SECURE CODING CSE2010

LAB-8

CH.SAI SUMEDH

REG NO:-18BCN7092

SLOT:-L39+L40

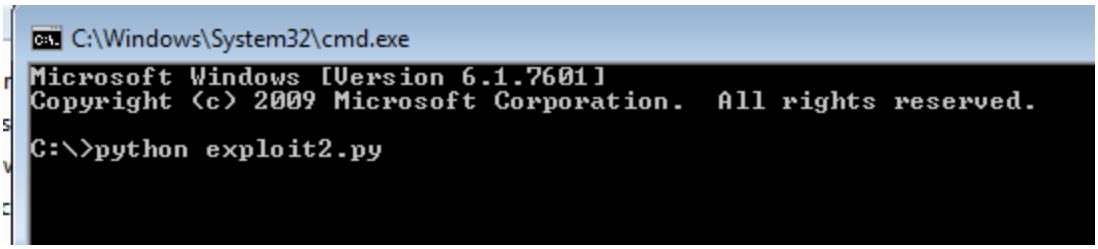
- **wLab experiment - Working with the memory vulnerabilities – Part II**

Task

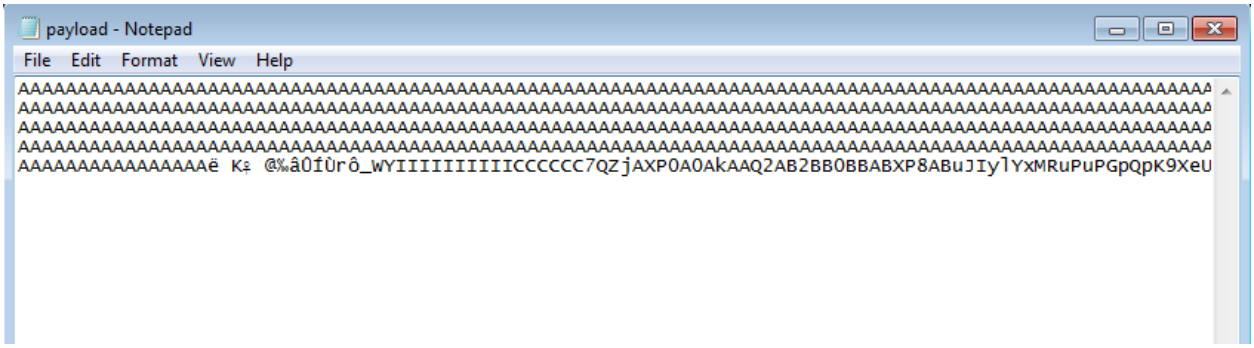
- **Download Vulln.zip from teams.**
- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**
- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**
- **Download and install python 2.7.* or 3.5.***
- **Run the exploit script II (exploit2.py- check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

Analysis

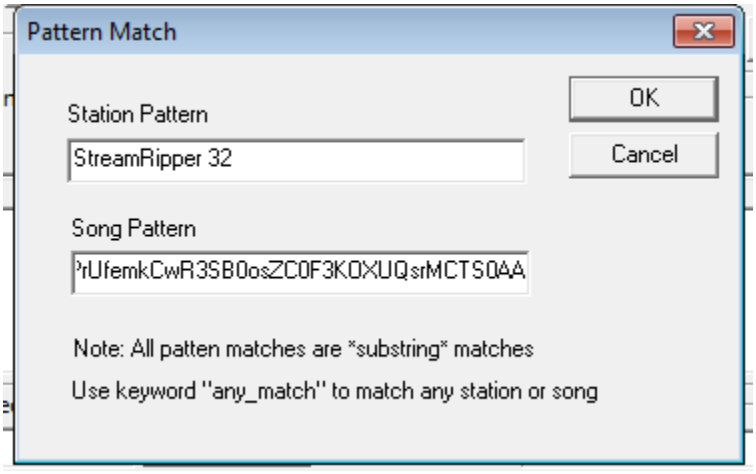
- **Try to crash the Vuln_Program_Stream program and exploit it.**
- **Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).**
  Example:
  msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
- **Change the default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



