Lab-8

Task

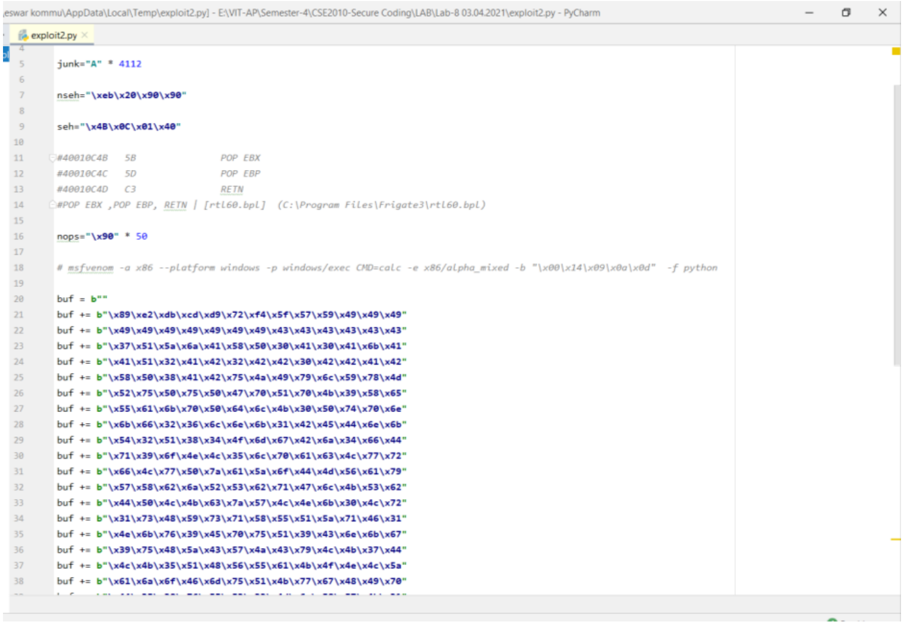
- **Download Vulln.zip from teams.**
- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**
- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**
- **Download and install python 2.7.* or 3.5.***
- **Run the exploit script II (exploit2.py- check today's folder) to generate the payload.**
    - **Replace the shellcode in the exploit2.py**
- **Install Vuln_Program_Stream.exe and Run the same**

Analysis

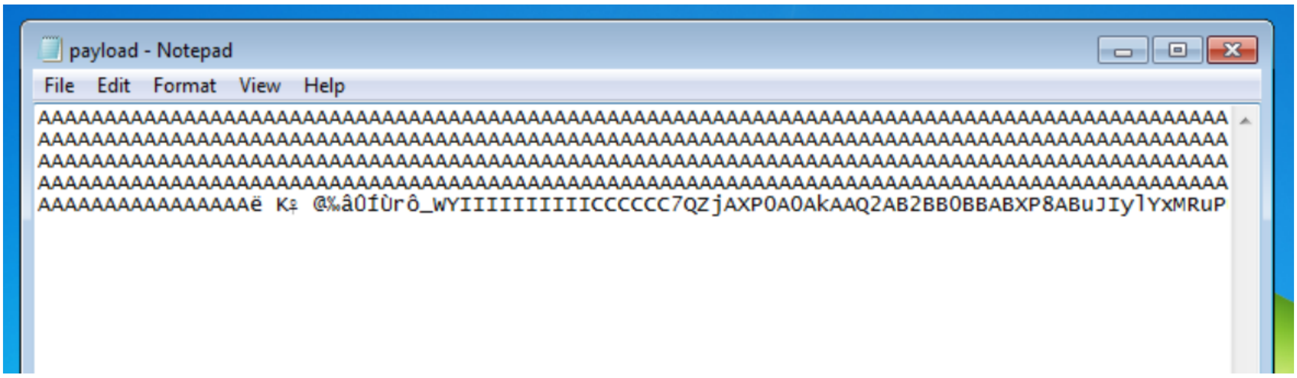
- **Try to crash the Vuln_Program_Stream program and exploit it.**
- **Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).**
  Example:
  msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
- **Change the default trigger to open control panel.**

Analysis- • Try to crash the Vuln_Program_Stream program and exploit it.

