

=====

## AVALIAÇÃO OPCIONAL #01: *CRACK THE CODE*

=====

Considere o arquivo executável denominado "ctc", que foi compilado para sistemas Linux AMD64. Seu objetivo é criar um fluxo de entrada que satisfaça os seguintes requisitos:

- Você deve acessar o sistema utilizando as seguintes credenciais:
  - Usuário: **SB**
  - Senha: **SB**
- O programa deve finalizar com a exibição da seguinte frase:
  - **A BANDEIRA É MINHA!**
- O programa não deve finalizar com falha de segmentação, ou falhas de qualquer outro tipo.

Observe que você só pode manipular o fluxo de entrada do programa e você não tem acesso ao arquivo código-fonte.

Porém, é importante observar que o arquivo executável foi gerado considerando o seguinte:

- Compilador GCC (11.4)
- Sistema operacional Linux (Ubuntu 21)
- Linha de compilação "gcc -g -fno-stack-protector ctc.c -o ctc"

Para facilitar e automatizar a configuração do ambiente de execução do programa proposto, utilize o algoritmo base fornecido no arquivo "cracker.c" para definir o seu fluxo de entrada. O fluxo de entrada é definido por um vetor de bytes em que cada entrada é separada por '\n'. Por exemplo, em "Um\nDois\n", a primeira leitura do programa receberá "Um" e a segunda receberá "Dois".

Além de definir o fluxo de entrada, o algoritmo "cracker.c" também realiza algumas alterações em variáveis de sistema que normalmente estão presentes em todos os sistemas Linux (embora tenha sido testado apenas nas distribuições Ubuntu e Mint).

O "cracker.c", após compilado, pode ser executado em três modos:

- Modo 1 (./cracker 1): executa o ctc
- Modo 2 (./cracker 2): "executa" o ctc através do gdb
- Modo 3 (./cracker 3): executa o ctc usando o fluxo de entrada definido

Você deve enviar o arquivo "cracker.c" adaptado com o seu fluxo de entrada que resolve o problema conforme as especificações fornecidas. O tópico de entrega do trabalho e o prazo serão fornecidos pelo Moodle.