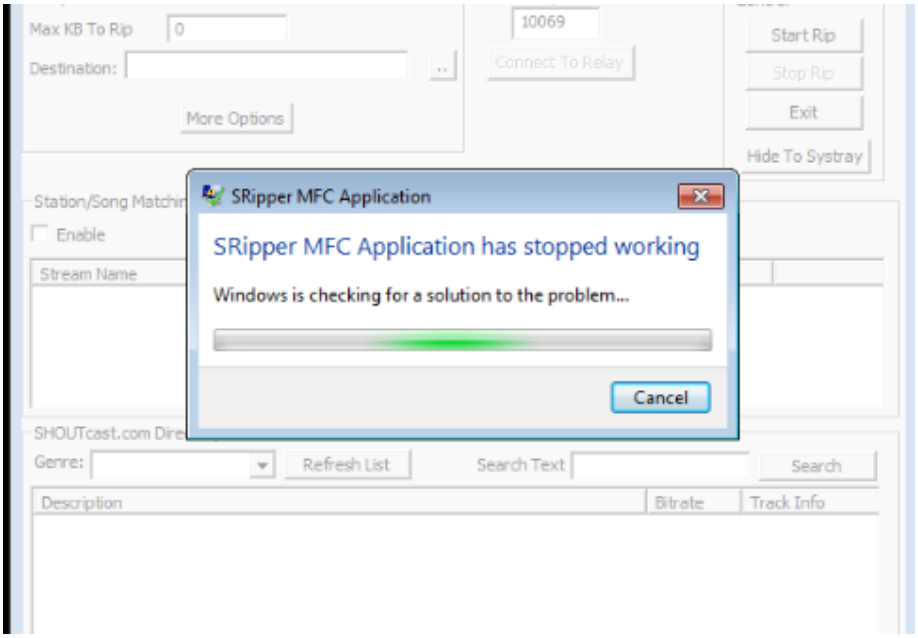
After executing the script file it will create a payload.

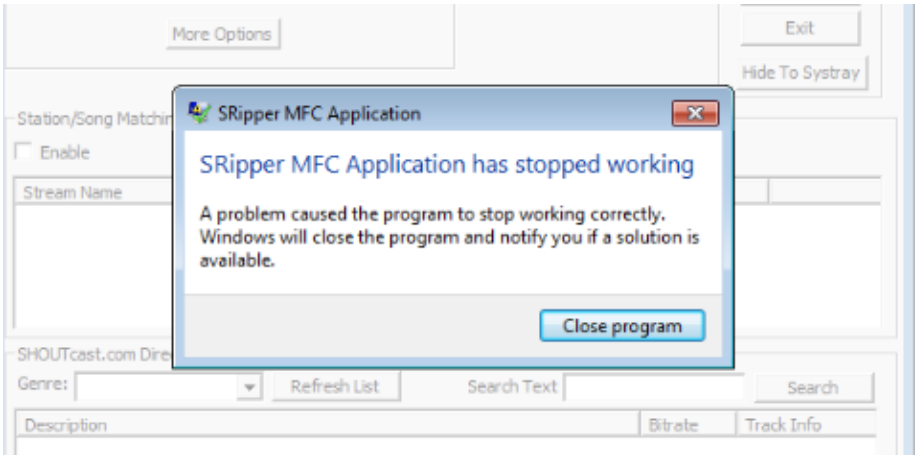


Now place that payload in the search pattern field.

