Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

| **Informações do documento** | |
| --- | --- |
| **Referência** | Cyborg – Artur Adam de Oliveira |
| **N° Revisão** | 1 |
| **Data de publicação** | 02/10/2025 |
| **Link** | <https://tryhackme.com/room/cyborgt8> |

| **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** | 02/10/2025 | Produção |
| **1** | 02/10/2025 | Revisão |
| **2** | 02/10/2025 | Aprovação |

| **Informações do CTF** | |
| --- | --- |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Enumeração, Cracking de Hashes, Escalonamento de privilégios |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_lsmxlqoi499x)

[Desenvolvimento 3](#_s3jfqtv4av6e)

**Scan the machine, how many ports are open?** [3](#_rbya4elmdyv0)

**What service is running on port 22?** [3](#_61d3a8f5zijx)

**What service is running on port 80?** [3](#_w0z2po95e5w7)

**What is the user.txt flag?** [3](#_oujm6qu674w7)

**What is the root.txt flag?**7

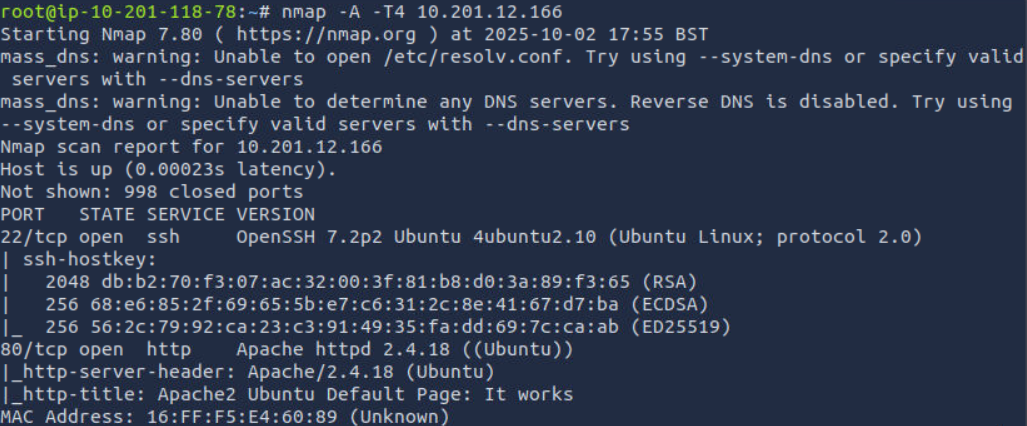
[Conclusão](#_55pnaapg893c) 8

**Contextualização**

Este é um CTF simples que aborda conceitos como escalonamento de privilégios e cracking de hashes de maneira simples e divertida.

**Desenvolvimento**

**Scan the machine, how many ports are open?**

Para solucionar esta pergunta, utilize o comando **nmap -A -T4 [IP\_da\_Máquina]:**

Pode se ver que existem duas ports abertas.

**What service is running on port 22?**

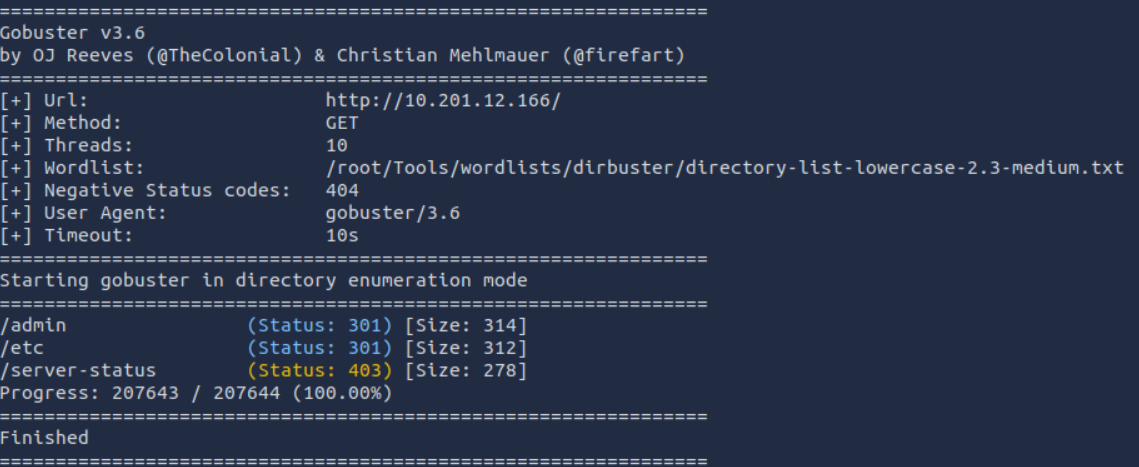
Analisando o nmap se vê que o serviço da port 22 é um SSH