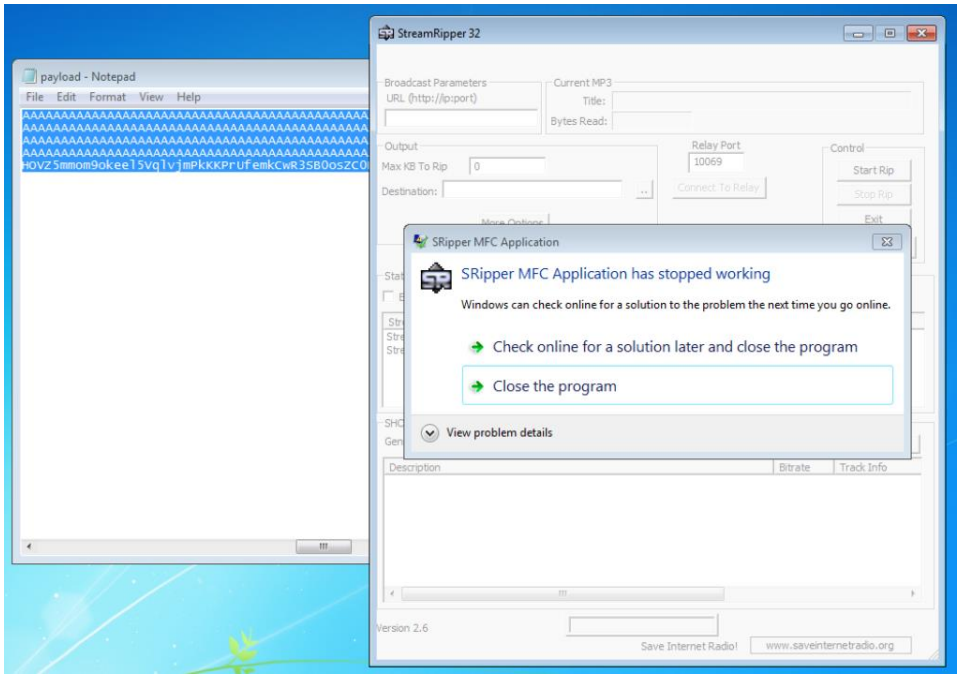
Script-



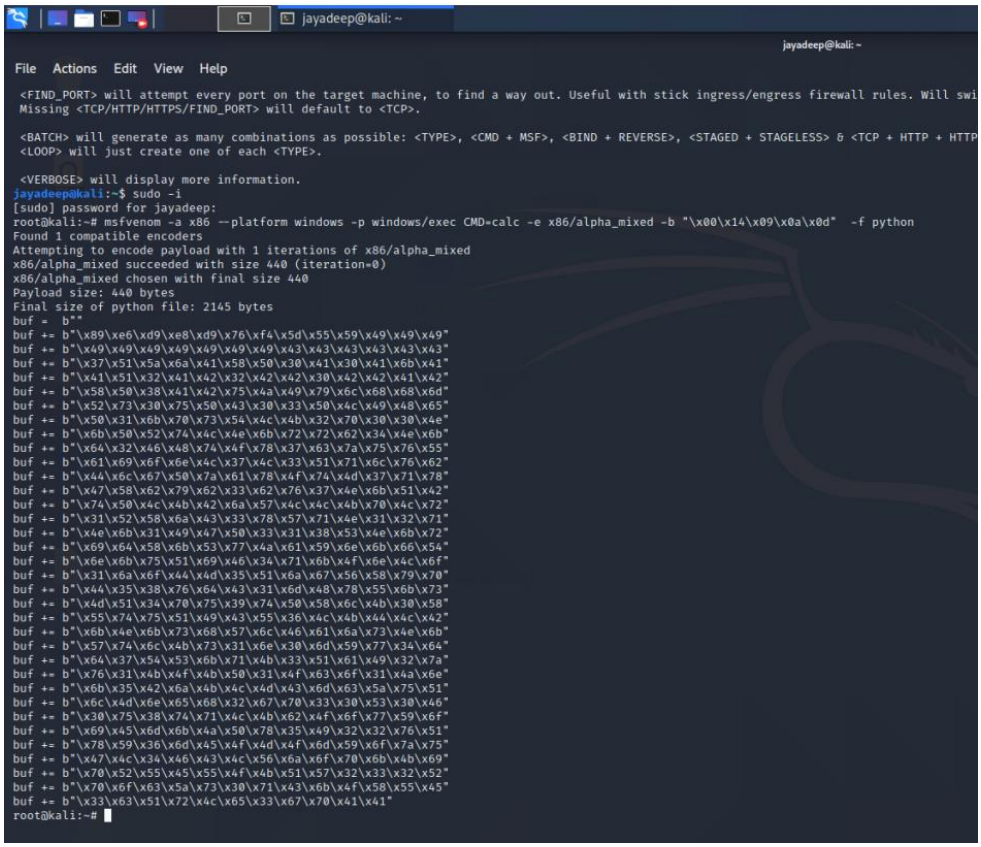
Payload Generated



