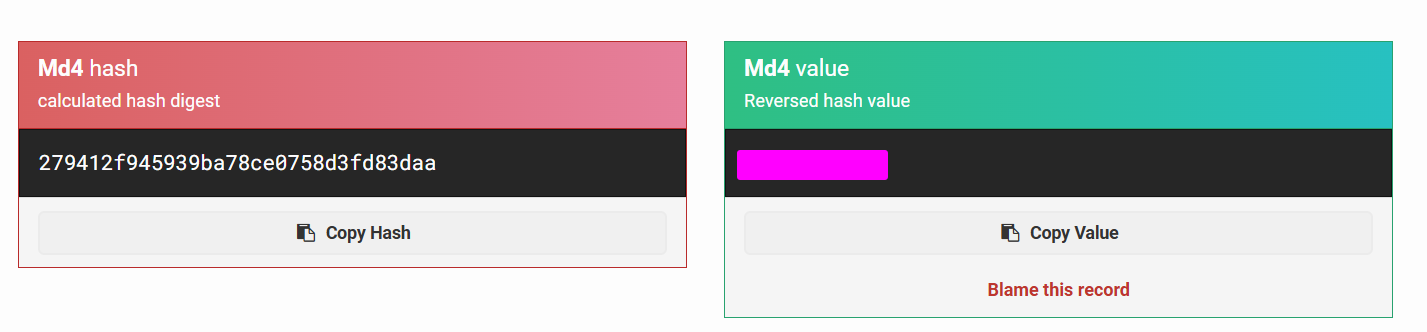


**279412f945939ba78ce0758d3fd83daa:**

Primeiramente coloque no site TunnelSup e descubra o tipo de hash:



Pode se ver que semelhante aos 3 primeiros exercícios este é um tipo de Hash comum, deste modo apenas coloque o hash em um decifrador e obtenha a resposta:

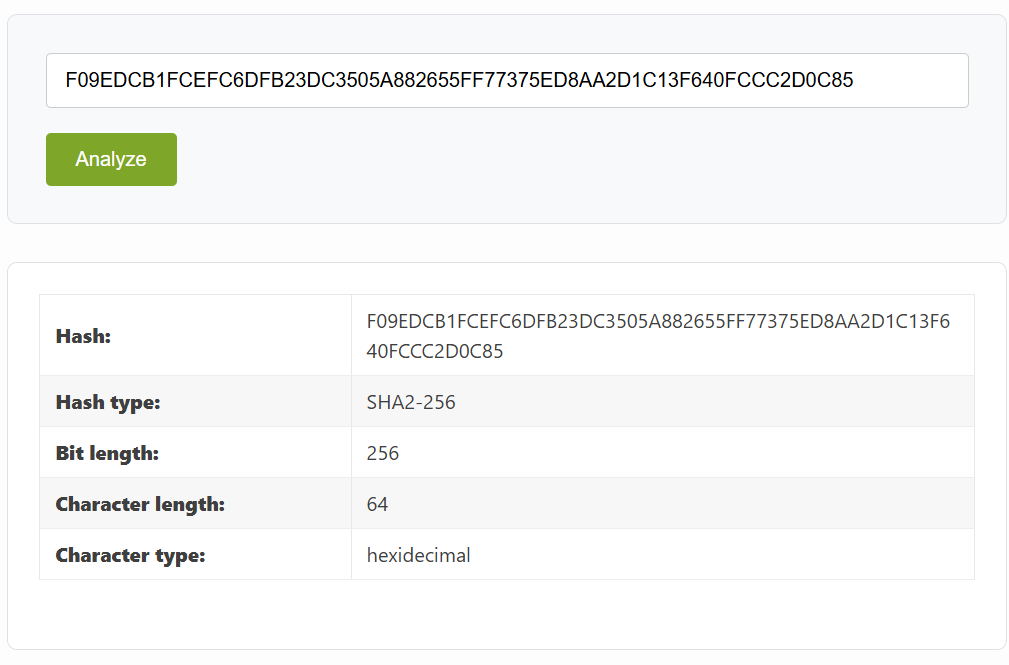


Level 2

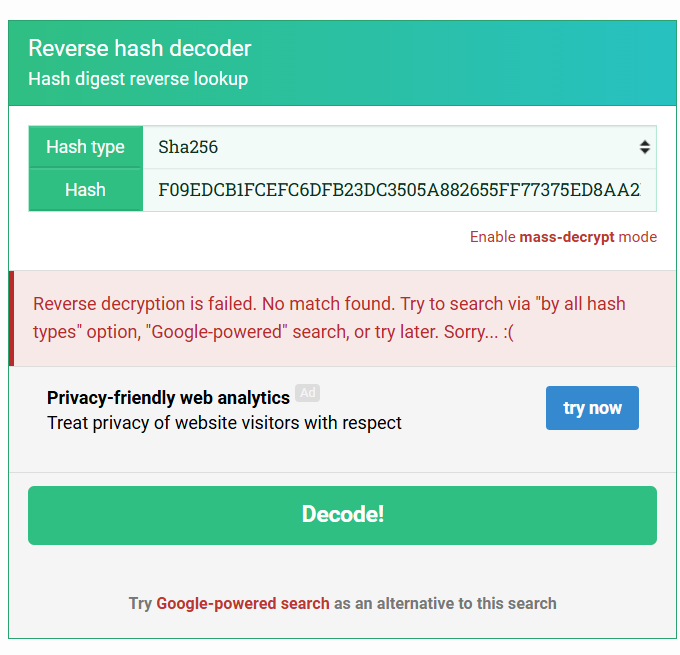
A partir deste ponto as perguntas se tornam mais difíceis em sua solução, embora a estrutura siga o mesmo padrão anterior.

**F09EDCB1FCEFC6DFB23DC3505A882655FF77375ED8AA2D1C13F640FCCC2D0C85:**

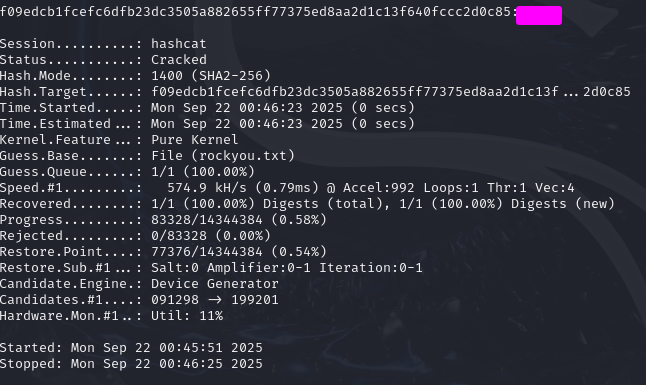
Como nos exercícios passados primeiramente verifique o tipo de Hash utilizado:



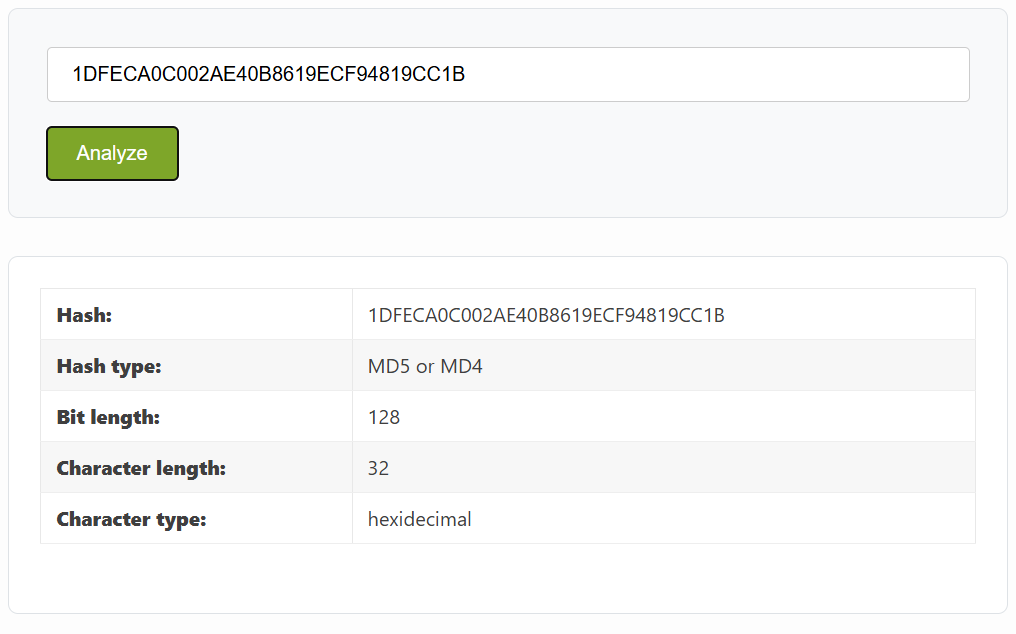
Porém ao tentar utilizar os decifradores online, eles se mostram incapazes de quebrar o Hash:



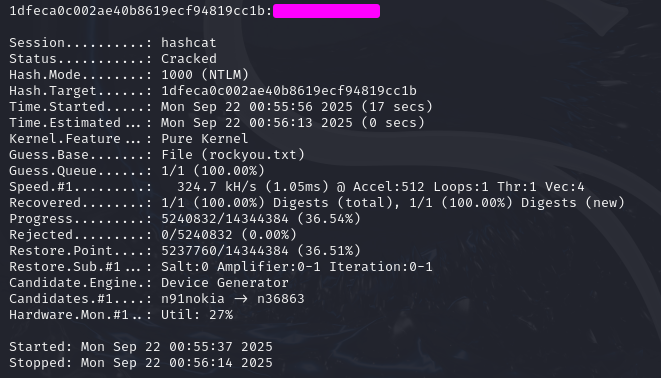
Para quebrar o Hash será utilizado o hashcat, novamente crie um arquivo com o Hash em sua máquina e utilize o seguinte comando: **hashcat -a 0 -m 1400 [Arquivo\_Hash] rockyou.txt** isso irá gerar o resultado desejado:



**1DFECA0C002AE40B8619ECF94819CC1B:**

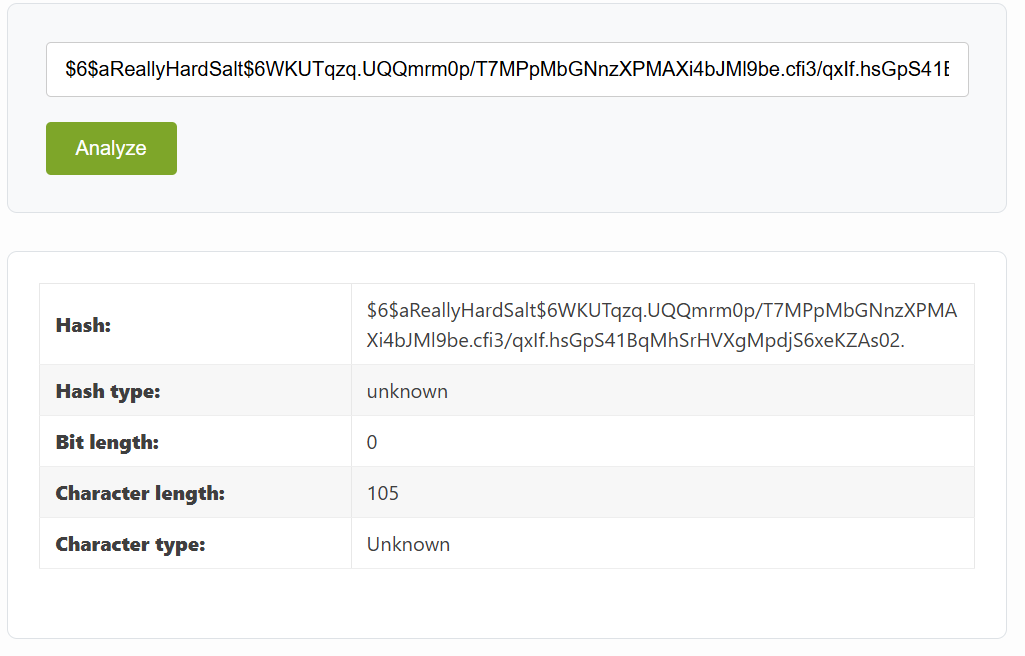
Primeiramente identifique o Hash 

Neste caso em específico infelizmente o identificador de Hash não está correto, o tipo deste Hash é na realidade um Hash NTLM, para quebrar este Hash específico utilize o comando: hashcat -a 0 -m 1000 [Arquivo\_Hash] rockyou.txt e deste modo pode ser obtido o resultado desejado:

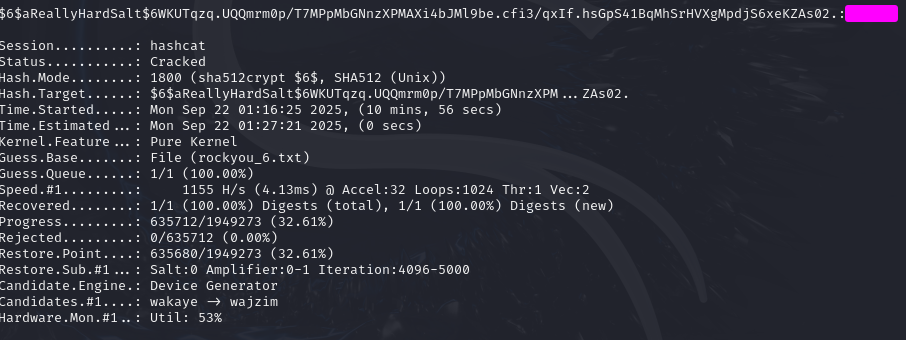


**$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.:**

Salt: aReallyHardSalt

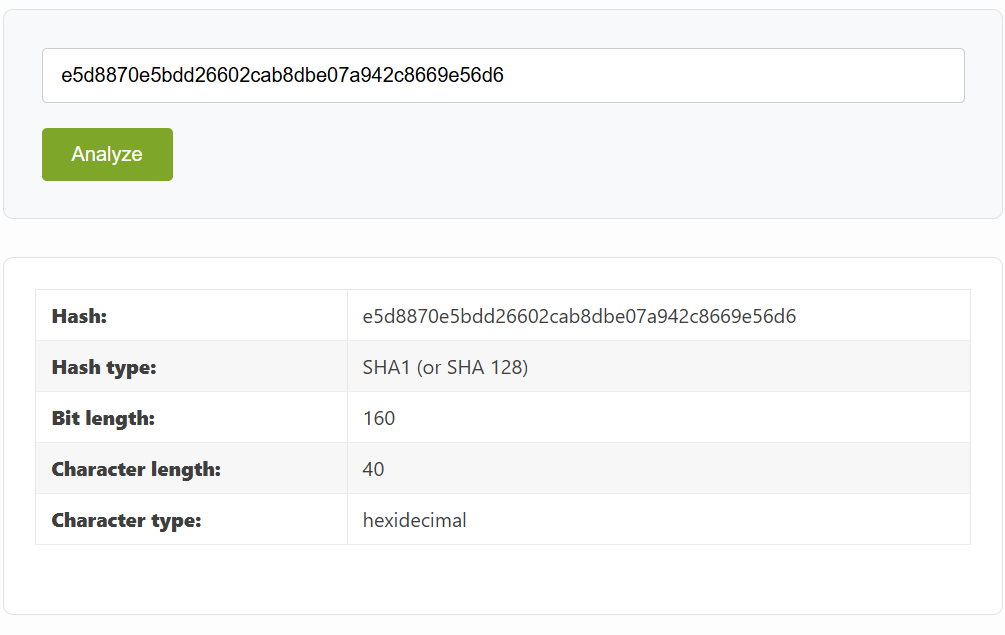
Desta vez o Hash possui um Salt fazendo com que o código normalmente utilizado para descriptografar este Hash não irá funcionar corretamente, além de fazer com que a tipagem não possa ser descoberta pelo site:

Porém pode ser encontrado o tipo de Hash ao analisar o modo que este Hash foi armazenado, o $6$ é o tipo do código, para descobrir qual especificamente, vá até o site <https://github.com/unstable-deadlock/brashendeavours.gitbook.io/blob/master/pentesting-cheatsheets/hashcat-hash-modes.md> que possui todos códigos -m para tipos de Hash, e ao observar a sessão de exemplos é possível notar que o código sendo utilizado é um SHA512

Agora, utilizando o novo código para o -m é possível encontrar a resposta através do comando: **hashcat -a 0 -m 1800 [Arquivo\_Hash] rockyou.txt**:

**e5d8870e5bdd26602cab8dbe07a942c8669e56d6:**

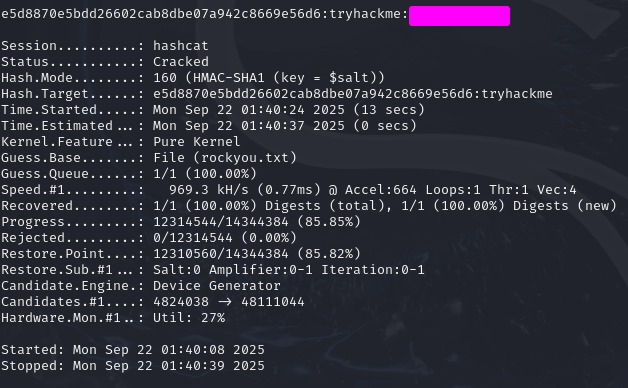
Salt: tryhackme

Assim como no último exercício existe um Salt para este Hash, para solucionar esta questão primeiro veja se é possível descobrir sua tipagem:

Sabendo que o tipo é SHA1 pode se procurar na base de Hashes para qual código -m melhor se adapta a este tipo:

Os códigos 100 - 150 não são próprias pois possuí-se apenas o salt, é importante notar que o Hash **DEVE** ter o salt em seguida no arquivo do Hash como demonstrado abaixo:



Feito isso coloque o seguinte código pode-se decifrar o Hash: **hashcat -a 0 -m 160 [Arquivo\_Hash] rockyou.txt**:

E assim está concluído este CTF.

Conclusão

Este é um ótimo CTF para aqueles que desejam se acostumar e aprender mais sobre o uso e funcionamento de Hashes e como elas podem ser quebradas e decifradas

Referências

<https://www.tunnelsup.com/hash-analyzer>

<https://md5hashing.net/hash/md4/279412f945939ba78ce0758d3fd83daa>

<https://github.com/unstable-deadlock/brashendeavours.gitbook.io/blob/master/pentesting-cheatsheets/hashcat-hash-modes.md>