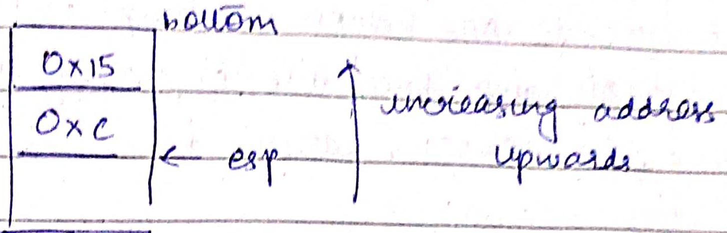
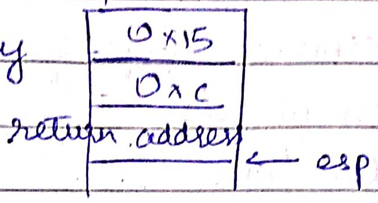
Ques4- assemblycode (0xc, 0x15)

push 0x15

push 0xc

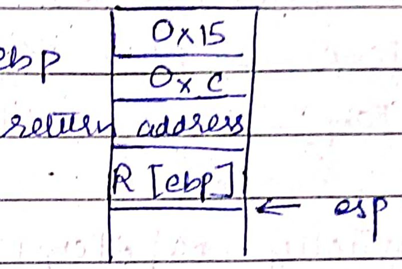


call assembly



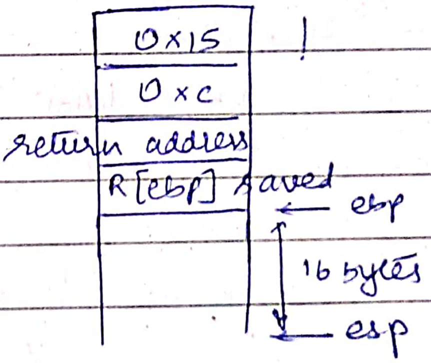
assembly code:

<+0x0> push ebp



<+1> mov ebp, esp R[ebp] = R[esp]

<+3> sub esp, 0x10 R[esp] = R[esp] - 0x10 →16 in hexa



<+6> mov eax, DWORD PTR [ebp+0xC]

<+9> mov DWORD PTR [ebp-0x4], eax

<+12> mov eax, DWORD PTR [ebp+0x8]

<+15> mov DWORD PTR [ebp-0x8], eax

→ R[eax] = M[R[ebp]+0xC] = 0x15

→ M[R[ebp]-0x4] = R[eax] = 0x15

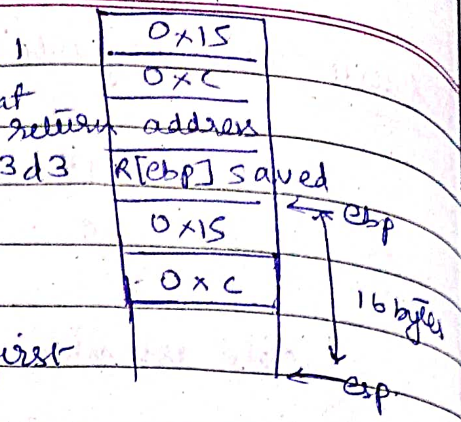
→ R[eax] = M[R[ebp]+0x8] = 0xc

→ M[R[ebp]-0x8] = R[eax] = 0x c

<+18> jmp 0x50c <assemblycode+31> → jump to line<+31>

Date
Page

1. <+20> add DWORD PTR[ebp-0x4], 0x 1
2. <+24> add DWORD PTR [ebp-0x 8], 0xaf
3. <+31> cmp DWORD PTR [ebp-0x 8], 0xa3d3
4. jle 0x 501 <assm 2 +20>



lines 1,2,3,4 forms a loop, first we jump to statement 31

3. M[R[ebp-0x8] - 0xa3d3

4. If M[R[ebp-0x8] - 0xa3d3 ≤ 0, Then jump to <+20>

1. M[R[ebp] - 0x4] = M[R[ebp]-0x4] + 0x1

2. M[R[ebp] - 0x8] = M[R[ebp] - 0x8] + 0xaf

let initially M[R[ebp] - 0x 8] = 12 (0x C)

Let the loop run n times i.e let line 1 & 2 run n times

Let initially M[R[ebp] - 0x4] = 0x 15.

$$0xaf = 175, \ a3d3$$

$$12 + (n-1)(175) \leq 41939$$

$$n-1 \leq \frac{41927}{175}$$

$$n \leq 240.582$$

$$n = 240$$

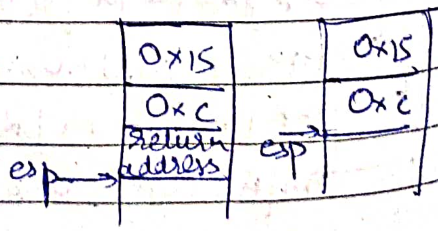
finally [M[R[ebp] -0x 4] = 21 + 240x1 = 261 = 0x105

<+40> mov eax DWORD PTR [ebp-0x4] R[eax] = 0x 105

<+43> leave (R[esp] = R[ebp]) and pops (R[ebp] saved)

<+44> ret (pops return address)

returns R[eax] = 0x105


0x15
0xC
return address
esp
esp
0x15
0xc