03/07/2023 – PicoCTF – Static ain't always noise

Link: <https://play.picoctf.org/practice/challenge/163?page=1&search=>

1. Verificando o que há em ambos os arquivos:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Verificando o tipo de cada arquivo:

Texto

Descrição gerada automaticamente

1. O conteúdo de static não é human-readable, mas percebe-se que ele é um executável:

Texto

Descrição gerada automaticamente

1. Com isso, deduz-se que o “ltdis.sh” utilizará “static” para encontrar a flag. Verificando o arquivo “ltdis.sh”, percebe-se que ele interage com algum arquivo “$1” e, portanto, será trocado o valor “$1” por “static”:

Texto

Descrição gerada automaticamente

1. Rodar o arquivo alterado:

Texto

Descrição gerada automaticamente

1. Verifica-se dois arquivos criados. Observar o “static.ltdis.strings.txt”:

Texto

Descrição gerada automaticamente

1. Procurar a flag com o comando “grep”:

Interface gráfica do usuário

Descrição gerada automaticamente com confiança média

Portanto, a flag é: $flag