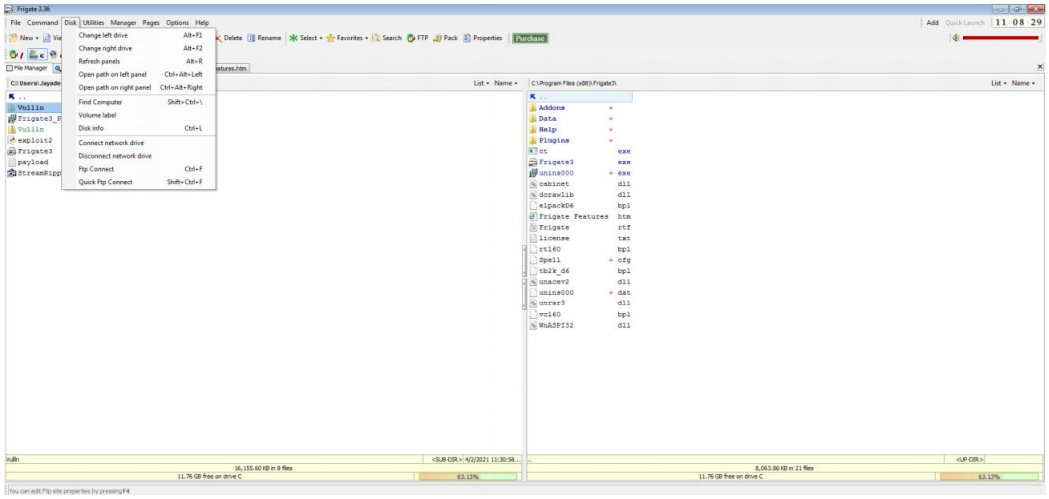
App Crashes

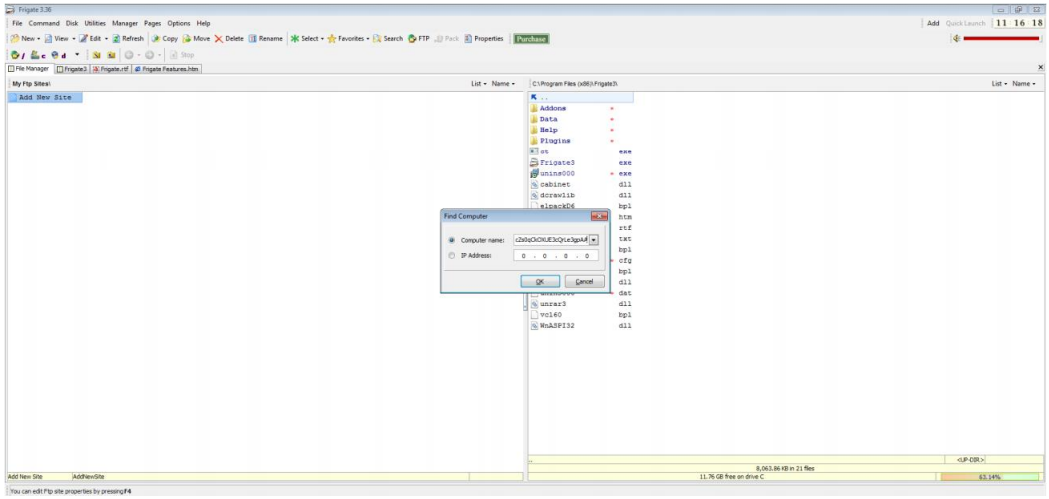


• Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).

