# PicoCTF

Tuesday, 2 June 2020 10:43 AM

## Vault Door #3

Original:

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | j | U | 5 | t | _ | a | _ | s | n | a | _ | 3 | l | p | m | 1 | 2 | g | b | 4 | 4 | - | u | _ | 4 | _ | m | 1 | r | 2 | 4 | 0 |
| Index: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| Output: | j | U | 5 | t | - | a | - | s | 1 | m | p | l | 3 | _ | a | n | 4 | g | r | 4 | m | _ | 4 | _ | u | - | 4 | 1 | b | 2 | 2 | 0 |

## asm1

```
    DWORD PTR [ebp +0x8] = 0x345

cmp   DWORD PTR [ebp+0x8], 0x37a     -> compare 0x345 and 0x37a

jg    0x512  <asm1 + 37>             -> jump greater   (0x345 not larger than 0x37)

cmp   DWORD PTR [ebp+0x8], 0x345     -> compare 0x345 and 0x345

jne   0x50a <asm1 +39>               -> jump not equal  (0x345 and 0x345 are equal, so no jump)

mov   eax , DWORD PTR [ebp +0x8]     -> mov 0x345 into eax

add   eax, 0x3          -> 0x345 + 0x3

pop   ebp               -> 0x348
```

## asm2

```
    DWORD PTR [ebp+0x8] -> 0x10
    DWORD PTR [ebp+0xc] -> 0x18

            push  ebp

            mov   ebp, esp

            sub   esp, 0x10

            mov   eax , DWORD PTR [ebp +0xc]

            mov   DWORD PTR [ebp-0x4] , eax        -> DWORD PTR [ebp-0x4] = 0x18

            mov   eax , DWORD PTR [ebp +0x8]

            mov   DWORD PTR [ebp-0x8] , eax        -> DWORD PTR [ebp-0x8] = 0x10

            jmp   0x50c  <asm2 +31>

  <+20>     add   DWORD PTR [ebp-0x4] , 0x1     ]
                                                 }- add values in a loop
            add   DWORD PTR [ebp-0x8] , 0xcb    ]       until
                                                  DWORD PTR [ebp -0x8] > 0x6693
  <+31>     cmp   DWORD PTR [ebp-0x8], 0x6693

            jle   0x501  <asm2+20>

            mov   eax , DWORD PTR [ebp-0x4]        -> get the value of DWORD PTR [ebp-0x4]
```