

## 1. ANTIDEBUG

**Input:** *"I\_10v3-y0U\_\_wh3n Y0u=c411..M3 Senor1t4"*

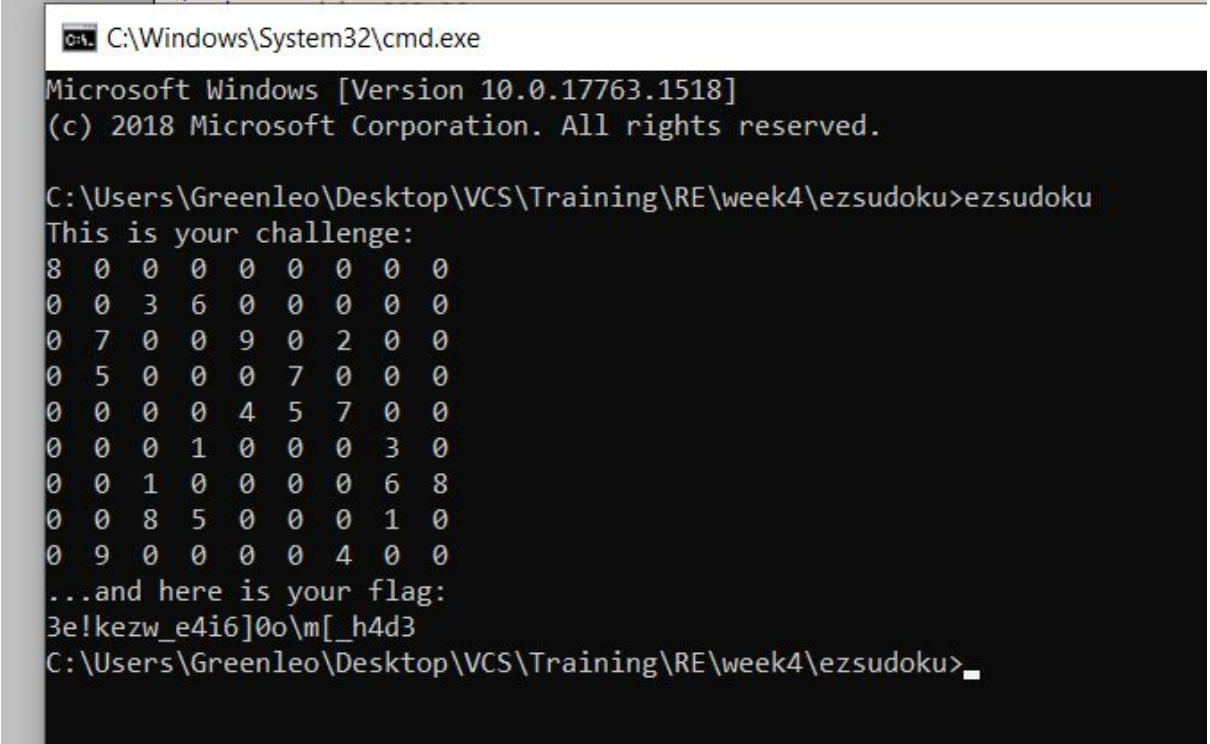
**Flag:** *"vcstraining{Th3\_U1tiM4t3\_ant1\_D3Bu9\_ref3r3ncE}"*

*//write up em xin phép làm sau :< em đang bận deadline trên trường*

## 2. EZSUDOKU

**Flag:** *"3a\$iest\_g4m3\_of\_mY\_l1f3"*

Chạy thử:



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Greenleo\Desktop\VCS\Training\RE\week4\ezsudoku>ezsudoku
This is your challenge:
8 0 0 0 0 0 0 0 0
0 0 3 6 0 0 0 0 0
0 7 0 0 9 0 2 0 0
0 5 0 0 0 7 0 0 0
0 0 0 0 4 5 7 0 0
0 0 0 1 0 0 0 3 0
0 0 1 0 0 0 0 6 8
0 0 8 5 0 0 0 1 0
0 9 0 0 0 0 4 0 0
...and here is your flag:
3e!kezw_e4i6]0o\m[_h4d3
C:\Users\Greenleo\Desktop\VCS\Training\RE\week4\ezsudoku>
```

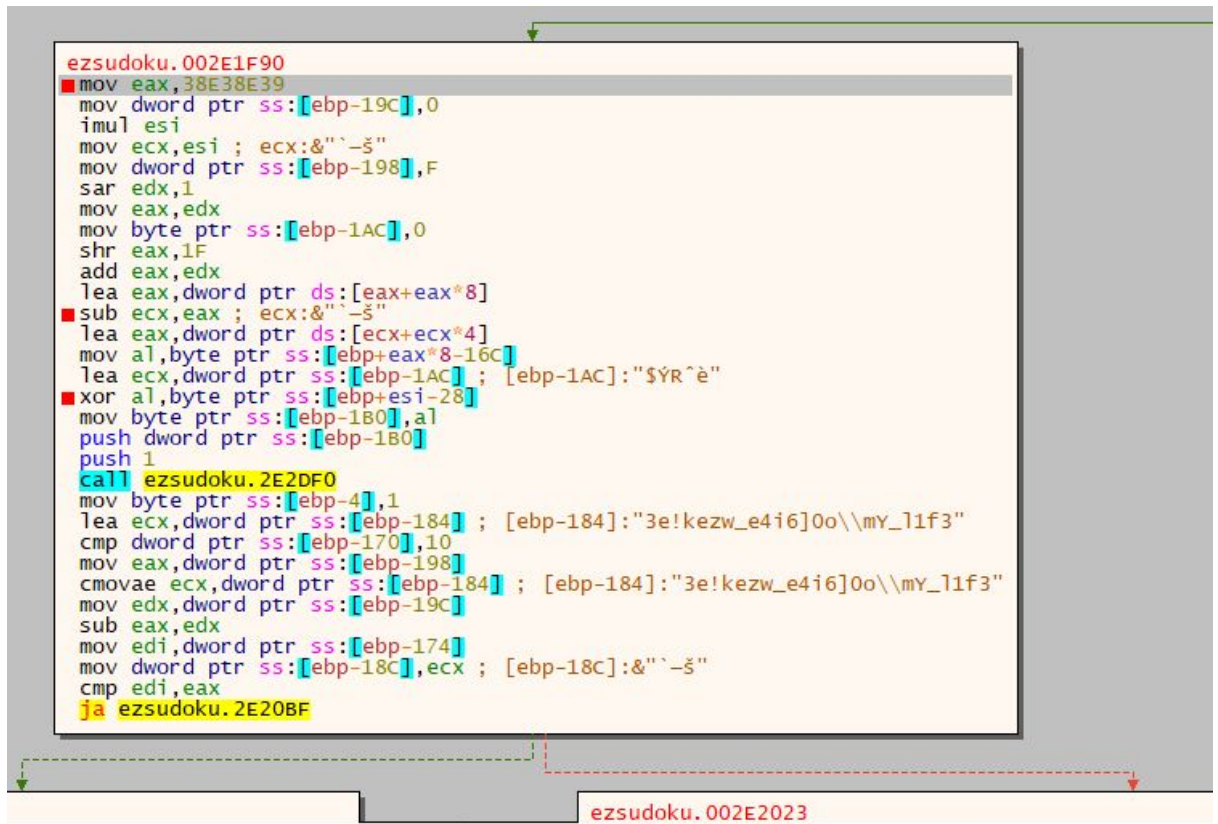
Phần main chính:

ezsudoku.002E1DB0

