P2 INF1018

Daniel Stulberg Huf – 1920468 – Turma 3WB

QUESTÃO 1

1. Antes da chamada à função boo dentro da função main, estão presentes os seguintes códigos em assembly: **push %rbp**, e em seguida, **movq %rsp, %rbp**. Isso significa que primeiro colocamos no topo da pilha o base pointer da função chamadora e o adequamos em um múltiplo de 16. Em seguida, a próxima instrução cria a base do Registro de Ativação da main. Deve-se preencher a tabela antes dessa última instrução. Nesse momento, o RIP ocupa o próximo endereço após o RSP

Dessa maneira, temos a seguinte tabela:

|  |  |
| --- | --- |
| **Endereço** | **Conteúdo** |
|  |  |
|  |  |
| 0x1FF0 | RBP (0x20F0) |
| 0x1FF8 |  |
| 0x2000 | RIP (0x1000) |
| 0x2008 | RSP |
|  |  |

1. Os eventos que ocorrem na pilha em seguida são: o rsp vai para onde está o rbp, a boo é chamada pela main, e coloca-se no topo da pilha o endereço de retorno da main (0x8752). O base pointer em seguida é movido para o topo da pilha, e há mais 24 bytes de memória utilizados pela função boo (4 \* 6 = 24). Entretanto, deve-se ocupar 32 bytes para manter o ordenamento em múltiplos de 16. O stack pointer é então colocado no topo da pilha novamente.

Dessa maneira, temos a seguinte tabela:



|  |  |
| --- | --- |
| **Endereço** | **Conteúdo** |
|  |  |
|  |  |
| 0x1FC0 | RSP |
|  | 32 bytes ocupados em boo |
| 0x1FE0 | RBP |
| 0x1FE8 | 0x8752 (ret) |
| 0x1FF0 |  |
|  |  |
| 0x2000 | RIP (0x1000) |
| 0x2008 |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |