Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

packer – PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | packer – Matheus Castilho |
| **N° Revisão** | 0 |
| **Data de publicação** | 11/03/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/421?category=3&difficulty=2&page=1 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Matheus da Cunha Castilho | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

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

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Engenharia Reversa |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

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

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

Descompressão

Flag

[Conclusão 7](#_heading=h.1t3h5sf)

[Referências 7](#_heading=h.4d34og8)

**Contextualização**

Neste CTF, é fornecido um arquivo, e possui uma descrição com a seguinte frase: “Reverse this linux executable?”. Ao abrir o arquivo em texto, não é possível encontrar nenhum texto legível. A dica diz para o usuário procurar como é feito para reduzir o tamanho de um arquivo binário após compilado, levando a entendimentos sobre compressão de arquivos. O CTF é simples, porém necessita de alguns conhecimentos prévios em criptografia e engenharia reversa.

**Desenvolvimento**

**Descompressão** A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Ao tentar executar o arquivo fornecido, não foi possível realizar nenhuma ação pois está protegido com senha. Ao abrir o arquivo como texto também não foi possível observar nada de útil.

A screenshot of a computer screen

AI-generated content may be incorrect.

Abrindo o arquivo utilizando o code browser do Ghidra, também não foi possível observar nenhuma string ou função útil.

A screenshot of a computer

AI-generated content may be incorrect.

Então, ao observar a dica, é possível levar ao entendimento de que o arquivo está comprimido.

A screenshot of a chat

AI-generated content may be incorrect.

Por isso, pode-se utilizar alguma ferramenta para remover a compressão, como no caso do upx.

A screenshot of a computer

AI-generated content may be incorrect.

**Flag**

Assim, ao executá-lo novamento no Ghidra, obtemos uma string com um texto criptografado, aparentemente em hex.

A screenshot of a computer

AI-generated content may be incorrect.

Ao descriptografar, obtemos a flag:

A screenshot of a computer

AI-generated content may be incorrect.

**Conclusão**

Neste CTF foi possível observar alguns conceitos de compressão de arquivo, engenharia reversa, e criptografia. É um CTF relativamente simples, porém requer conhecimento prévio em engenharia reversa e Linux. Utilizando-se de softwares como Ghidra, esse CTF pode ser um bom exercício para a aprendizagem de análise de código Assembly para engenharia reversa.

**Referências**

<https://www.kali.org/tools/upx-ucl/#:~:text=UPX%20is%20an%20advanced%20executable,other%20files%20for%20different%20OS.>

<https://upx.github.io>

<https://codebeautify.org/hex-string-converter>