Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

| **Informações do documento** | |
| --- | --- |
| **Referência** | CTF de estudo – Nome do realizador |
| **N° Revisão** | 1 |
| **Data de publicação** | 07/09/2025 |
| **Link** | Link para acessar o CTF |

| **Redação** | Artur Adam de Oliveira | Estudante |
| --- | --- | --- |
| **Revisão** | Artur Adam de Oliveira | Orientador |
| **Aprovação** | Artur Adam de Oliveira | Diretor |

| **Histórico de revisões** | | |
| --- | --- | --- |
| **N°** | **Entregas** | **Descrição** |
| **0** | 03/09/2025 | Produção |
| **1** | 07/09/2025 | Revisão |
| **2** | 07/09/2025 | Aprovação |

| **Informações do CTF** | |
| --- | --- |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Nmap, brute force, escalonamento de privilégios |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_6qoij54v5sqf)

[Subtítulo caso necessário 3](#_feojg7bwtjq)

[Desenvolvimento 3](#_9baz6o4larfs)

Find Open ports in the Machine [3](#_roudyfuxi4z4)

Who wrote the Task list? [3](#_3sftt3j6hc2v)

What service can you bruteforce with the text file found? [3](#_kr95zn1dn60t)

What is the User Password? 3

User.txt 3

Root.txt [3](#_fpr81z76bli6)

[Conclusão 3](#_rqyqteb4ou70)

[Referências 3](#_jvcyswj2e7zc)

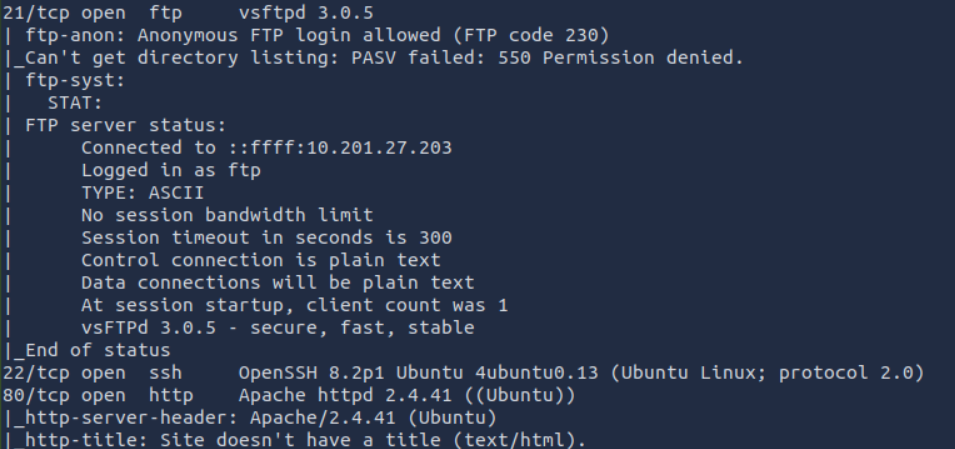
**Contextualização**

Bounty Hacker é um CTF simples que tem sua trama baseada no anime cowboy bebop, o CTF utiliza conceitos como brute force e escalonamento de privilégios para com o objetivo de obter as chaves existentes nos arquivos User.txt e Root.txt

