Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Anonforce - TryHackMe

| **Informações do documento** | |
| --- | --- |
| **Referência** | Anonforce – Gustavo Fernandes Arantes Maluta |
| **N° Revisão** | 1 |
| **Data de publicação** | 18/10/2025 |
| **Link** | https://tryhackme.com/room/bsidesgtanonforce |

| **Redação** | Gustavo Fernandes Arantes Maluta | Estudante |
| --- | --- | --- |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

| **Histórico de revisões** | | |
| --- | --- | --- |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

| **Informações do CTF** | |
| --- | --- |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | FTP, Brute Force, john, gpg2john |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

user.txt [3](#_heading=h.3znysh7)

root.txt4

[Conclusão](#_heading=h.1t3h5sf) 7

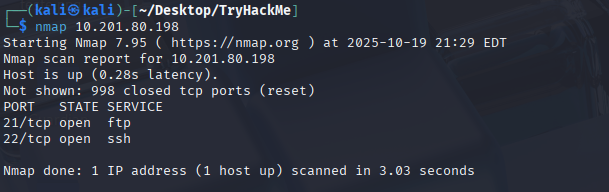
**Contextualização**

O CTF Anonforce é um desafio simples no qual é possível treinar aspectos muito utilizados como exploração do serviço FTP e quebra de hash code.

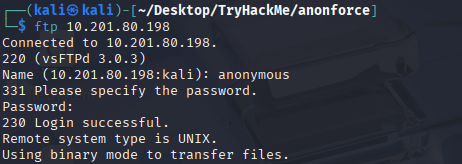
**Desenvolvimento**

**user.txt**

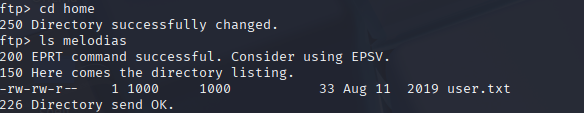
Utilizei o comando nmap para verificar os serviços que estão rodando no servidor.



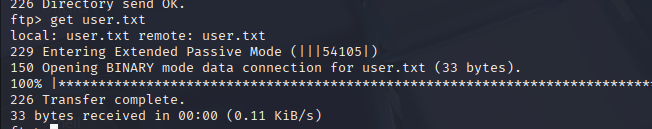
Acesse o serviço FTP como anonymous.



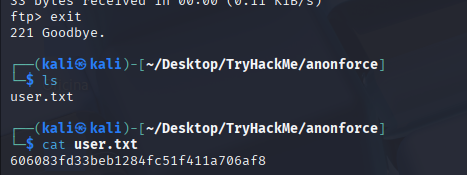
Ao acessar o diretório /home/melodias, encontrei o arquivo use.txt.



Utilizei o comando get, para baixar o arquivo.

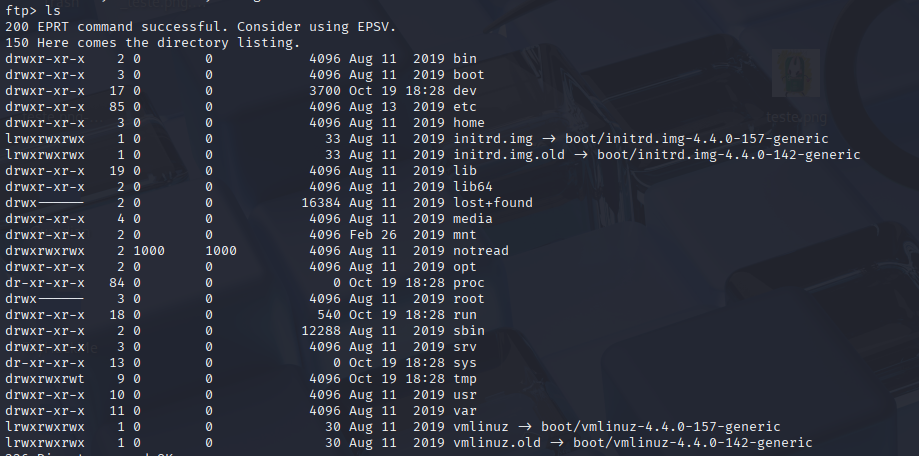


Saindo do FTP e utilizando o comando cat para verificar o conteudo.