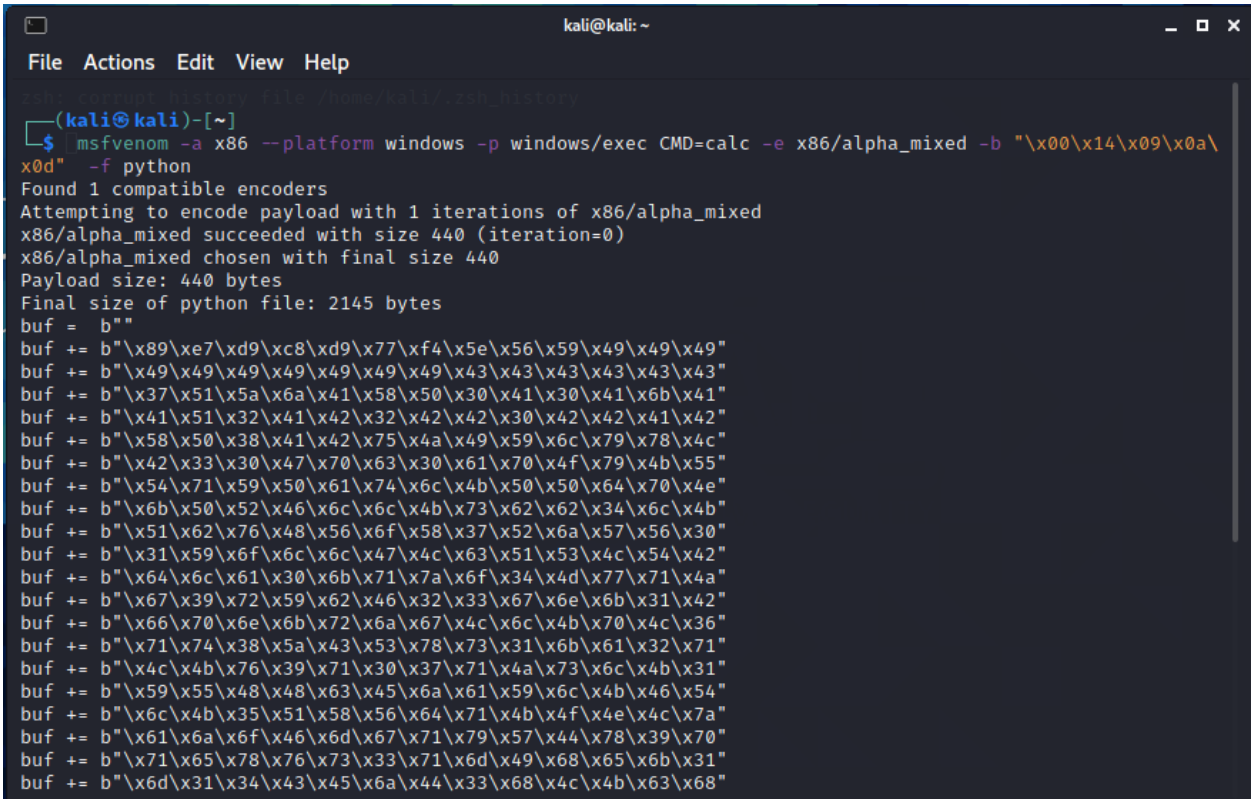


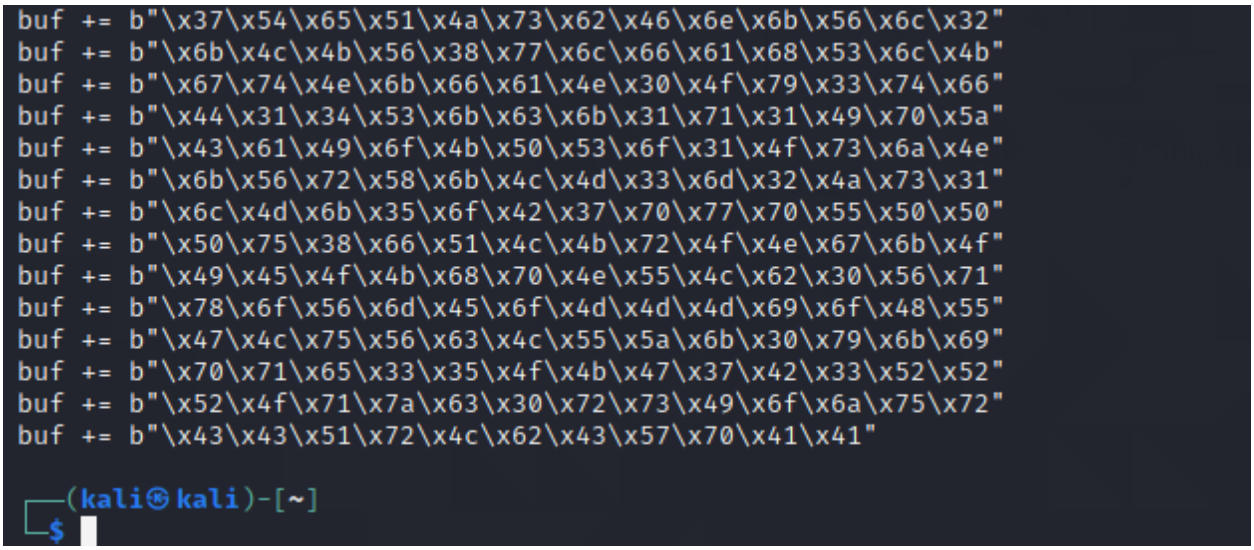
When I click ok the software gets crashed.





