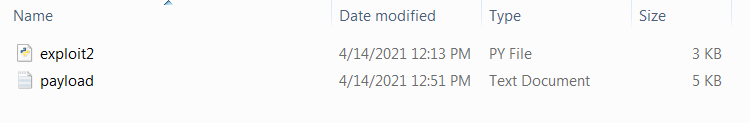
**SECURE CODING LAB 9**

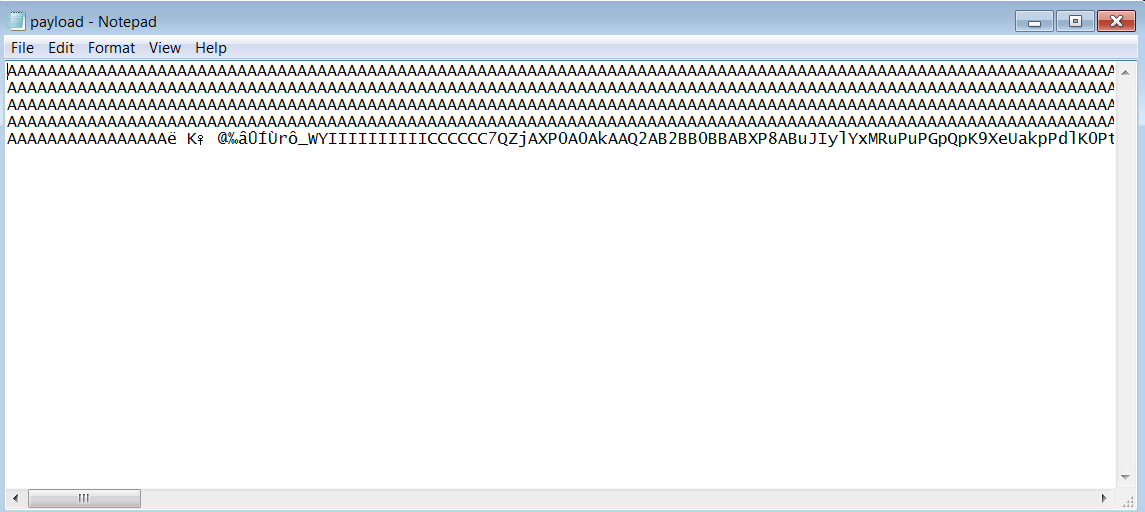
**WORKING WITH MEMORY VULNERABILITIES-3**