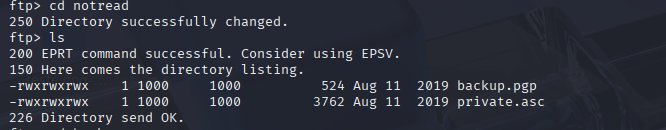


**root.txt**

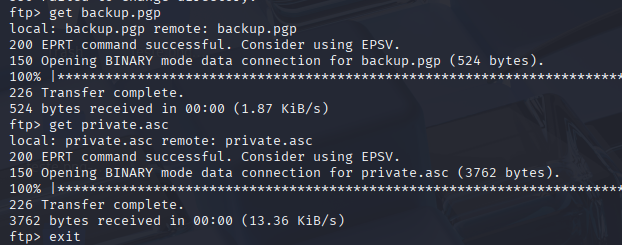
Acesse novamente o FTP como anonymous e encontrei um arquivo estranho.



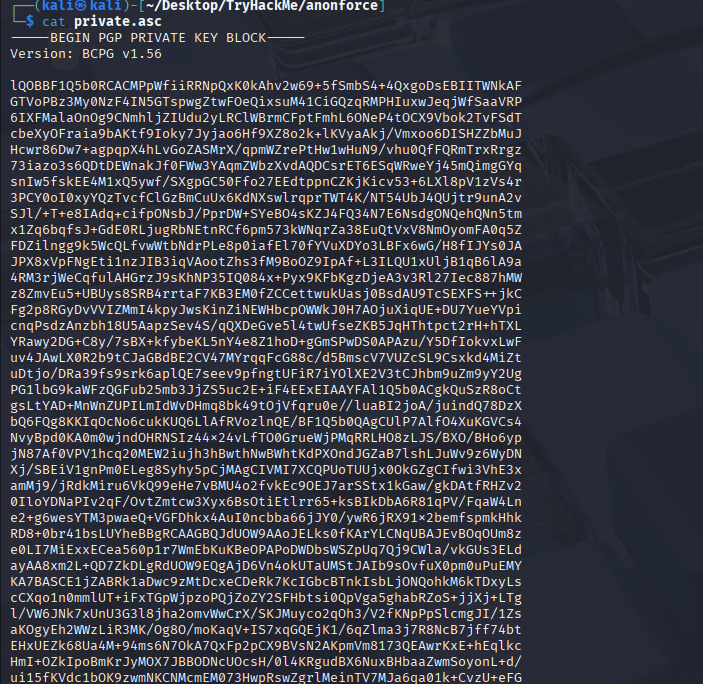
Acesse o diretório “notread”.



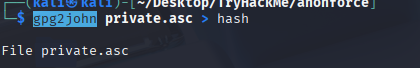
Utilize o comando get para pegar ambos os arquivo.



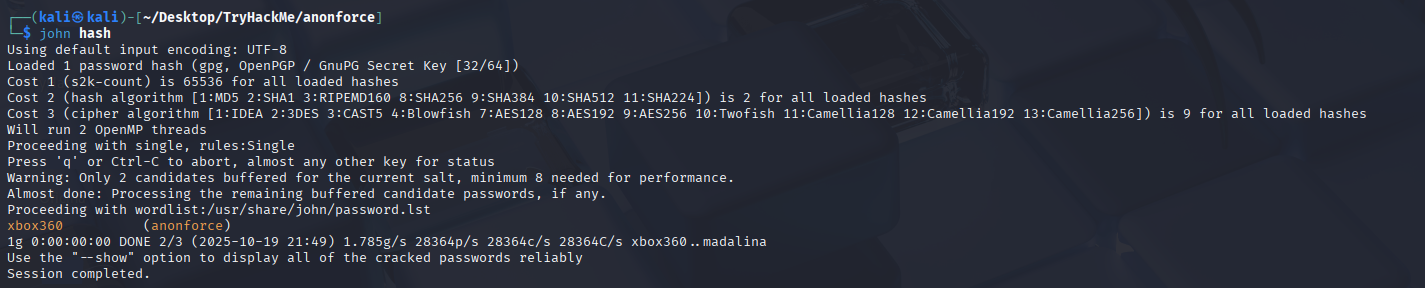
Verificando o conteúdo do arquivo descobri que em um deles contem uma chave criptografada.