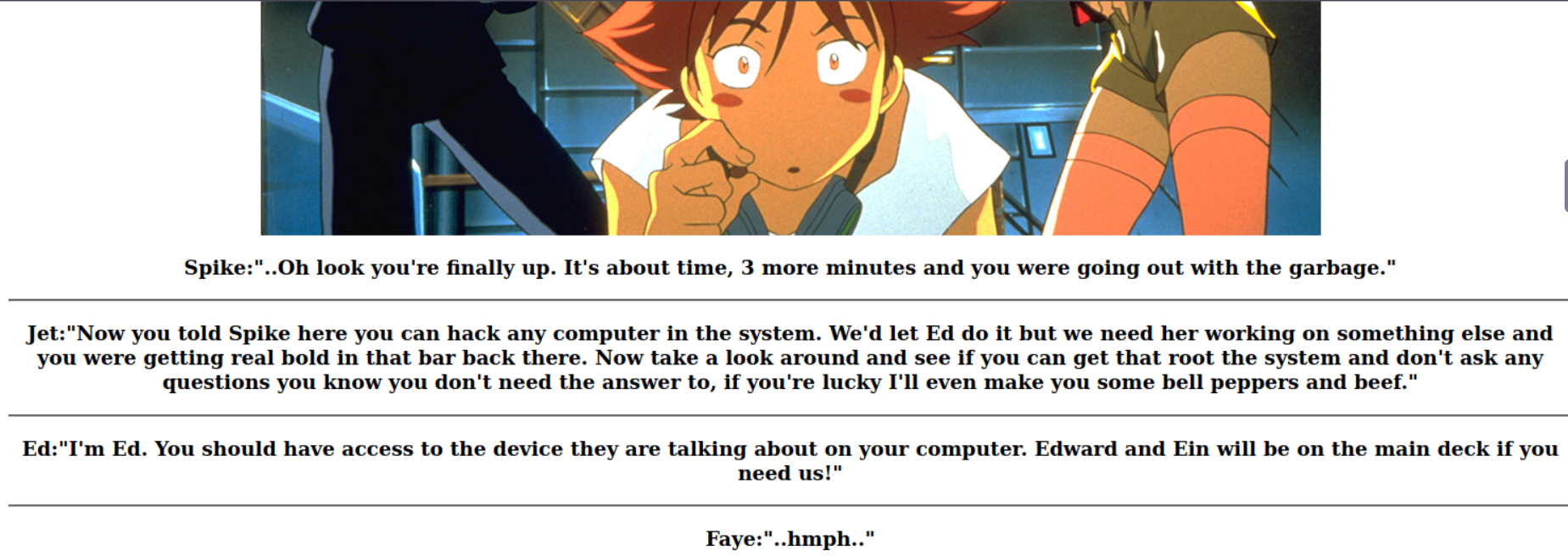
**Desenvolvimento**

**Find open ports on the machine**

Para solucionar esta questão necessita-se apenas utilizar o comando **nmap -A -T4 [IP\_da\_máquina]** para encontrar as portas abertas:

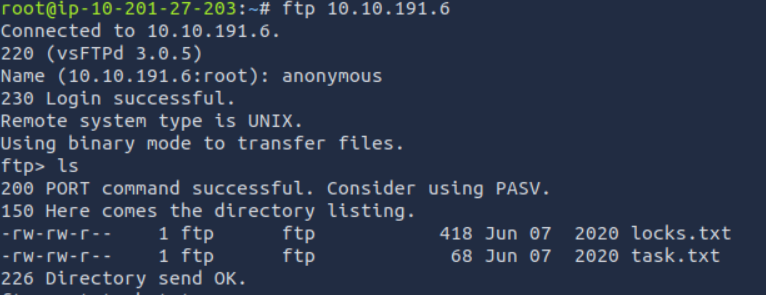


Pode-se ver que este IP possui uma port FTP e uma port HTTP abertas, checando a port HTTP se encontra um site simples que indica que sua tarefa é conseguir acesso ao sistema root

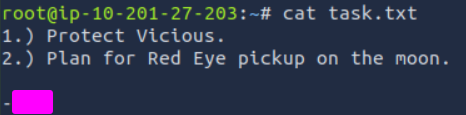


**Who wrote the task list?**

Para acessar o FTP é necessário utilizar o comando **ftp [IP\_da\_máquina]** e colocar o nome como **anonymous** e será possível acessar os conteúdos do FTP:



Utilize o comando **get** em ambos arquivos para copiá-los em sua máquina e dessa forma, ao ver a lista task.txt se descobre quem a escreveu:

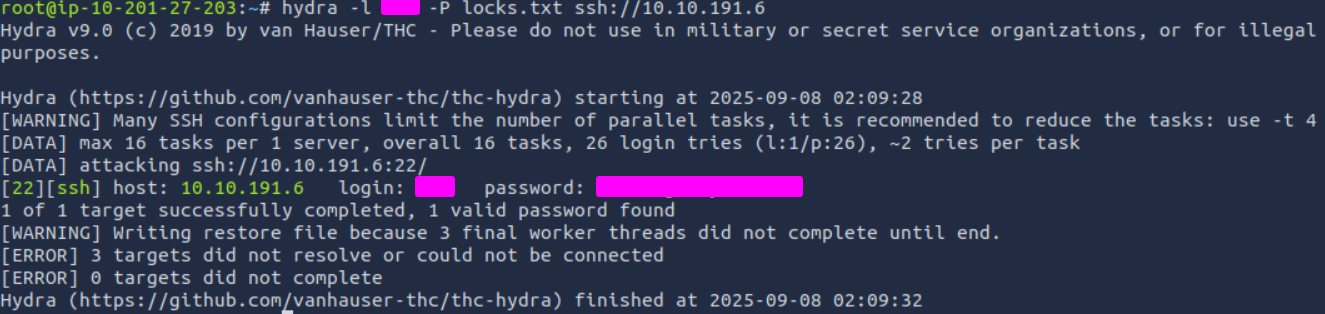


**What service can you bruteforce with the text file found?**

Como o último serviço que resta a ser verificado é o SSH pode-se presumir que esta é a resposta da pergunta.

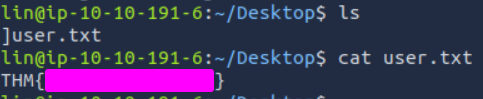
**What is the users password?**

Ao analisar o arquivo locks.txt pode-se ver que são diversas senhas que podem ser utilizadas para realizar um bruteforce do SSH, utilizando o hydra com o comando **hydra -l [Pessoa\_que\_escreveu\_a\_lista] -P locks.txt ssh://[IP\_da\_máquina]** pode se encontrar a senha:



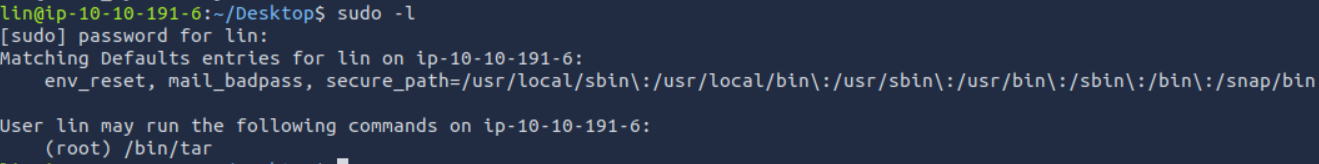
**user.txt**

Agora que se possui acesso ao SSH do usuário pode-se entrar e obter a primeira flag:

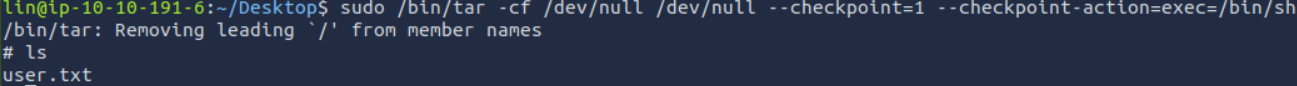


**root.txt**

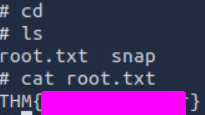
Agora, para poder realizar o escalonamento de privilégios é necessário que primeiramente se cheque quais comandos este usuário tem acesso com o comando **sudo -l**:



O usuário pode utilizar o comando **tar**, pesquisando sobre este comando no site GTFObins mostra que o comando **tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh** pode ser utilizado para realizar este escalonamento:



Agora que se possui acesso ao root vá até o diretório do root para encontrar a flag final:



**Conclusão**

Este é um CTF simples e divertido, mostrando de modo simples e intuitivo como os comandos e itens devem ser utilizados, fazendo com que seja ótimo para simples treinos nos conceitos abordados.

**Referências**

<https://gtfobins.github.io/gtfobins/tar>