Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Compute Magic – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Compute Magic – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 29/03/2025 |
| **Link** | https://tryhackme.com/room/HackfinityBattleEncore |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 29/03/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Engenharia reversa |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 2](#_Toc191235304)

[Desenvolvimento 3](#_Toc191235305)

[What is the flag? 3](#_Toc191235306)

[Conclusão 14](#_Toc191235308)

[Referências 14](#_Toc191235309)

Contextualização

O Compute Magic é um dos CTF criados para a competição mundial para estudantes Hackfinity Battle da plataforma TryHackMe. Ele é um CTF categorizado como um desafio de engenharia reversa de nível fácil.

Desenvolvimento

What is the flag?

Para iniciar, o desafio dispõe uma conexão via TCP para o usuário conectar. Use o **Netcat** para realizar essa conexão no IP e porta especificado.

Interface gráfica do usuário, Aplicativo, Teams

O conteúdo gerado por IA pode estar incorreto.

Ao fazer a conexão, a máquina exibe ‘Compute some magic!’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Tente digitar um comando terminal, para retirar suspeitas de um possível RCE (Remote Code Execution).

Texto

O conteúdo gerado por IA pode estar incorreto.

Ao digitar ‘whoami’ o programa encerrou inesperadamente, é possível concluir que para qualquer entrada inválida o programa encerra.

Voltando ao início do desafio, a plataforma disponibiliza um arquivo para baixar, descarregue esse arquivo na máquina local.

Texto

O conteúdo gerado por IA pode estar incorreto.

Ele resulta em um arquivo compactado chamado ‘computemagic.zip’. Use o comando ‘unzip’ para descompactar esse arquivo. Então, com o arquivo executável, use o **Ghidra** para descompilar o código e fazer uma possível engenharia reversa.

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

À esquerda está o código ‘assembly’, o mais próximo a linguagem de máquina e de pouca legibilidade. A ferramenta é capaz de transformar esse programa em um código legível Java (Código à direita).

O código representado está localizado na função *main*, a função principal do código.

Parte desse código é responsável apenas por disponibilizar a conexão TCP, mas a linha 66 parece responsável por fazer uma verificação, provavelmente para exibir a flag. Consulte o método ‘checkSpell’ na linha 66.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

A seguinte função exibe um *Switch Case* com todas as letras do alfabeto, de A a Z. Caso seja digitado alguma letra, alguma função será chamada.

A maioria das funções está presente apenas para criar uma confusão para quem está solucionando o desafio.

Entre as funções, verifique a função 24, que será invocada caso o usuário digite a letra ‘X’.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Clique nela para exibir o código da função.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Essa função é responsável por invocar a função ‘read\_flag’, que exibirá a flag no terminal.

Então, volte para a conexão original e digite ‘X’. Esse caractere será verificado no *Switch Case* visto anteriormente que por sua vez, chamará a função 24 encarregada de invocar a função ‘read\_flag’

Texto

O conteúdo gerado por IA pode estar incorreto.

Conclusão

Esse CTF é um desafio de engenharia reversa de nível fácil, ótimo para quem está estudando sobre o tema e quer praticar. Um desafio excelente para praticar ferramentas como **Ghidra** e analise de código.

Referências

<https://ghidra-sre.org/>