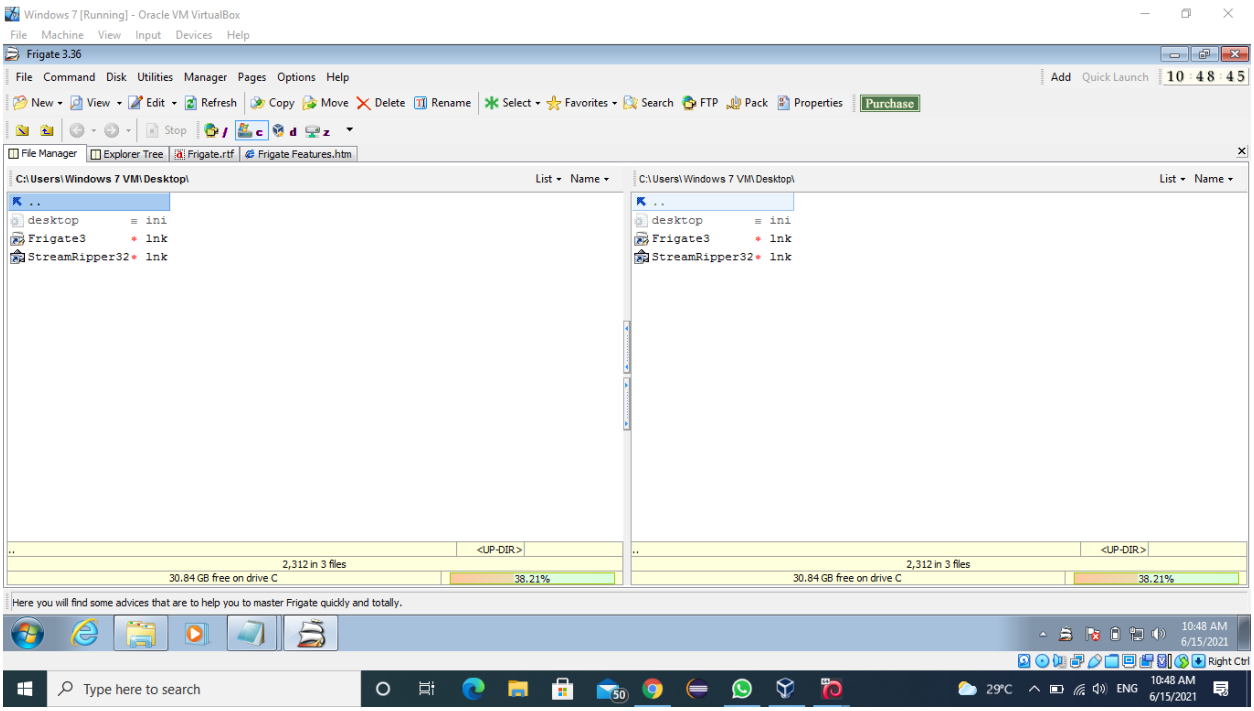
After executing the metasploit command:-



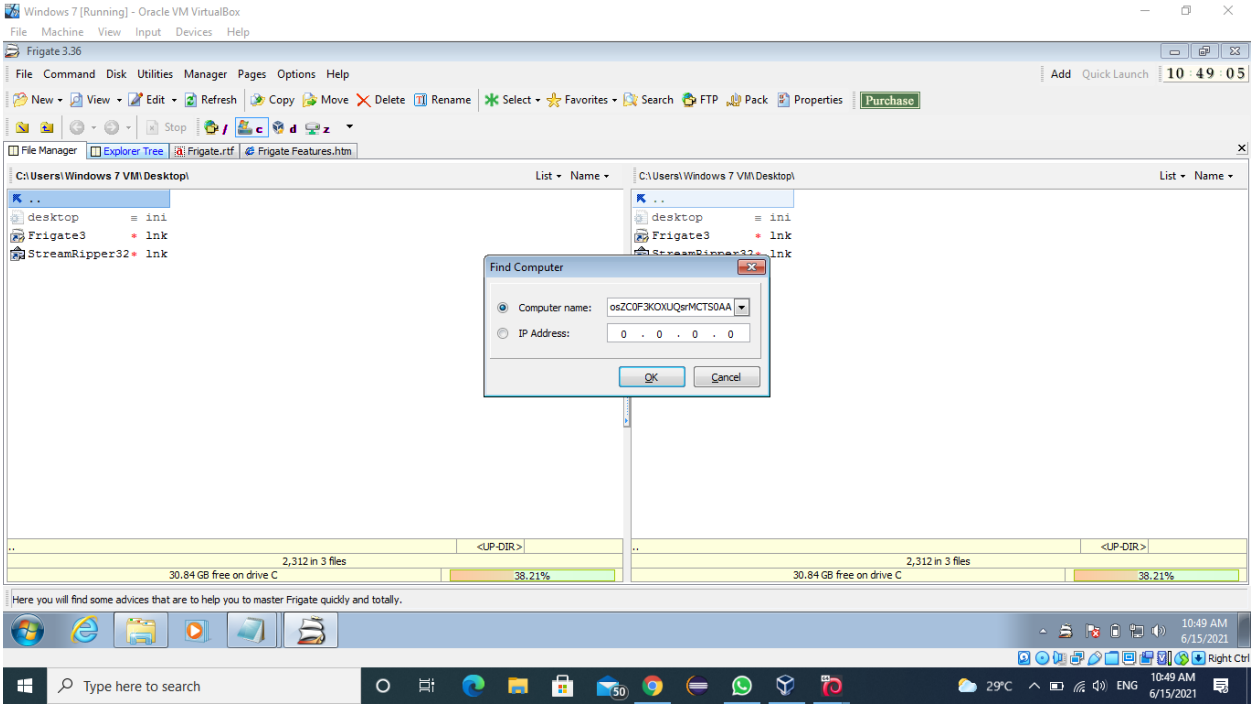


Download and install Frigate Software in your PC.