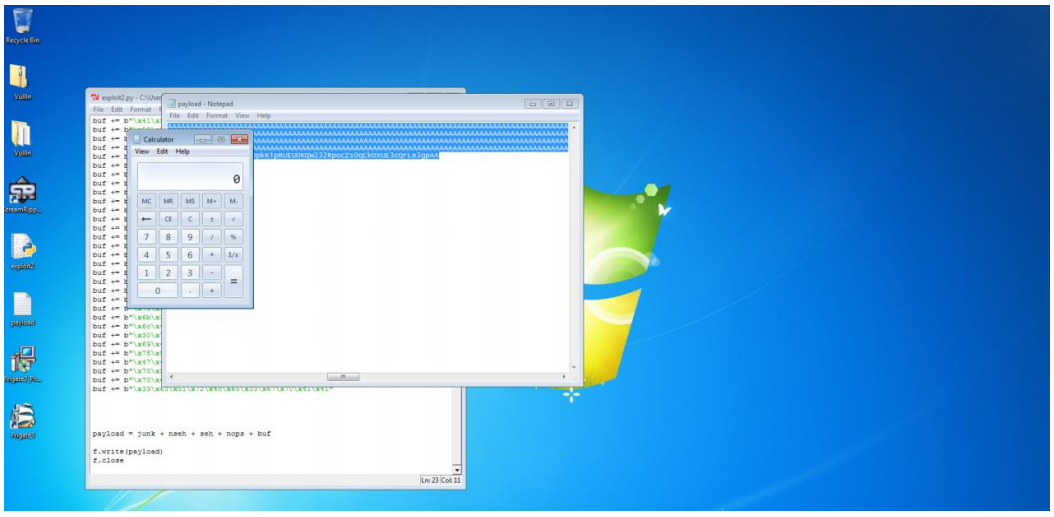


Copy pasting the Generated payload in exploit2.py and then using it in frigate

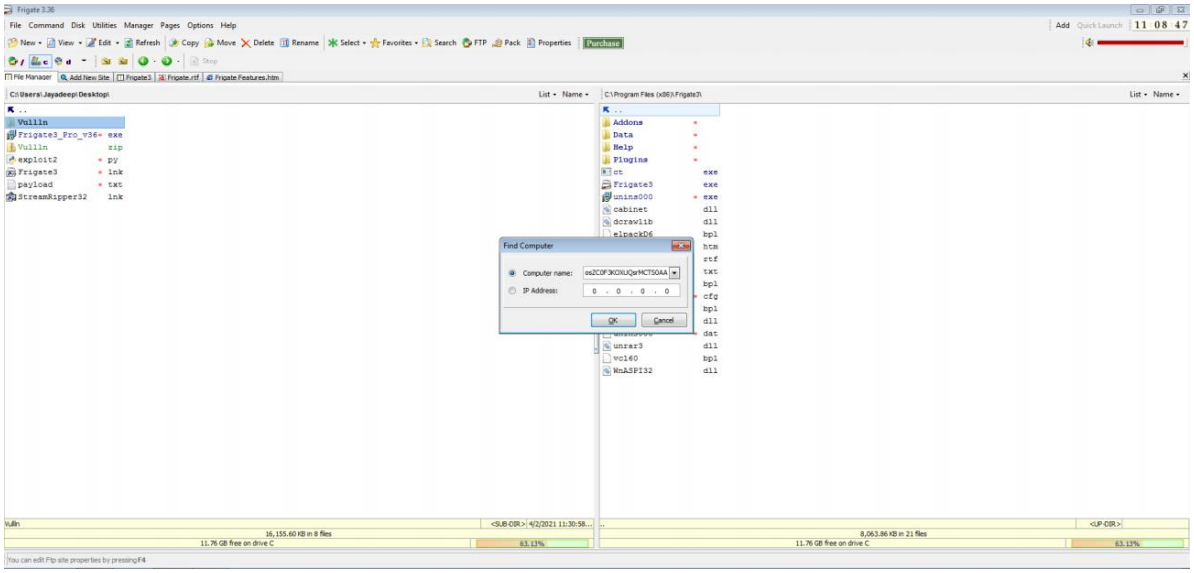




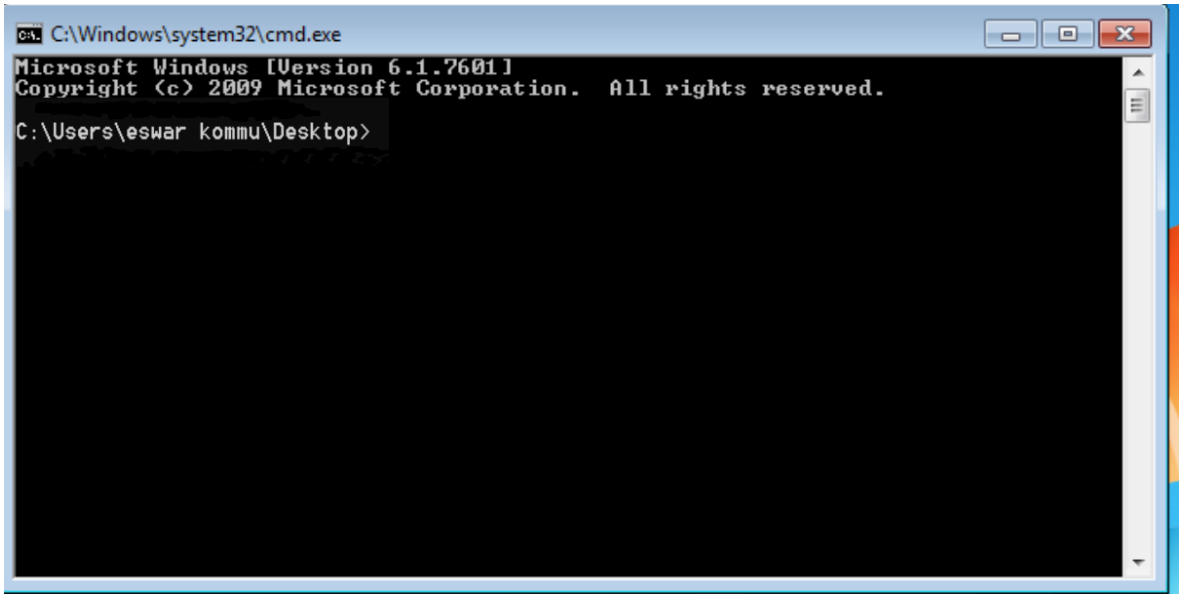
