Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Library – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Library – Gabriel F. Sabino |
| **N° Revisão** |  |
| **Data de publicação** | 01/11/2025 |
| **Link** | https://tryhackme.com/room/bsidesgtlibrary |

|  |  |  |
| --- | --- | --- |
| **Redação** | Gabriel F. Sabino | Estudante |
| **Revisão** |  |  |
| **Aprovação** |  |  |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 01/11/2025 | Gabriel F. Sabino |
| **1** |  |  |
| **2** |  |  |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Exploração Web, Escalação de Privilégio, Brute Force, Code Injection |
| **Plataforma** | Tryhackme |
| **Área** | Red |

Sumário

[Contextualização 3](#_Toc212913667)

[Desenvolvimento 3](#_Toc212913668)

[USER.TXT 3](#_Toc212913669)

[ROOT.TXT 5](#_Toc212913670)

[Conclusão 6](#_Toc212913671)

[Referências 6](#_Toc212913672)

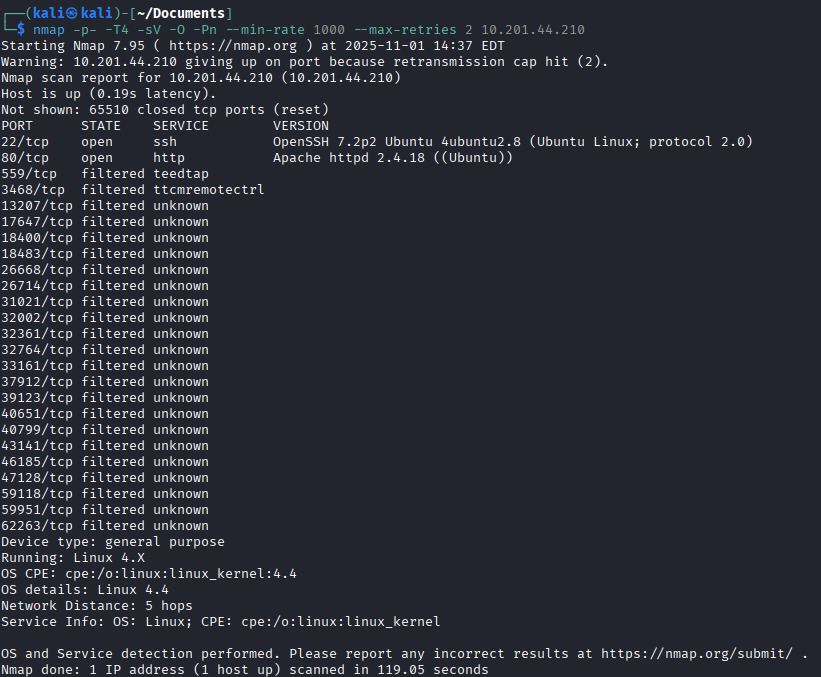
Contextualização

O CTF "LIbrary" do TryHackMe é um desafio visando testar habilidades de webhacking, como exploração web e escalação de privilégio, além de o desafiar a analisar o sistema e fazer o usuário pensar em como alterar o conteúdo de um códigos que não tenha permissão.