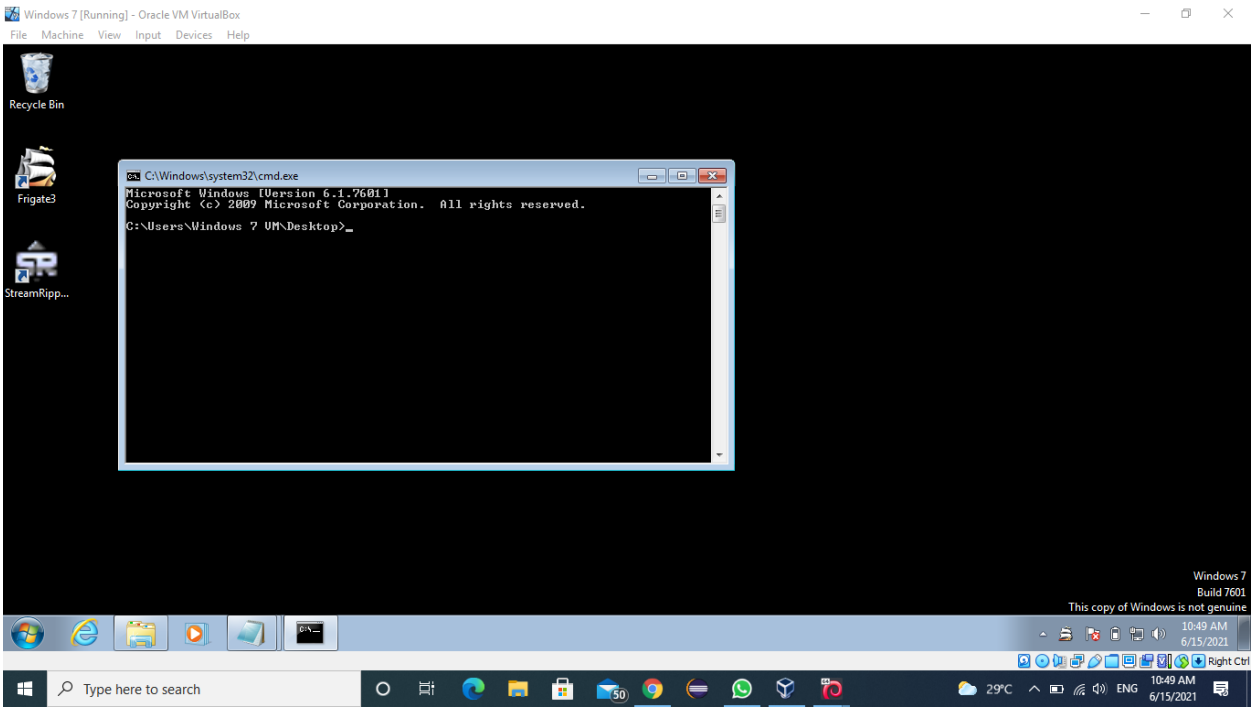
Now open Frigate and click on disks and click on find computer.



