Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Gotta Catch'em All! – Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 05/03/2025 |
| **Link** | https://tryhackme.com/room/pokemon |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 12/03/2025 | Eike G. Barbosa |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Hashing, exploração web, escalação de privilégio |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

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

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

Find the Grass-Type Pokemon3

Find the Water-Type Pokemon4

[Find the Fire-Type Pokemon](#_heading=h.tyjcwt) 5

[Who is Root’s favorite Pokemon?](#_heading=h.3dy6vkm) 5

[Conclusão](#_heading=h.1t3h5sf) 6

[Referências](#_heading=h.4d34og8) 6

**Contextualização**

O CTF "Gotta Catch'em All!" do TryHackMe é um desafio temático inspirado no universo Pokémon, projetado para testar diversas habilidades em segurança ofensiva.

**Desenvolvimento**

**Find the Grass-Type Pokemon**

DPrimeiramente fazemos uma simples scan com o nmap

Comando usado: **nmap -sS -sV <target\_ip>**

Texto

O conteúdo gerado por IA pode estar incorreto.

Vemos que temos 2 portas abertas, http e ssh, focaremos primeiro na http. É uma página default apache, entrando na view page source, encontramos uma coisa interessante.

Uma imagem contendo objeto, relógio, escuro, monitor

O conteúdo gerado por IA pode estar incorreto.

Então agora podemos acessar o ssh com o user e a senha.

Comando usado: **ssh <usr>@<target\_ip>**

Texto

O conteúdo gerado por IA pode estar incorreto.

Acessando e fazendo uma simples busca, conseguimos achar a primeira flag em um arquivo zip, só dar um unzip e entrar no diretório, porém, ela está codificada em hexadecimal.

Texto

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Apenas decodificar e conseguir a primeira flag.

**Find the Water-Type Pokemon**

Para achar a segunda arquivo, utilizamos o mesmo formato do outro e usamos o “locate” para saber onde ele está, algo bem simples. Ela está codificada em cifra de Cesar.

Comando usado: **locate <arquivo>**

Texto

O conteúdo gerado por IA pode estar incorreto.

Indo em qualquer site pra decodificar, temos a nossa segunda flag.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

**Find the Fire-Type Pokemon**

**Parte superior do formulário**

E com a mesma lógica do último, encontramos a terceira flag, a única diferença, é que ela está no formato de bas64.

Texto

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

**Who is Root's Favorite Pokemon?**

**Parte superior do formulário**

Para acessarmos a próxima flag, é preciso de uma escalação de privilégio, então vamos atras disto.

Esta etapa já é um pouco mais complicada, pois entramos em um diretório que não faz muito sentido de entrar.

Texto

O conteúdo gerado por IA pode estar incorreto.

Ao acessar este arquivo, vemos que temos um código muito simples em C++.   
Podemos notar que temos a senha do user “ash”.

Acessando este usuário, temos direito root e podemos descobrir a última flag

Texto

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

Este CTF é ótimo para nos deixar mais adequados a rodar diversos diretórios sem preguiça, pois precisamos dele, além de ter um tema muito incrível.

**Referências**

<https://www.dcode.fr/caesar-cipher>

<https://chatgpt.com/>

<https://base64.guru/converter/decode>