Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Hashcrack – PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Hashcrack – Isabela Tamie Miyazato |
| **N° Revisão** | 1 |
| **Data de publicação** | DD/MM/AAAA |
| **Link** | [hashcrack](https://play.picoctf.org/practice/challenge/475?page=1&search=cr) |

|  |  |  |
| --- | --- | --- |
| **Redação** | Isabela Tamie Miyazato | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Orientador |
| **Aprovação** | Sérgio Guidi Trovo | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 07/09/2025 | Produção |
| **1** | 30/10/2025 | 1ª Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil, Médio ou Difícil |
| **Tipo de acesso** | Gratuito ou Pago |
| **Conceitos envolvidos** | Conceitos envolvidos no CTF |
| **Plataforma** | Tryhackme, PicoCTF ou HackTheBox |
| **Área** | Red ou Blue |

**Sumário**

[Contextualização 3](#_lz46fn7zw38k)

[Subtítulo caso necessário 3](#_yg3m0hnza1yl)

[Desenvolvimento 3](#_163vg3lu1f0n)

[Pergunta 1 3](#_50xig5m5j0a7)

[Pergunta 2 3](#_3qd9v6mcot0n)

[Pergunta 3 3](#_fi4xucy0wd53)

[Pergunta N 3](#_kgme1xamuy74)

[Conclusão 3](#_ihbsrvi4vcav)

[Referências 3](#_ep6yrjc7nwj4)

**Contextualização**

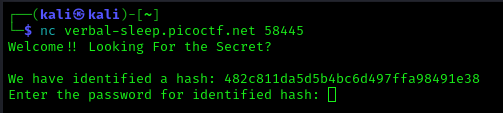
Aqui se encontram as informações básicas do CTF.

**Subtítulo caso necessário**

Espaço de tópico extra caso necessário

**Desenvolvimento**

**Pergunta 1**



É necessário descobrir a senha que corresponde à esse hash para passar para a próxima parte. Para descobrir ela, foi utilizado o JohnTheRipper.

### **O que é JohnTheRipper?**

JohnTheRipper é uma ferramenta poderosa para quebrar hashes de senha.

Com uma lista de senhas comuns (como por exemplo, a rockyou.txt) é possível tentar adivinhar a senha que corresponde ao hash com o método Rainbow Table.

**O que é Rainbow Table?**

Uma tabela arco-íris é uma tabela pré-computada para reverter funções hash criptográficas, geralmente para quebrar hashes de senhas,

john --wordlist=rockyou.txt hash.tx

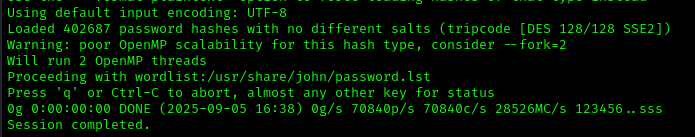
* --wordlist=rockyou.txt

Especifica o uso de um dicionário (wordlist) chamado "rockyou.txt"

* hash.txt

Arquivo que contém os hashes MD5 que você quer quebrar

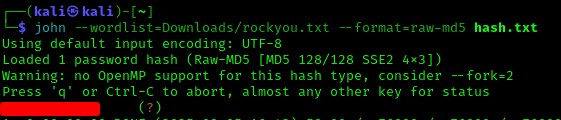
Porém, tentando com esse comando, o JohnTheRipper tem certa dificuldade em encontrar a resposta.



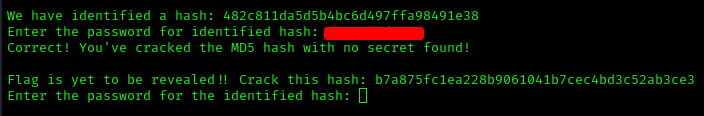
Para facilitar o trabalho dele, utilize um comando que o ajude a identificar o tipo de hash utilizado nele:

hash-identifier



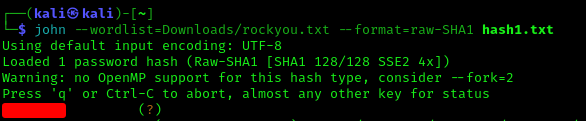
Sabendo disso, é possível encontrar a senha pelo John:  


**Pergunta 2**

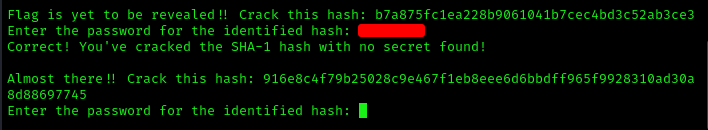


Utilizando de novo a ferramenta de detecção de hash:

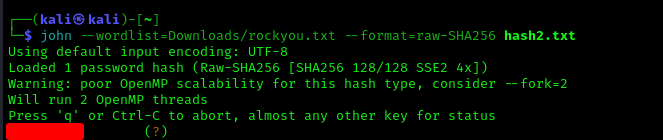


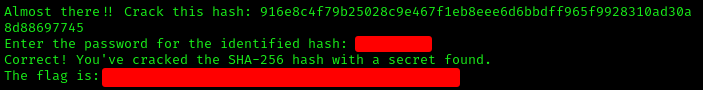


**Pergunta 3**









**Conclusão**

Considerações finais a respeito do CTF.

**Referências**

Caminho dos materiais utilizados para a solução do CTF.