**What service is running on port 80?**

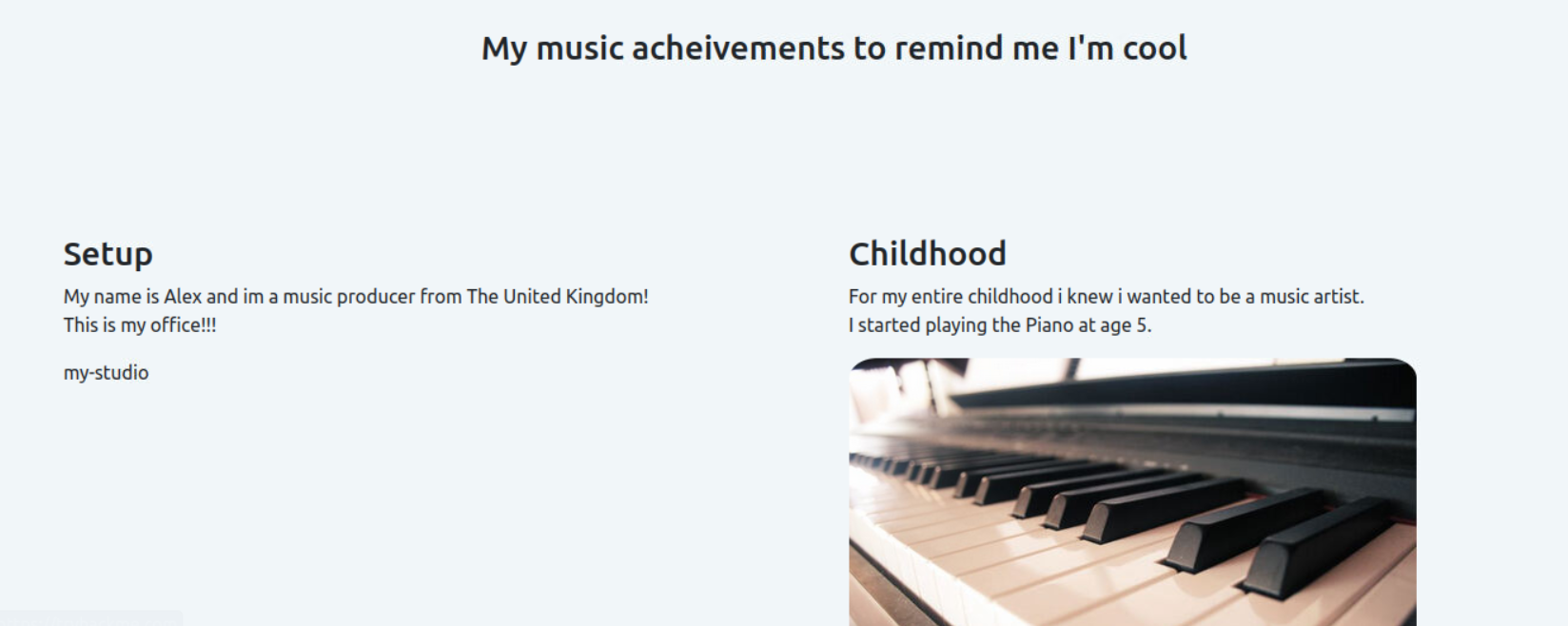
Analisando o nmap se vê que o serviço da port 80 é um HTTP .

**What is the user.txt flag?**

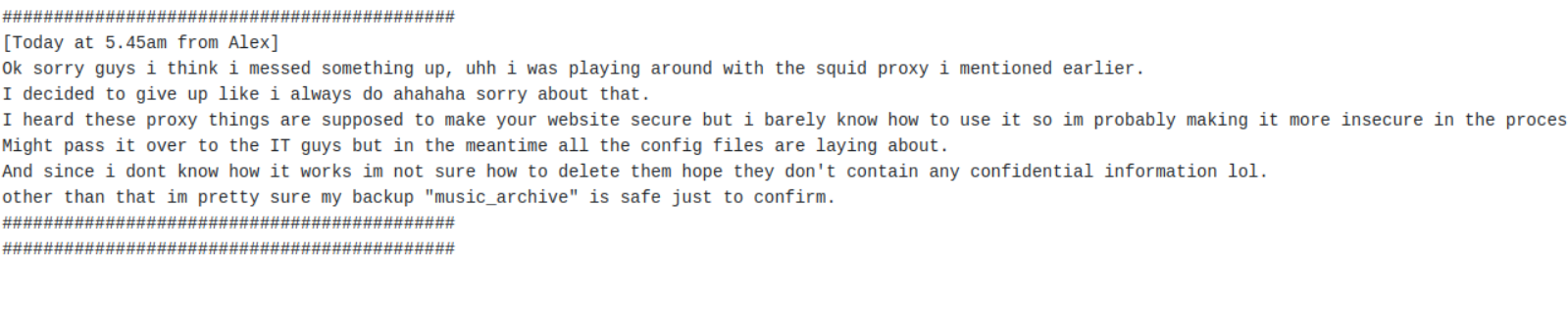
Como existe um port http utilize o gobuster com o comando **gobuster dir -u** [**http://[IP\_da\_Máquina**](about:blank)**] -w [Wordlist\_para\_gobuster]:**