**NAME : SREENIDHI GANACHARI**

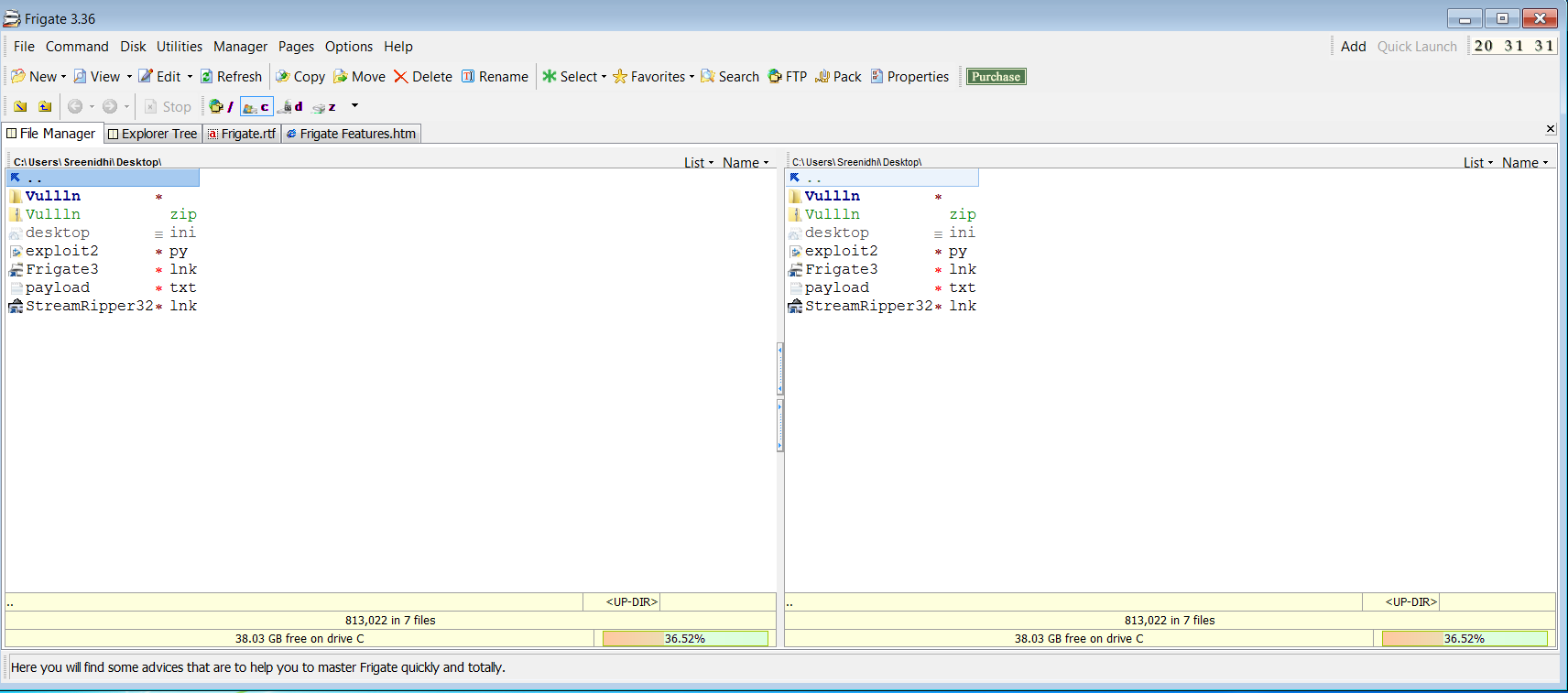
**REGISTRATION NUMBER : 19BCE7230**

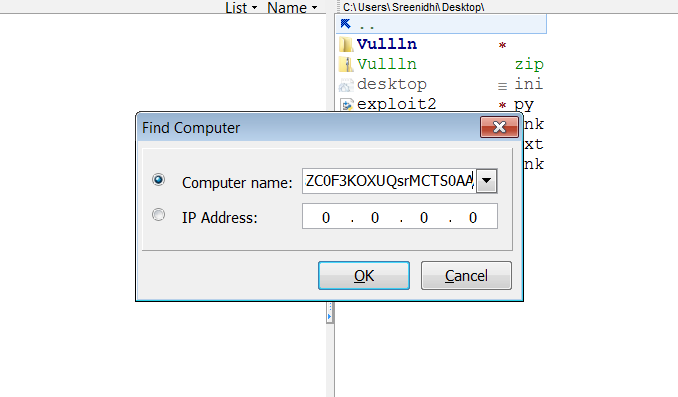
**1) The payload is generated after running the python exploit code in python 2.7**

