Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Pickle Rick – Nicolas Mota Engles |
| **N° Revisão** | 1 |
| **Data de publicação** | 26/10/2025 |
| **Link** | https://tryhackme.com/room/picklerick |

|  |  |  |
| --- | --- | --- |
| **Redação** | Nicolas Mota Engles | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 26/10/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Directory Scanning, Remote Code Execution (RCE), Privilege Escalation (PrivEsc) |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 2](#_Toc212399592)

[Desenvolvimento 3](#_Toc212399593)

[Primeiro Ingrediente 3](#_Toc212399594)

[Segundo Ingrediente 6](#_Toc212399595)

[Terceiro Ingrediente 6](#_Toc212399596)

[Conclusão 7](#_Toc212399597)

[Referências 7](#_Toc212399598)

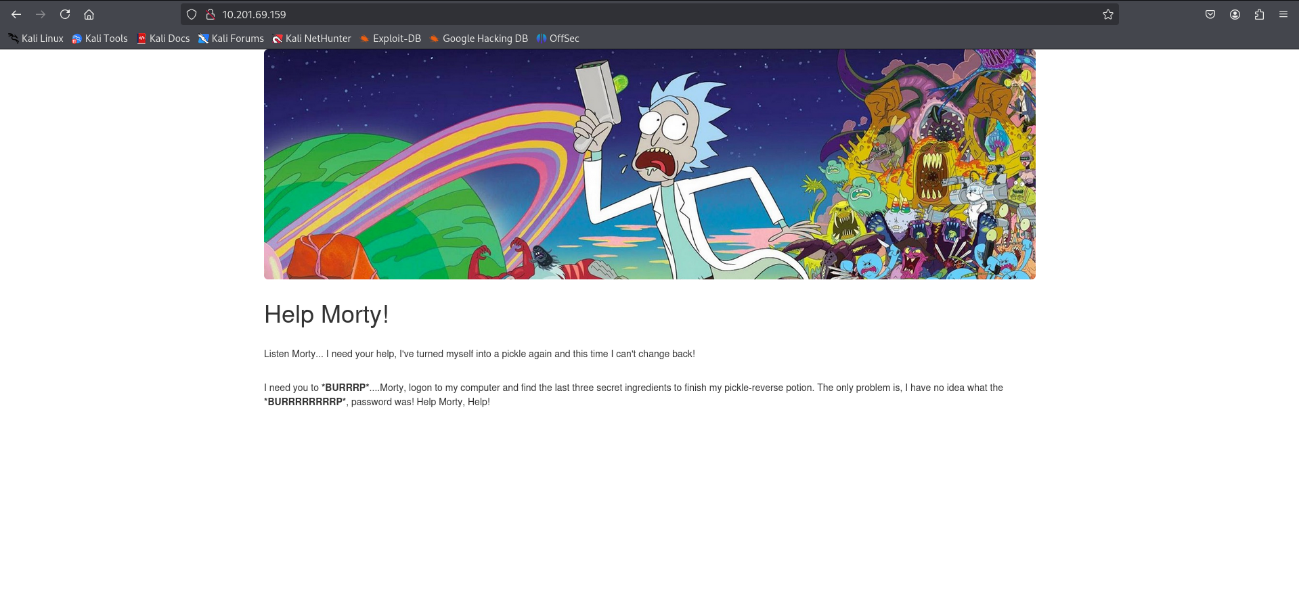
Contextualização

*Pickle Rick* se trata de um CTF temático do seriado de TV *Rick & Morty.* O objetivo é exploitar um servidor web em busca das três flags que, no caso, são os três ingredientes que o *Pickle Rick* precisa para se transformar de volta em humano.