Desenvolvimento

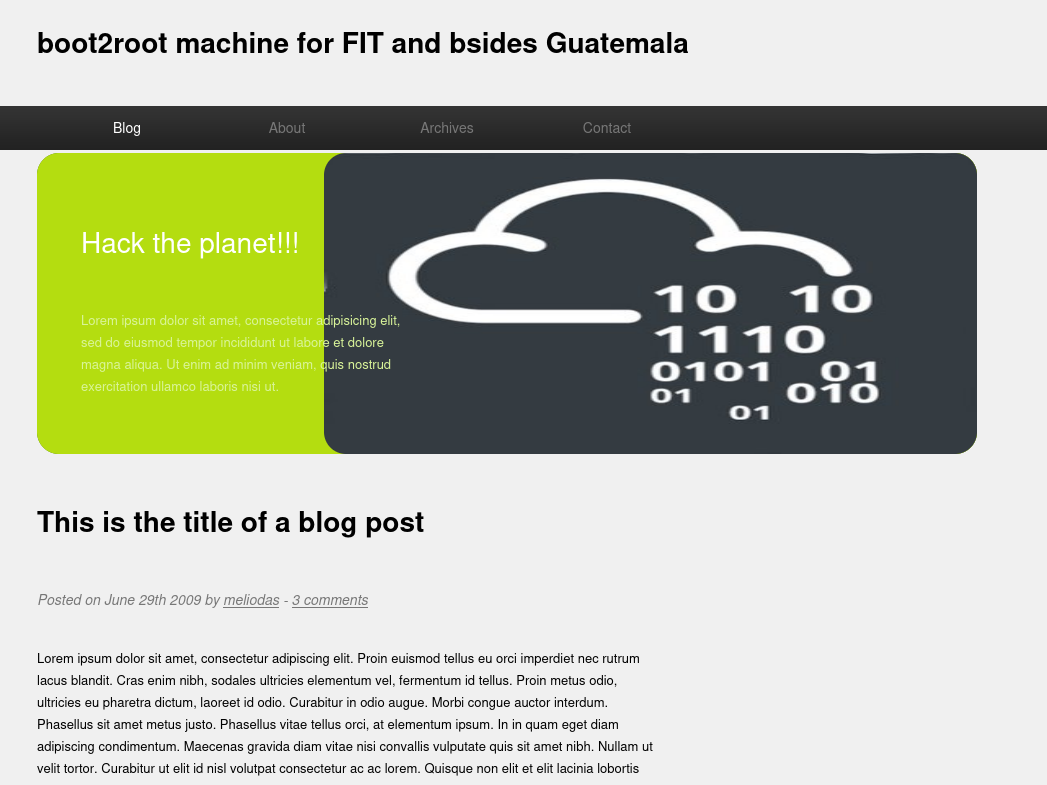
USER.TXT

Iniciamos rodando um nmap:

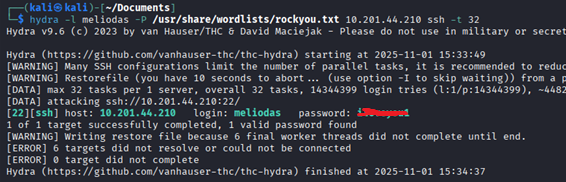


Buscando no google a versão do ssh, encontramos uma vulnerabilidade que permite fazer bruteforce.

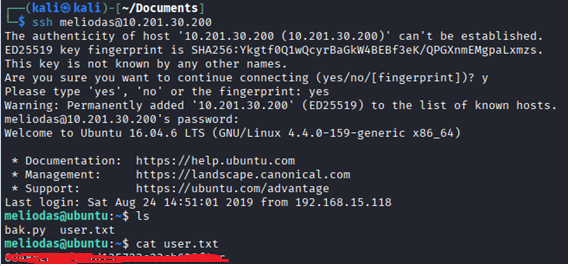
Indo até a porta 80 temos:



Aqui encontramos o usuário (meliodas), com ele em mãos, vamos tentar usar o hydra para descobrir a senha do ssh:

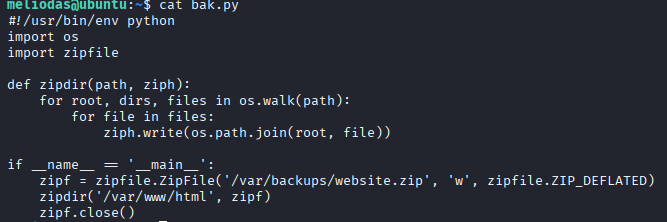


Utilizando essa senha e login no ssh conseguimos logar e encontrar a flag:

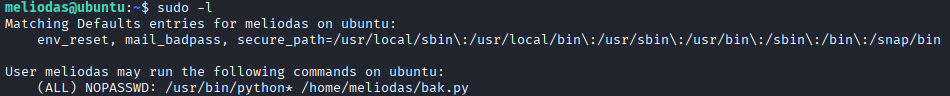


ROOT.TXT

Vamos ver o que esse bak.py faz:

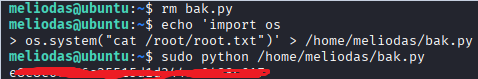


Nós conseguimos rodar esse código como sudo?



Parece que sim, vamos tentar alterar o seu conteúdo para que ele acesse a flag.

Inicialmente tentei alterar com nano, mas tinha permissão, então removi o arquivo e criei um novo contendo o código que eu queria e mantive o seu nome e endereço pois é o que o user meliodas tem permissão para rodar como sudo:



Conclusão

Este CTF leva a pessoa a saber sobre ataques de força bruta em autenticação web e uma das falhas mais clássicas de escalação de privilégios: permissões incorretas no sudo.

É uma boa porta de entrada para esses conteúdos, já que com apenas buscas simples no Google consegue-se encontrar facilmente conteúdos relevantes (como o uso do hydra para logins ou a exploração de scripts via sudo -l), além de não se aprofundar muito nos temas.

Referências

<https://chatgpt.com/>

<https://www.exploit-db.com/exploits/45939>

<https://nvd.nist.gov/vuln/detail/cve-2018-15473>