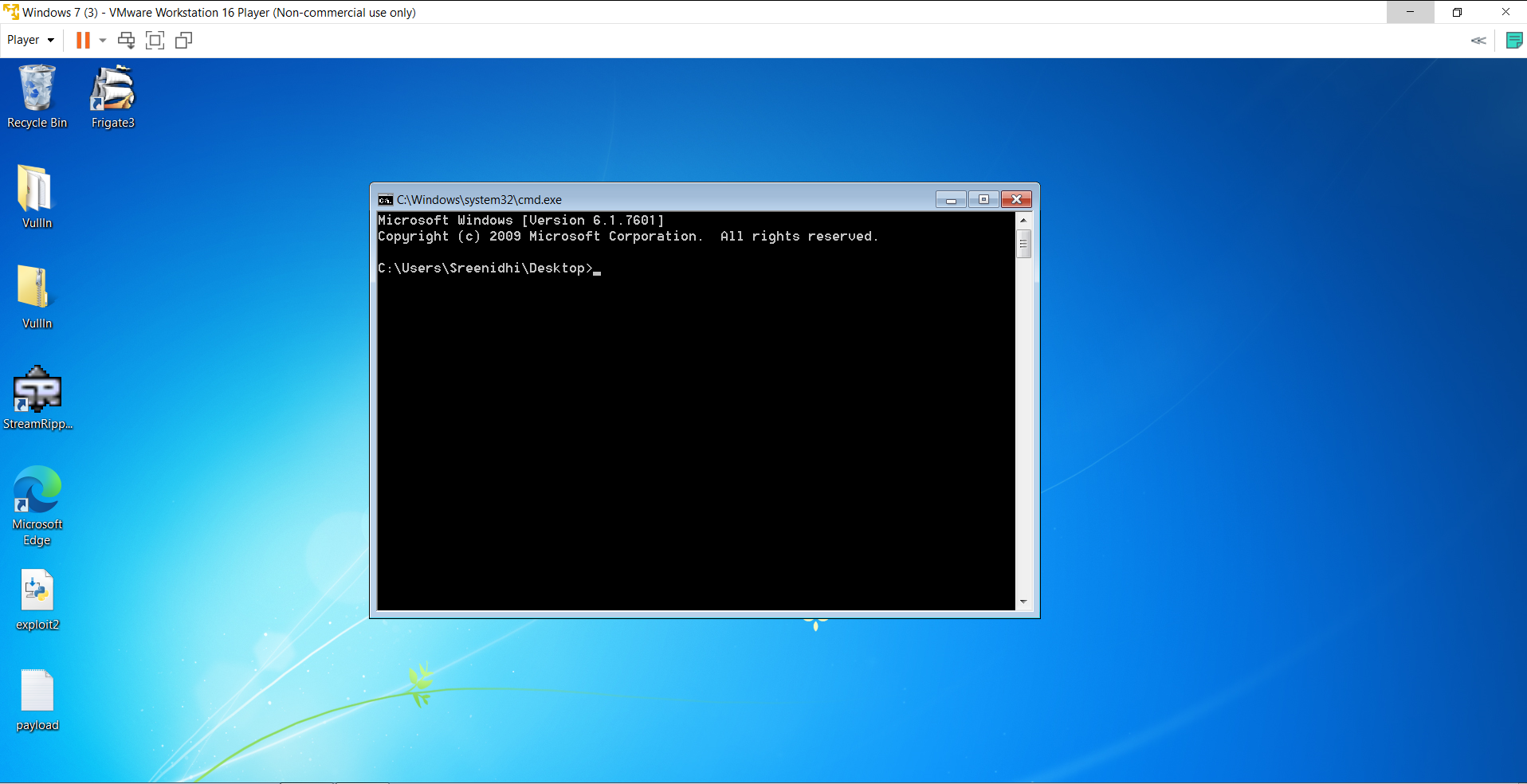




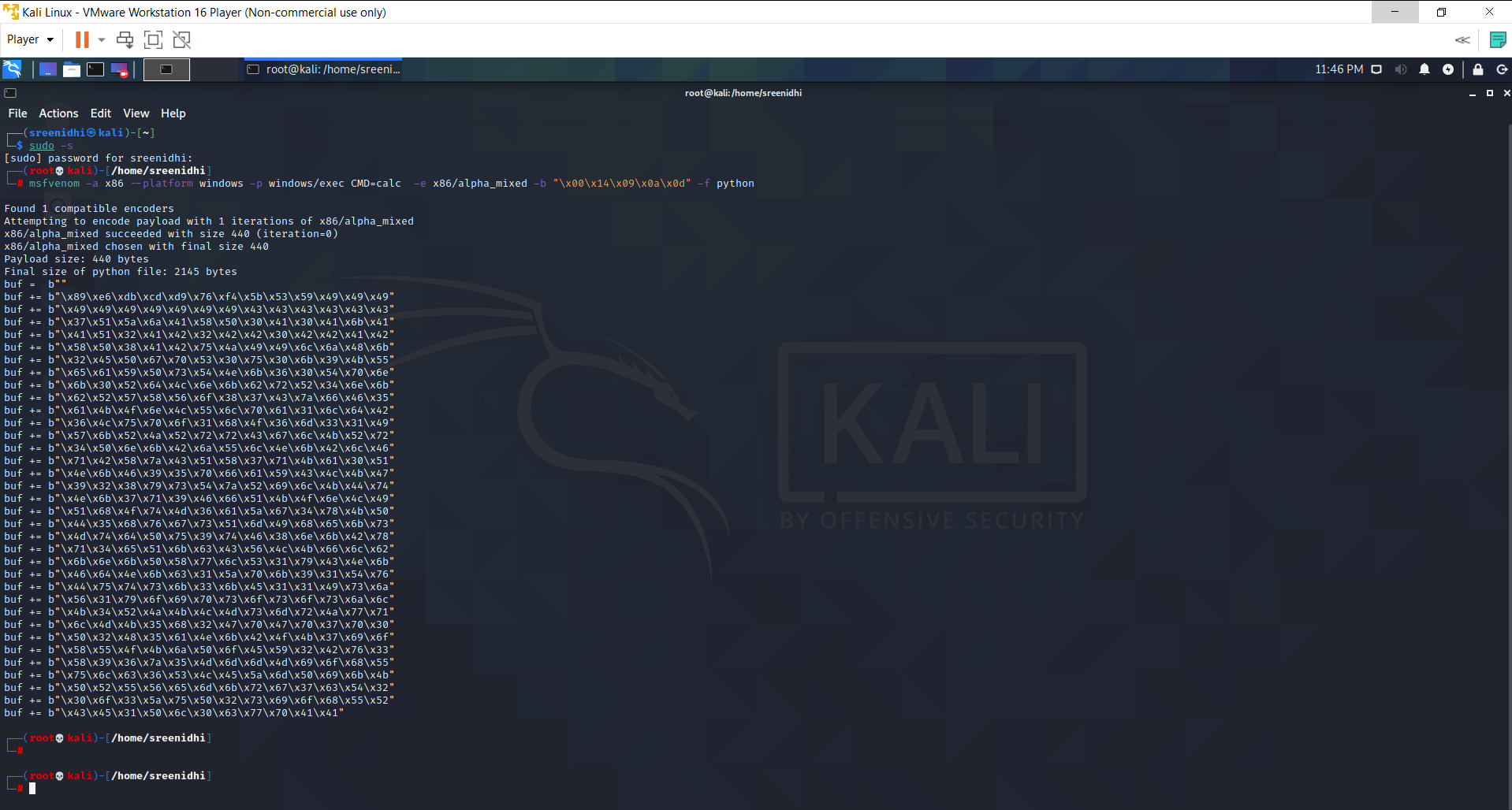
**2)After downloading frigate3.36 if the payload generated is run , the application crashes and it displays the command prompt.**



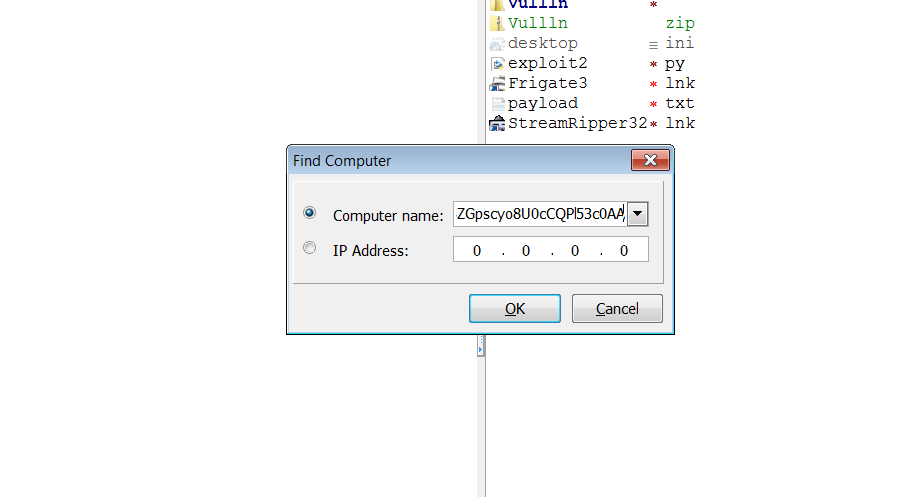


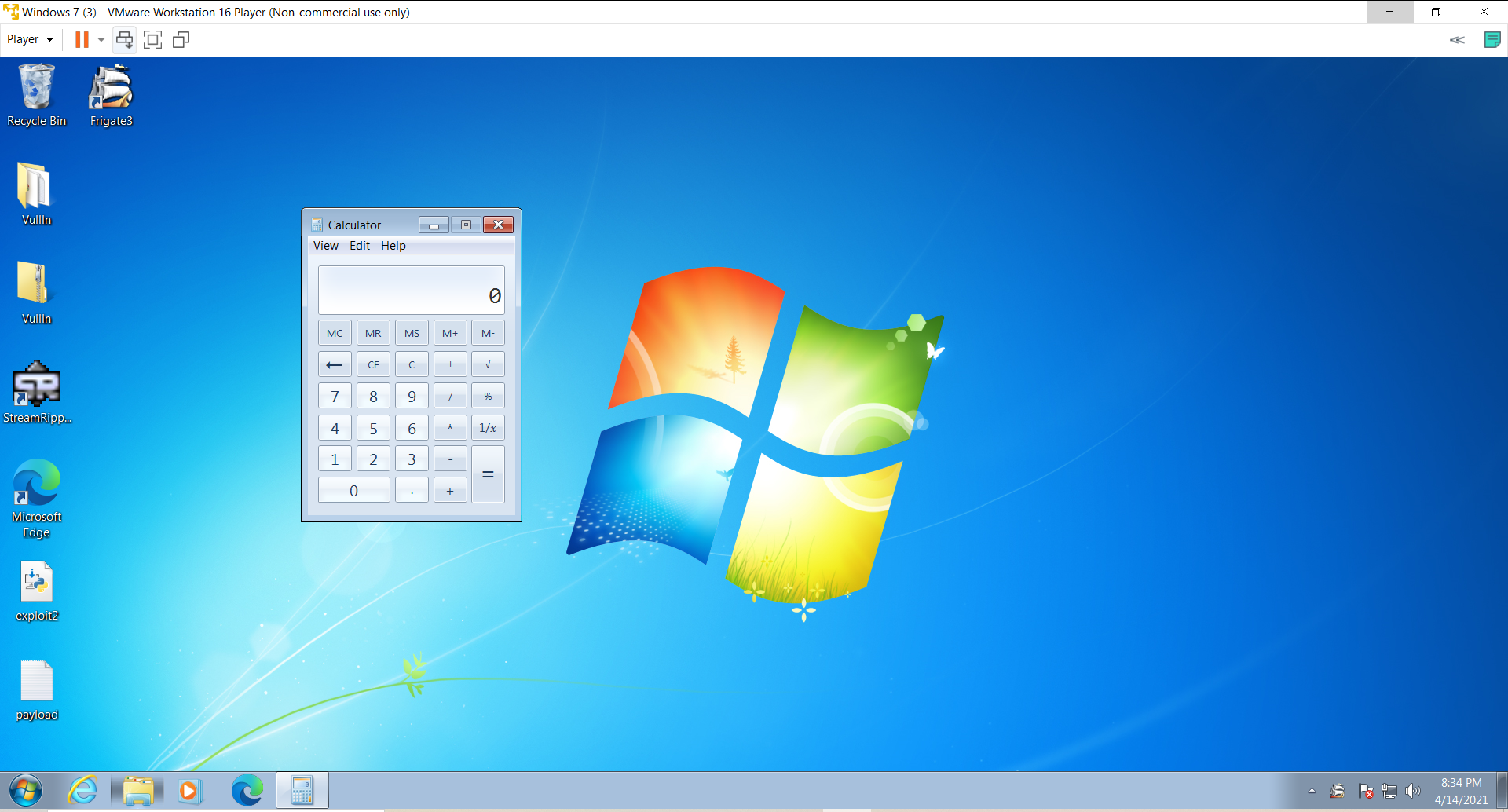


**3)After installing kali linux in vmware virtual machine using the iso , we use msfvenom to generate a similar code for a calculator**

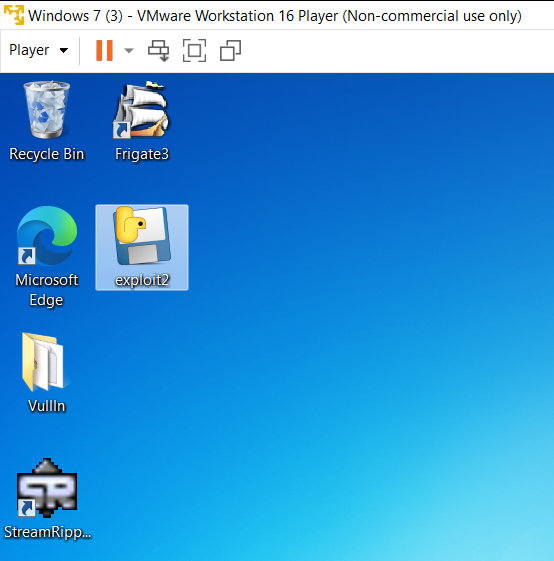


**4)After replacing the code , we again generate a payload and the run it in frigate .The application crashes and opens a calculator** .





**5) The .py file of exploit to converted to .exe file .**



**6) After downloading the debugger , the .exe file of exploit 2 is run in it .**