****

Pode se encontrar um diretório /admin, ao ir até este diretório onde existe um site com uma breve informação sobre o admin:



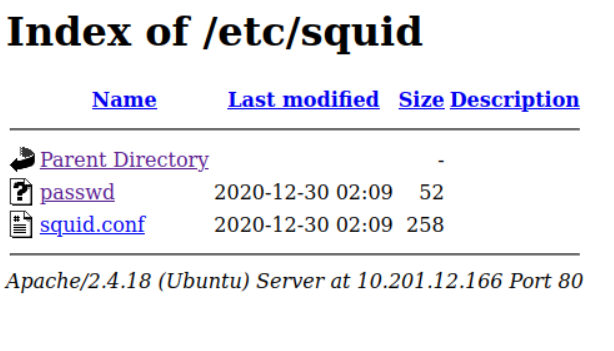
No topo da página existe um uma aba de downloads que permite que seja realizado o download do arquivo “archive.tar” que sera utilizado depois além disso, há um chatlog ao dos admins, onde é informado que eles estavam utilizando um squid proxy:

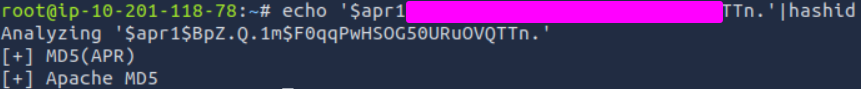


Como isso é tudo que pode ser encontrado neste site agora verifique o /etc, que leva a um armazenamento de arquivos:

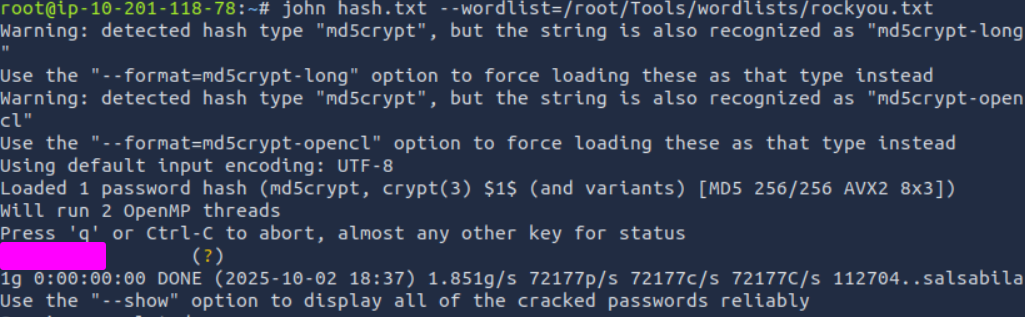


Indo para o arquivo /etc/squid/ pode ser encontrado um arquivo chamado “passwd”:

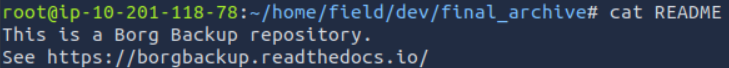


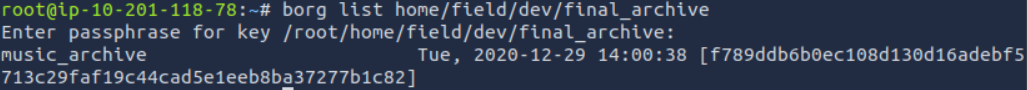
Dentro deste arquivo existe um hash do que pode ser presumido ser a chave, primeiramente identifique o com o comando **echo ‘[HASH’| hashid** (caso não possua hashid instalado instale com o comando **apt install hashid**): 

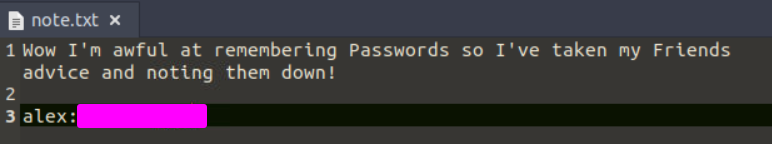
Agora que se sabe que o Hash é um MD5, pode-se utilizar o JohnTheRipper para descobrir a senha (sugere-se passar o hash para um arquivo para maior facilidade de uso), utilizando o comando **john [Arquivo\_Hash] --wordlist=[rockyou.txt]**:

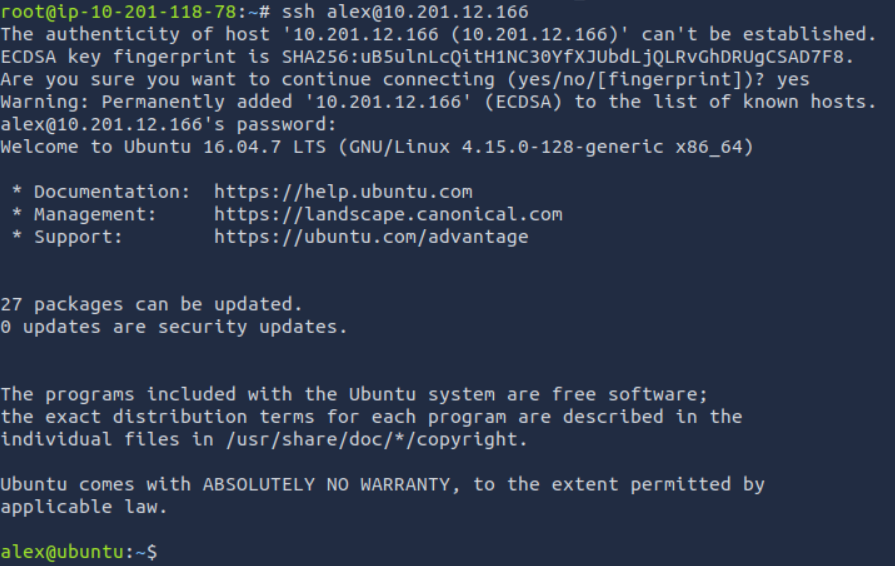


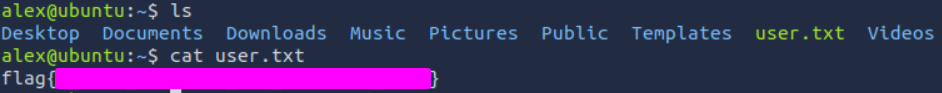
Perfeito! Agora que a senha foi obtida retorne para o arquivo “archive.tar” previamente mencionado, neste arquivo, pode ser encontrado um arquivo “README”, ao abri-lo ele diz que este é um repositório de backups Borg e providencia um link:



Agora que se sabe disso, é possível utilizar o comando **borg list home/field/dev/final\_archive** e a senha que foi descoberta a pouco tempo: 

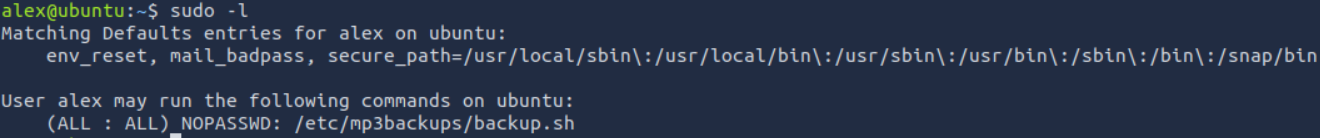
Agora que se sabe o nome do arquivo armazenado utilize o comando **borg extract home/field/dev/final\_archive/::music\_archive** para obter acesso. feito isso um arquivo novo é liberado chamado “Alex” na pasta /home, neste arquivo existe um arquivo “note.txt” que aparenta possuir um usuário e senha para um SSH:

Para acessar o SSH do Alex utilize o comando **ssh alex@[IP\_da\_Máquina]** e coloque a senha quando requisitado:

Feito isso apenas extraia a flag de user.txt e essa pergunta está concluída:****

**What is the root.txt flag?**

Primeiramente utilize o comando **sudo -l** para descobrir quais comandos sudo podem ser utilizados:



Isso mostra que se possui permissão de rodar um arquivo “[backup.sh](http://backup.sh)” como sudo, ao analisar este arquivo com o comando **cat /etc/mp3backups/backup.sh** as duas últimas linhas chamam atenção:



Essas linhas dizem que, qualquer coisa que esta em “$command” é rodado por “$cmd” e isso depois o output é exibido quando finalizado e os conteúdos de “$command” é determinado pelo argumento -c permitindo com que qualquer comando seja rodado como root utilizando isto. Por tanto tudo que é necessário fazer é rodar o comando **sudo /etc/mp3backups/backup.sh -c "cat /root/root.txt"** e a flag será retornada:



E assim termina o CTF.

**Conclusão**

Este é um CTF bem simples que incentiva aquele que está praticando a pesquisar sobre alguns sistemas que pode não ter conhecido antes, além de compreender de melhor forma como códigos podem ser abusados para este tipo de fim.