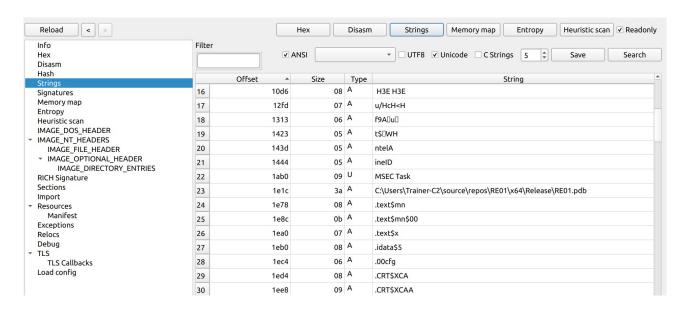
Write-up RE01

Đề bài cho ta một file exe, load file vào DIE để kiểm tra sơ bộ:

ile name								
/home/n33r9/D	ownloads/0.ctf/MSEC_	CTF_2022/re/re	01/RE01.exe					
ile type	Entry point	Entry point		Base address				
PE64	00000001			000000140000000		Memory map		
PE	Export	Import	Resources	.NET	TLS	Ov	verlay	
Sections	ctions Time date stamp Size of image Resources				Resources			
0006	> 2022-08-0	01 13:30:15	00009000		Manifest	Version		
Scan		ess Mode	Architecture		Туре			
Automatic		▼ LE	64-bit	AMD64		Console		
	Microsoft Visual C/C++ crosoft Linker(14.32**)		sole]			S S	? ?	
Signatures	▼ Deep scan						N <u>u</u>	
Directory	10	100% > Log 60 msec					Scan	



Sau khi chạy file, chương trình cho ta một flag fake:

```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]

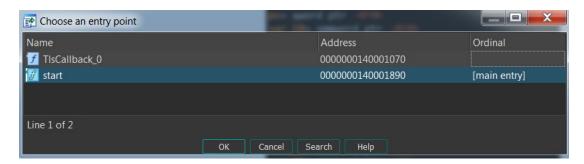
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin>C:\Users\Admin\Desktop\RE01.exe

MSEC{nope_this_is_fake_flag_try_again!}

C:\Users\Admin>
```

Load file vào IDA64, ta chú ý đến hàm tlscallback_0. TLScallback sẽ được gọi và thực thi trước khi nhảy đến entry point của chương trình(main). IDA pro có thể phát hiện ra hoạt động của hàm này. Ctrl+E để kiểm tra entry point của file thực thi trong IDA, ta sẽ thấy hàm Tlscallback_0.



Để debug được, ta có thể config debugger in IDA chọn suspend when process created, hoặc đặt breakpoint tại hàm Tlscallback_0.

Disassemble hàm này, ta thấy cách thức hoạt động của nó và hàm main khá giống nhau, đều thực hiện biến đổi một mảng các ký tự.

Có thể flag thật được tạo ra ở hàm tlscallback, nhưng sau khi thực hiện hàm main, flag giả lại được in ra cho người dùng thấy

Sau khi thực thi xong hàm tlscallback, view memory, ta sẽ thấy flag thật được tạo ra.

```
[]sCallback_0 proc near
    _100= dword ptr -10
_F8= qword ptr -0F8
qword ptr -0F0h
       = xmmword ptr
       = xmmword ptr
          xmmword ptr
          xmmword ptr
       0= dword ptr
       C= dword ptr
     0= aword ptr
push
lea
mov
          rax, cs.__securit
rax, rsp
[rbp+30h+var_10],
xor
          xmm0, cs:xmmword_1400032D0
movups
```

Flag: MSEC{my_name_is_TLS_callback_hope_you_fun!}