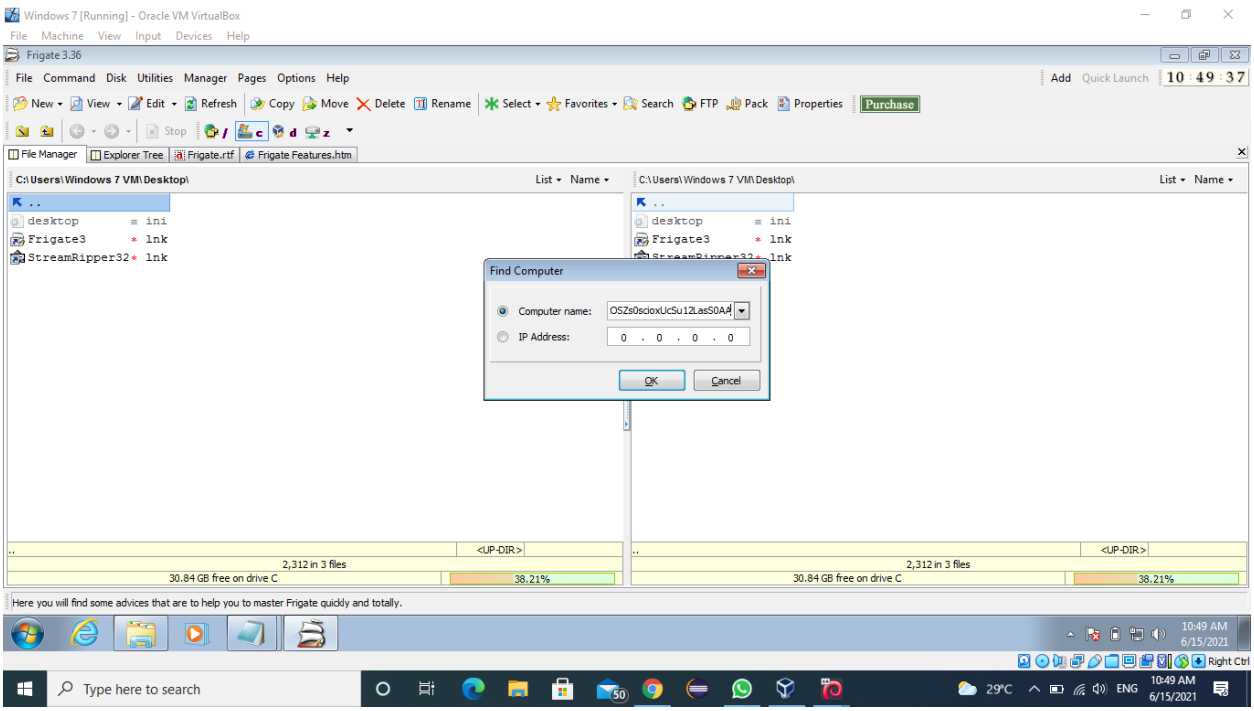
Now copy the payload which was generated in the beginning and paste it in the text field.

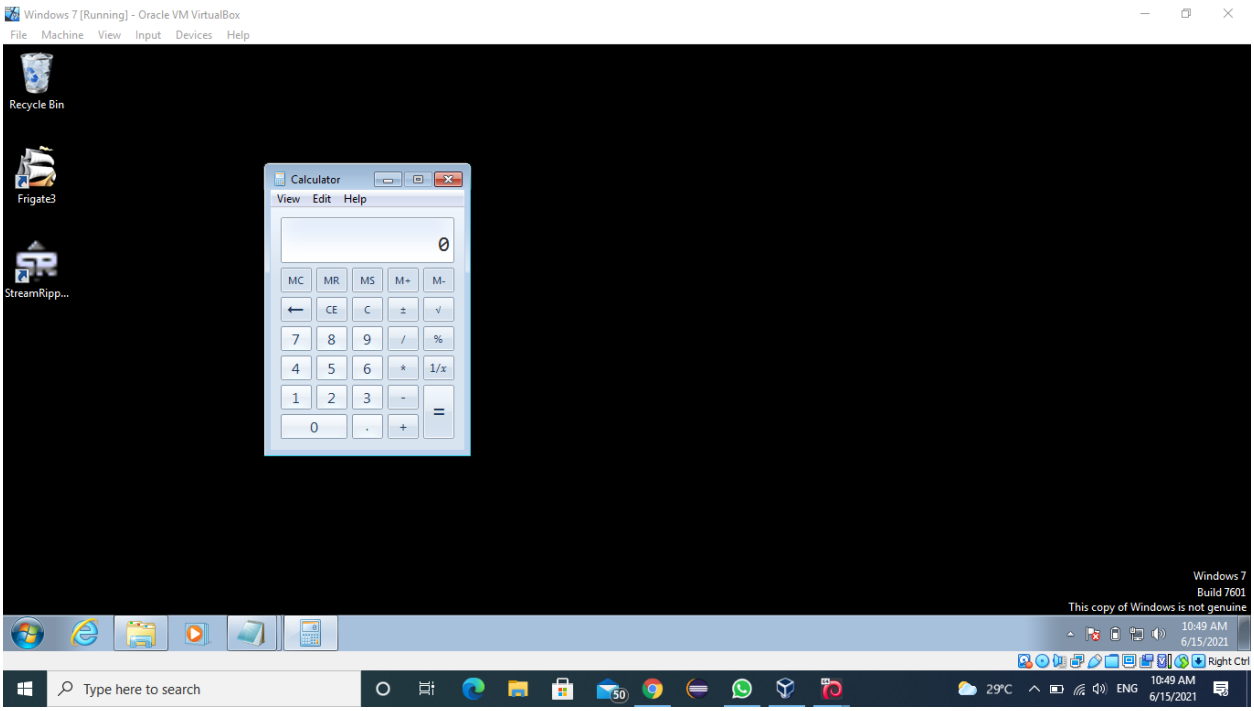


After executing that command the software crashed and it automatically opens Command Prompt.