The app crashes and calculator opens



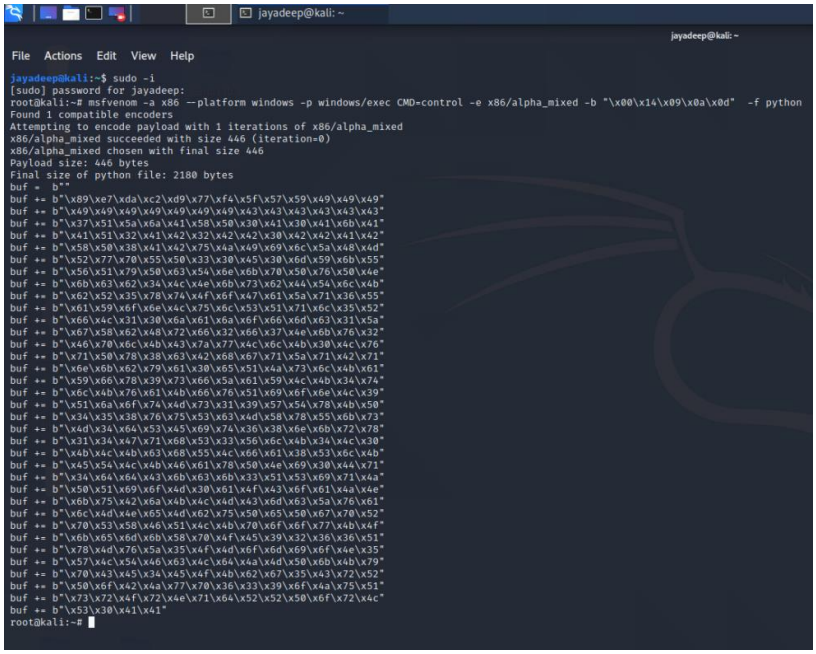
Similarly using payload for cmd



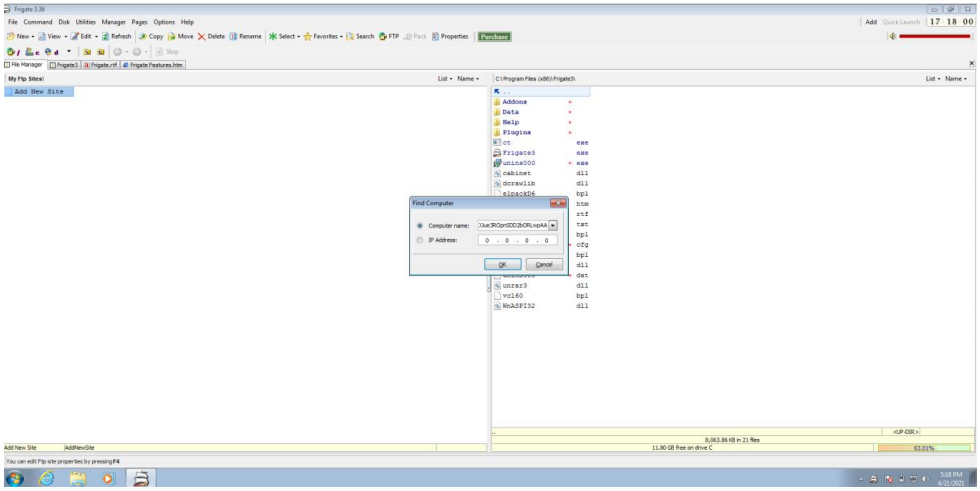
The App crashes and CMD opens



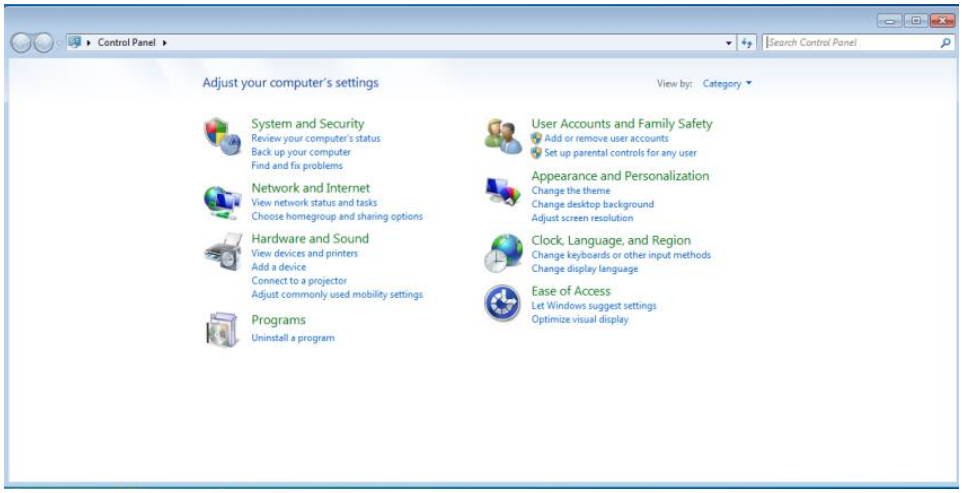
• Change the default trigger to open the control panel.



Copy pasting the Generated payload in exploit2.py and then using it in frigate



The app crashes and the control panel opens



K.Bala Eswar

19BCN7003