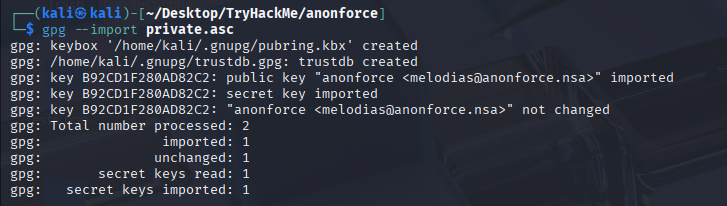
Utilizei o comando gpg2john para transformar essa chave em um arquivo no qual a ferramenta John consiga ler.



Utilizei a ferramenta john para descriptografar a chave.



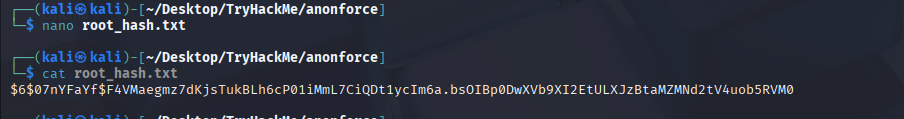
Importei a chave utilizando o comando gpg.

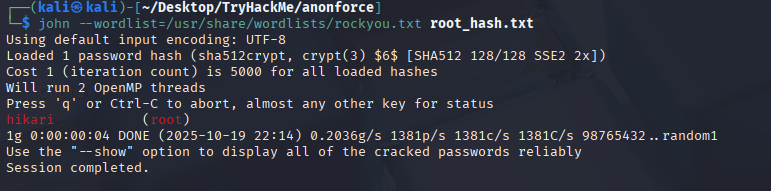


Utilizando novamente o comando gpg, consegui acessar o conteúdo do arquivo “backup.pgp”, no qual contem o conteúdo de um arquivo shadow.

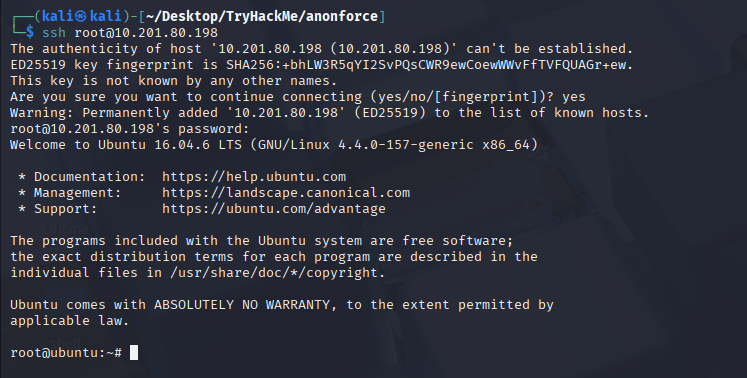


Pegando o hash referente ao acesso root do servidor e utilizando com o john, consegui acessar o servidor.

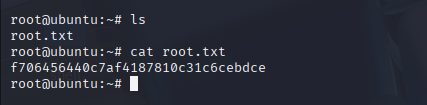




Acesse o servidor SSH como root.



Utilizando o comando ls e cat consegui achar o root.txt.



**Conclusão**

Nesse CTF utilizei conceitos simples de exploração do serviço FTP, quebra de hash com o john.