Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Don’t you Love Banners – PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | dont-you-love-banners – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 11/03/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/437 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 03/03/2025 | Produção |
| **1** | 11/03/2025 | Revisão |
| **2** | 11/03/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Engenharia reversa de scripts, exploração de vulnerabilidades |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

[Contextualização 2](#_Toc191910034)

[Desenvolvimento 3](#_Toc191910035)

[What is the flag? 3](#_Toc191910036)

[Conclusão 8](#_Toc191910037)

[Referências 8](#_Toc191910038)

Contextualização

O seguinte CTF é um desafio de nível médio que aborda temas simples, mas que exige experiência com outros CTFs, leitura de código em geral e familiaridade com sistemas Linux.

Desenvolvimento

What is the flag?

Para iniciar, a plataforma disponibiliza duas conexões TCP para serem feitas com o **Netcat**.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Uma das conexões solicita uma senha para continuar, enquanto a outra, disponibiliza a senha. Digite a senha dada no primeiro terminal.

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Em seguida, aparecerá outra pergunta.

Texto

O conteúdo gerado por IA pode estar incorreto.

A resposta dessa pergunta pode ser adquirida com uma simples pesquisa. Então, digite ‘DEFCON’ para prosseguir.

Texto

O conteúdo gerado por IA pode estar incorreto.

Assim como a pergunta anterior, pesquise para encontrar a resposta, que é ‘John Thomas Draper’.

Texto

O conteúdo gerado por IA pode estar incorreto.

Após as perguntas, é obtido acesso ao terminal. Ao explorar o diretório inicial ‘/home/player’ é possível encontrar dois arquivos de texto: ‘banner’ e ‘text’.

Use o comando ‘cat’ para visualizar o conteúdo dos arquivos.

Texto

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Algo interessante, o arquivo banner é o arquivo processado para formar a mensagem de boas-vindas visto no começo da conexão, isso pode ser usado futuramente.

Texto

O conteúdo gerado por IA pode estar incorreto.

Para continuar, procure por alguma vulnerabilidade que permita realizar um escalonamento de privilégios ou que permita contornar a permissão de visualização da flag.

Explorando os diretórios, é notável que mesmo como um usuário comum, é possível ter acesso ao diretório `/root`, então, explore esse diretório.

Texto

O conteúdo gerado por IA pode estar incorreto.

Ainda não é possível visualizar a flag, mas o arquivo python ‘script.py’ não exige autorização para visualizá-lo. Novamente, use o comando ‘cat’ para visualizar o conteúdo do código.

Texto

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

O código é o desafio interativo que aparece ao iniciar a conexão TCP. Esse código pode ser capaz de exibir a flag sem permissão, pois a linha 8 do código é responsável por abrir um arquivo de texto e exibir. Caso, não exista arquivo de texto para ser lido, será exibido o banner da linha 11 a 14.

Para testar, remova o arquivo ‘banner.txt’ do diretório ‘/home/player’ e faça a conexão com o **Netcat** novamente.

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Como esperado, foi exibido o banner feito no código. Com essa informação, pode ser possível fazer um *symlink* no arquivo da flag.

*Symlink*, semelhante ao atalho do Windows, é capaz de criar um link simbólico que funciona de atalho para arquivos ou diretórios.

Então, crie um *symlink* para o arquivo da flag e nomeie de banner no diretório onde estava o banner original que foi excluído.

Texto

O conteúdo gerado por IA pode estar incorreto.

Refaça a conexão com o **Netcat** e em vez de exibir o banner do código, será exibido a flag.

Texto

O conteúdo gerado por IA pode estar incorreto.

Conclusão

Esse desafio desafia os conhecimentos Linux do participante, e exige um certo conhecimento na linguagem Python. Ademais, esse desafio pode ser resolvido facilmente e abre possibilidade de expandir o conhecimento em relação ao sistema Linux.

Referências

<https://www.futurelearn.com/info/courses/linux-for-bioinformatics/0/steps/201767>

<https://docs.python.org/3/library/os.html>