Tài liệu tham khảo: Lab 1

Kiểm tra các giá trị

Message BoxW 010011A8



Virtual addresse: 16000

Raw address: 13600

Graphical user interface, application

Description automatically generated

Address of entry point

Graphical user interface

Description automatically generated with low confidence

**Tính toán**

Info:

1BF70 – 13600 = X – 16000

X = 1E970

Add image base 0101E970 (70 E9 01 01)

Text:

1BFA0 – 13600 = Y – 16000

Y = 1E9A0

Add image base 0101E9A0 (A0 E9 01 01)

Code:

New entry point:

1BF50 – 13600 + 16000 = 1E950

Old entry point = jmp + Virtual address + 5 + R\_VA

01012475 = 0001E950 + image base + 14 + 5 + + R\_VA

R\_VA = FFFF 3B 0C

**Payload**

**Assembly**

push 0

push Caption

push Text

push 0

call [MessageBoxW]

jmp Origianl\_Entry\_Point

**Hex**

6A 00

68 70 E9 01 01

68 A0 E9 01 01

6A 00

FF 15 A8 11 00 01

E9 0C 3B FF FF

**Code chèn**

6A 00 68 70 E9 01 01 68 A0 E9 01 01 6A 00 FF 15 A8 11 00 01 E9 0C 3B FF FF

49006e00660065006300740069006f006e0020006200790020004e005400320033003000

320030003500320030003600300035005f00320030003500320030003600340038005f0032003000350032003000380031003500

Chèn vào chương trình