**1.STACK SMASHING**

**PROGRAM:**

**Int main(){**

**Int a[3];**

**Int I = 0;**

**While(I < 1024){**

**A[I] = 1;**

**I++;**

**}**

**Return 0;**

**}**

**STACK FRAME rsp0**

|  |
| --- |
| **1** |
| **rsp1 1 rbp1** |
| **1** |
| **1** |
| **1** |
| **1** |
| **1** |
| **0** |
|  |
|  |
|  |

**rsp2**

rbp0 gets replaced with the value 1 and the stack bound is violated. The stack size assigned is 32 bytes

2.**RECURSIVE PROGRAM**

**PROGRAM**

**Int fact(int num){**

**If(num == 0){**

**return 1;**

**}**

**else{**

**return num \* fact(num – 1);**

**}**

**Int main{**

**Int result = fact(3);**

**return 0;**

**}**

**rsp0 STACK FRAME**

|  |
| --- |
| **rsp1 rbp0 rbp1** |
| **6** |
| **3** |
|  |
| **rsp2 1169** |
| **rsp3 rbp1 rbp2** |
| **3** |
|  |
|  |
| **rsp4 114a** |
| **rsp5 rbp2 rbp3** |
| **2** |
|  |
|  |
| **rsp6 114a** |
| **rsp7 rbp3 rbp4** |
| **1** |
|  |
|  |
| **rsp8 114a** |
| **rsp9 rbp4 rbp5** |
| **0** |
|  |
|  |
| **rsp10** |

**Each slot is allotted 16 bytes**

**The numbers 1169, 114a are contents of the instruction pointer**