```
push ebp
mov ebp,esp
push FFFFFFFF
push ezsudoku.302E36
mov eax,dword ptr [0] ; [00000000]:&"äüï"
push eax
sub esp,1BC
mov eax,dword ptr ds:[313068] ; 00313068:"öBq;u"
xor eax,ebp
mov dword ptr ss:[ebp-10],eax ; [ebp-10]:&"äüï"
push esi ; esi:&"C:\\Users\\Greenleo\\Desktop\\VCS\\Training\\RE\\week4\\ezsudoku\\ezsudoku.exe"
push edi ; edi:&"ALLUSERSPROFILE=C:\\ProgramData"
push eax
lea eax,dword ptr ss:[ebp-C]
mov dword ptr [0],eax ; [00000000]:&"äüï"
movups xmm0,xmmword ptr ds:[3100E4] ; 003100E4:";e!kazw^e<i6]4o\\l[wh4d7"
mov edx,ezsudoku.3100FC ; 3100FC:"This is your challenge: "
mov dword ptr ss:[ebp-2C],0 ; [ebp-2C]:EntryPoint
mov ecx,ezsudoku.313F50 ; 313F50:"CO"
movups xmmword ptr ss:[ebp-28],xmm0
movq xmm0,qword ptr ds:[3100F4] ; 003100F4:"l[wh4d7"
movq qword ptr ss:[ebp-18],xmm0
movaps xmm0,xmmword ptr ds:[3101E0]
movups xmmword ptr ss:[ebp-16C],xmm0
xorps xmm0,xmm0
movups xmmword ptr ss:[ebp-15C],xmm0
movaps xmm0,xmmword ptr ds:[310260]
movups xmmword ptr ss:[ebp-14C],xmm0
movaps xmm0,xmmword ptr ds:[3101C0]
movups xmmword ptr ss:[ebp-13C],xmm0
movaps xmm0,xmmword ptr ds:[310270]
movups xmmword ptr ss:[ebp-12C],xmm0
movaps xmm0,xmmword ptr ds:[310250]
movups xmmword ptr ss:[ebp-11C],xmm0
movaps xmm0,xmmword ptr ds:[310190]
movups xmmword ptr ss:[ebp-10C],xmm0
```

### Phần tạo flag:

- Đoạn đầu



- Đoạn cuối:





**Mô tả:**

- Phần flag được tạo từ string có sẵn: “;e!kazw^e<i6]4o!l[Wh4d7” thông qua xor với các giá trị của map sudoku
- Map sudoku ban đầu có dạng như “ảnh 1“, được lấy và store tại **[ebp - 16C]**

008FFC7C	F4	A3	EE	EA	A4	FC	8F	00	00	00	00	0F	00	00	00	0#redu.....
008FFC8C	08	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFC9C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFCAC	00	00	00	00	00	00	00	00	00	00	00	03	00	00	00	
008FFCBC	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFCCC	00	00	00	00	00	00	00	00	00	00	00	07	00	00	00	
008FFCDC	00	00	00	00	00	00	00	00	09	00	00	00	00	00	00	
008FFCEC	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFCFE	05	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFD0C	07	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFD1C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFD2C	04	00	00	00	05	00	00	00	07	00	00	00	00	00	00	
008FFD3C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFD4C	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFD5C	03	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFD6C	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
008FFD7C	00	00	00	00	06	00	00	00	08	00	00	00	00	00	00	
008FFD8C	00	00	00	00	08	00	00	00	05	00	00	00	00	00	00	
008FFD9C	00	00	00	00	00	00	00	00	01	00	00	00	00	00	00	
008FFDAC	00	00	00	00	09	00	00	00	00	00	00	00	00	00	00	
008FFDBC	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	
008FFDCC	00	00	AE	EA	3B	65	21	6B	61	7A	77	5E	65	3C	69	36
008FFDDC	5D	34	6F	5C	6C	5B	57	68	34	64	37	00	5C	45	50	EA
008FFDEC	20	55	85	20	36	35	30	20	20	20	20	20	48	55	85	20

=> Giải sudoku, đẩy lấy map đúng, rồi sửa data map của sudoku trong stack

008FFC7C	F4 A5 EE EA	A4 FC 8F 00	00 00 00 00	0F 00 00 00	0#1e9u.....
008FFC8C	08 00 00 00	01 00 00 00	02 00 00 00	07 00 00 00	.
008FFC9C	05 00 00 00	03 00 00 00	06 00 00 00	04 00 00 00	.
008FFCAC	09 00 00 00	09 00 00 00	04 00 00 00	03 00 00 00	.
008FFCBC	06 00 00 00	08 00 00 00	02 00 00 00	01 00 00 00	.
008FFCCC	07 00 00 00	05 00 00 00	06 00 00 00	07 00 00 00	.
008FFCDC	05 00 00 00	04 00 00 00	09 00 00 00	01 00 00 00	.
008FFCEC	02 00 00 00	08 00 00 00	03 00 00 00	01 00 00 00	.
008FFCF4	05 00 00 00	04 00 00 00	02 00 00 00	03 00 00 00	.
008FFD0C	07 00 00 00	08 00 00 00	09 00 00 00		[008FFCF7] = 00000100 (User Data)
008FFD1C	03 00 00 00	06 00 00 00	09 00 00 00		.
008FFD2C	04 00 00 00	05 00 00 00	07 00 00 00	02 00 00 00	.
008FFD3C	01 00 00 00	02 00 00 00	08 00 00 00	07 00 00 00	.
008FFD4C	01 00 00 00	06 00 00 00	09 00 00 00	05 00 00 00	.
008FFD5C	03 00 00 00	04 00 00 00	05 00 00 00	02 00 00 00	.
008FFD6C	01 00 00 00	09 00 00 00	07 00 00 00	04 00 00 00	.
008FFD7C	03 00 00 00	06 00 00 00	08 00 00 00	04 00 00 00	.
008FFD8C	03 00 00 00	08 00 00 00	05 00 00 00	02 00 00 00	.
008FFD9C	06 00 00 00	09 00 00 00	01 00 00 00	07 00 00 00	.
008FFDAC	07 00 00 00	09 00 00 00	06 00 00 00	03 00 00 00	.
008FFDBC	01 00 00 00	08 00 00 00	04 00 00 00	05 00 00 00	.
008FFDDC	02 00 00 00	3B 65 21 6B	61 7A 77 5E	65 3C 69 36	...;e!kazw^e<i6
008FFDDC	5D 34 6F 5C	6C 5B 57 68	34 64 37 00	5C 45 50 EA	]4o\l[wh4d7.\EPè

**=> Kết quả**

- Flag lưu tại [ebp-184]
- Flag: "3a\$iest\_g4m3\_of\_mY\_l1f3"
- Kết quả chạy tại console:

This is your challenge:

```
8 0 0 0 0 0 0 0 0
0 0 3 6 0 0 0 0 0
0 7 0 0 9 0 2 0 0
0 5 0 0 0 7 0 0 0
0 0 0 0 4 5 7 0 0
0 0 0 1 0 0 0 3 0
0 0 1 0 0 0 0 6 8
0 0 8 5 0 0 0 1 0
0 9 0 0 0 0 4 0 0
```

...and here is your flag:

3a\$iest\_g4m3\_of\_mY\_l1f3