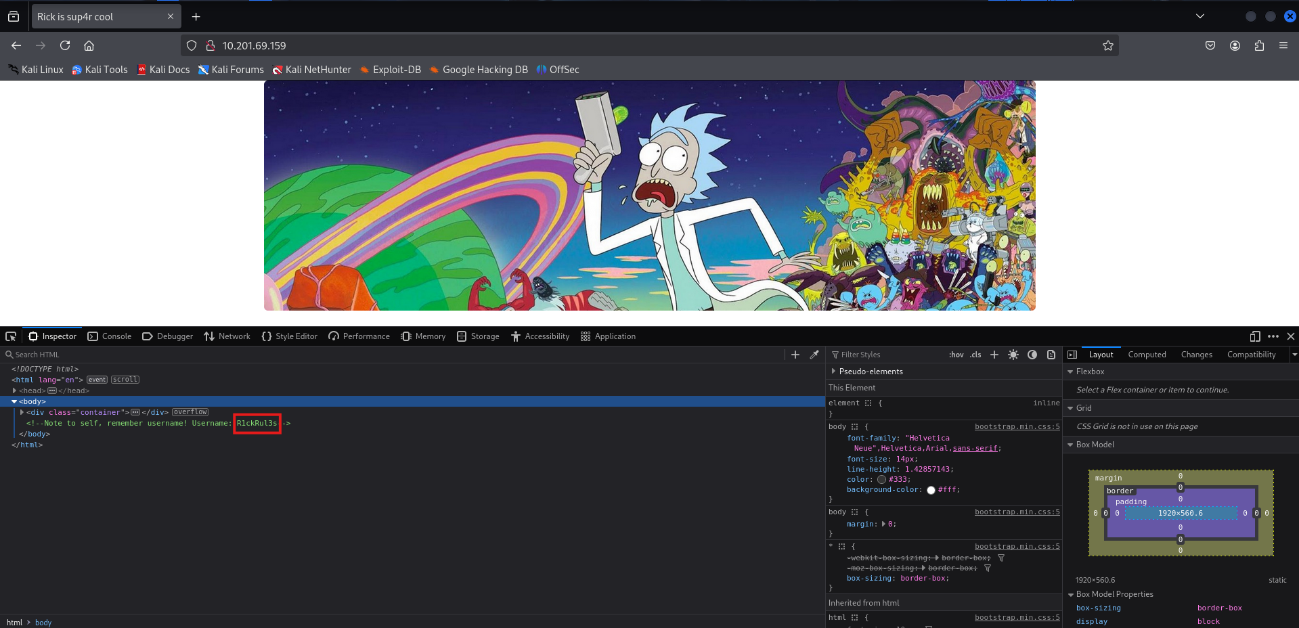
Desenvolvimento

Primeiro Ingrediente

Ao abrir o IP do alvo no navegador, nos deparamos com uma página que apresenta um desafio: “Encontrar a senha do computador do Rick”.



Ao inspecionar o código fonte da página, encontramos o nome de usuário do “computador do Rick”, porém sem a senha.

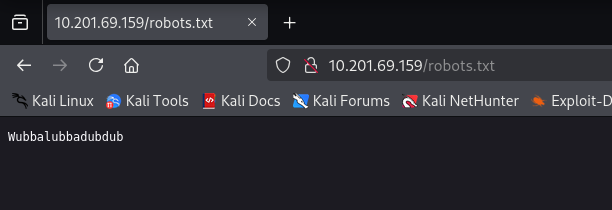


Utilizamos a ferramenta Gobuster para encontrar outros diretórios além da página inicial no servidor web. O resultado nos mostra dois diretórios de interessе: “robots.txt” e “login.php”.

A screenshot of a computer

AI-generated content may be incorrect.

Ao acessar o diretório “robots.txt”, encontramos uma possível senha para o nome de usuário encontrado anteriormente.



No diretório “login.php”, utilizamos o nome de usuário encontrado na página inicial e o texto encontrado no diretório “robots.txt”.

A screenshot of a computer

AI-generated content may be incorrect.

Dessa maneira, obtivemos acesso a um prompt de comando

A screenshot of a computer

AI-generated content may be incorrect.

Utilizamos o comando “whoami” para averiguar se esse se tratava de um prompt de comando de um sistema Linux.

A white rectangular object with a black border

AI-generated content may be incorrect.

Após confirmar o funcionamento desse comando, utilizamos o comando “ls -la” para verificar o que havia no diretório atual da máquina.

A screenshot of a computer

AI-generated content may be incorrect.

No diretório, observamos o arquivo “Sup3rS3cretPickl3Ingred.txt” e utilizamos o comando “less Sup3rS3cretPickl3Ingred.txt” para acessá-lo, encontrando assim o primeiro ingrediente.

A white rectangular object with a black stripe

AI-generated content may be incorrect.

Segundo Ingrediente

Após encontrar o primeiro ingrediente, observamos o arquivo “clue.txt” (que siginifica “dica”) no mesmo diretório, logo utilizamos o comando “less clue.txt” para acessá-lo.

A dica contida no arquivo em questão sugeria que procurássemos os próximos ingredientes em outros diretórios da máquina. Foi possível encontrar o segundo ingrediente no diretório “ls -la ../../../home/rick” e, utilizando o comando “less ../../../home/rick/’second ingredients’”, foi possível encontrá-lo.

A white rectangular object with a black border

AI-generated content may be incorrect.

Terceiro Ingrediente

Da mesma maneira que encontramos o segundo ingrediente, encontramos também o terceiro, localizado no diretório root, que, por padrão, era de acesso proibido. Para burlar isso, primeiro averiguamos quais comandos o nosso usuário tinha permissão de executar.

A screenshot of a computer

AI-generated content may be incorrect.

Vendo que o nosso usuário tem permissão para executar qualquer comando, utilizamos “sudo -i” para acessar o diretório root e, consequentemente, o arquivo contendo o terceiro ingrediente.

A white rectangular object with a black border

AI-generated content may be incorrect.

Conclusão

O CTF apresenta um desafio relativamente simples, sendo assim um bom material de estudo para principiantes em Pentest.

Referências

<https://gemini.google.com/>