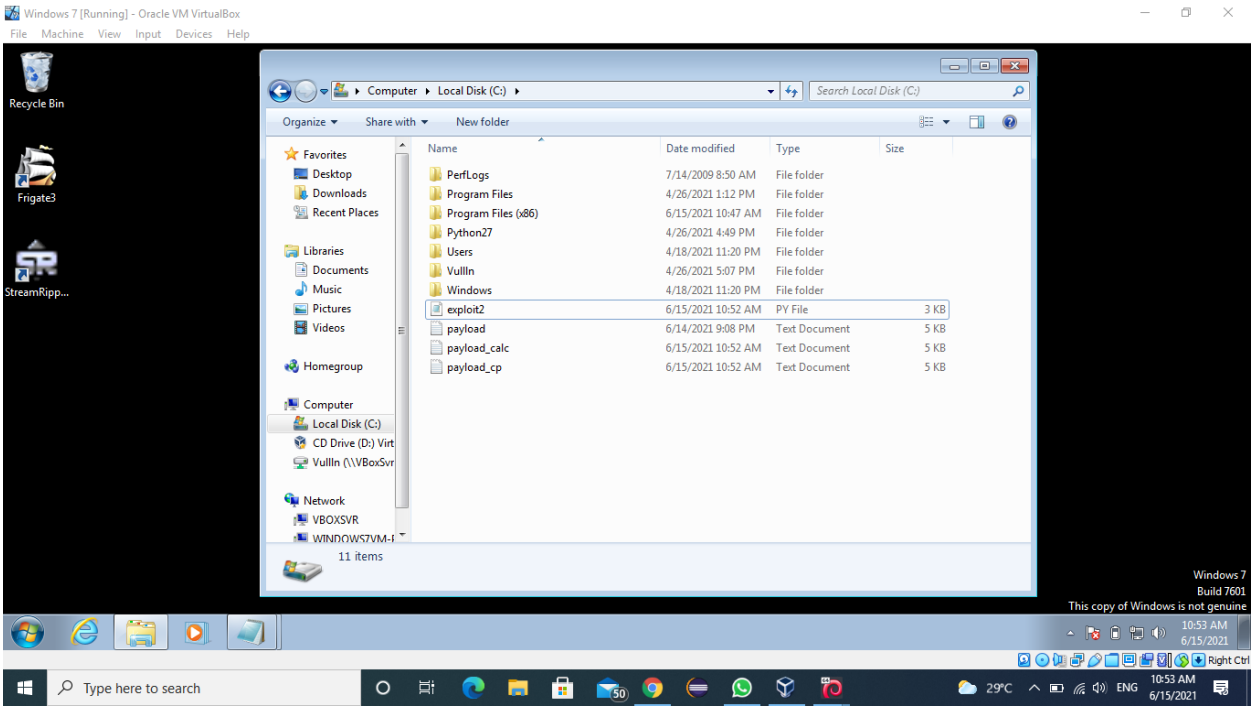


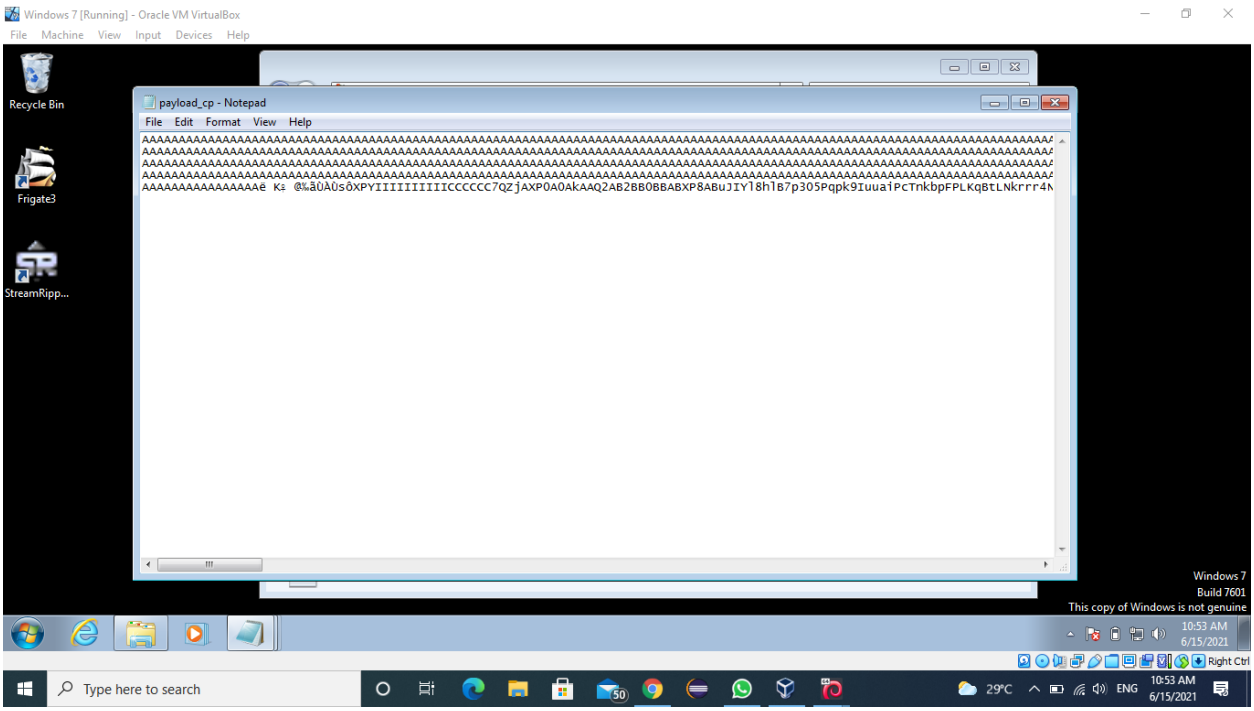
Now execute the command in kali linux to generate some code and paste it in python script then run that script