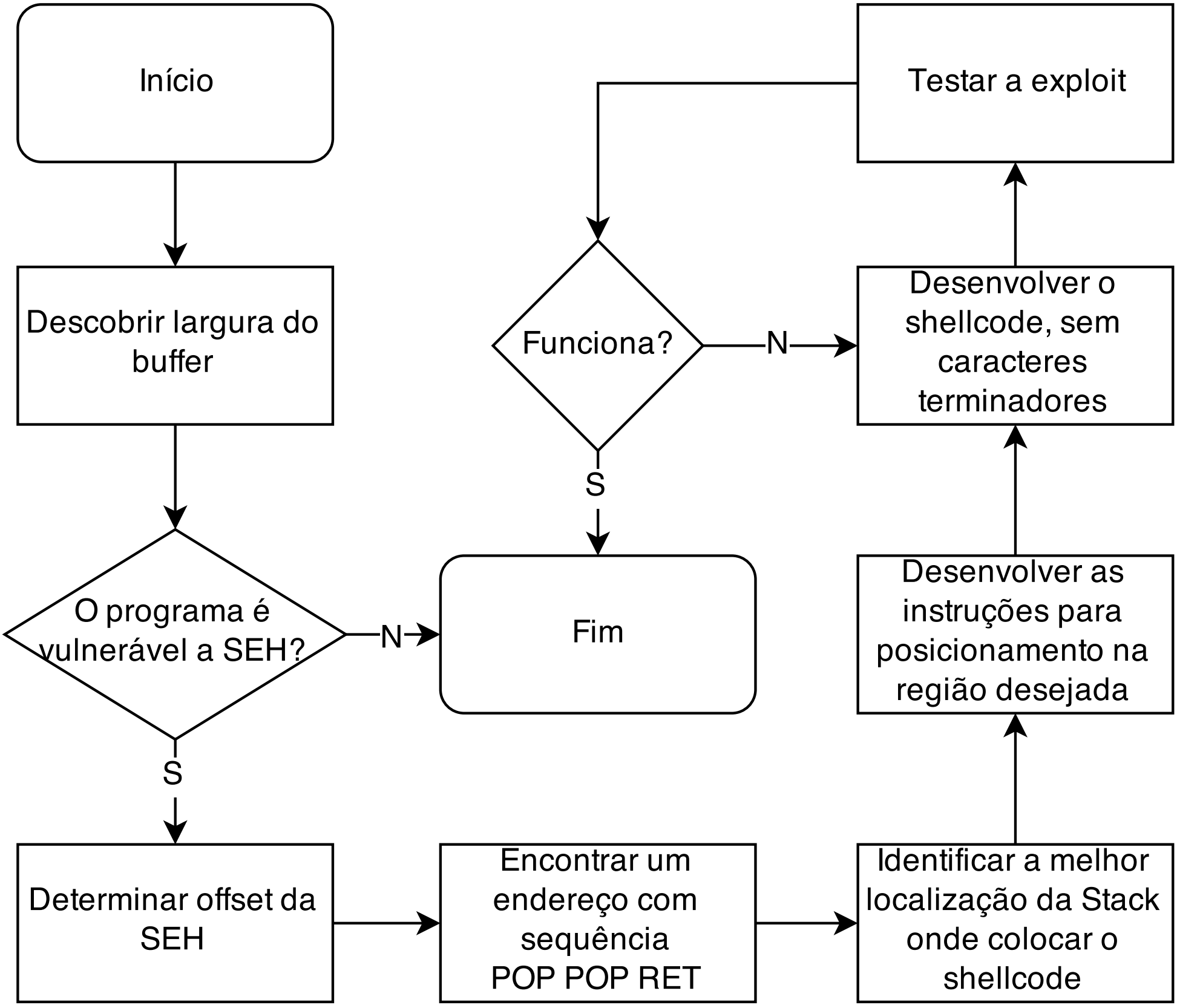
Início
Descobrir largura do buffer
O programa é vulnerável a SEH?
N
Fim
S
Determinar offset da SEH
Encontrar um endereço com sequência POP POP RET
Identificar a melhor localização da Stack onde colocar o shellcode
Desenvolver as instruções para posicionamento na região desejada
Desenvolver o shellcode, sem caracteres terminadores
Funciona?
N
S
Testar a exploit