it will give you another payload. Again do the same thing open frigate paste the payload in it then it will crash and opens calculator.

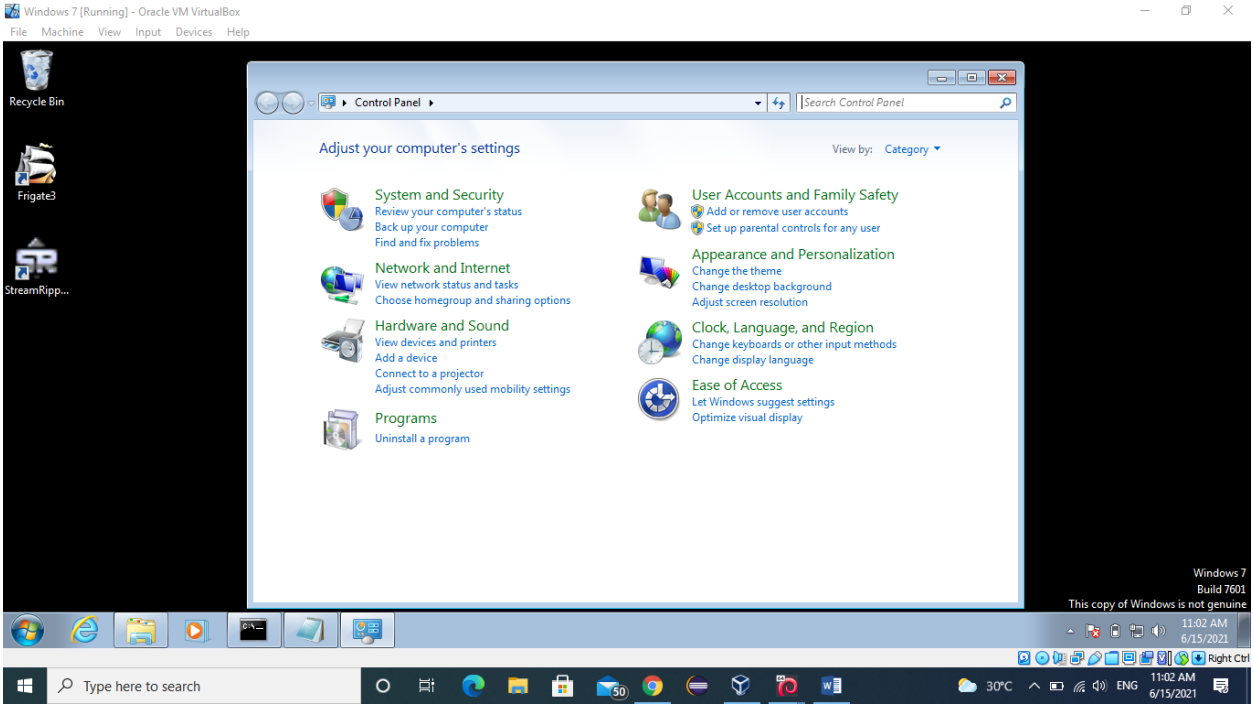




Now again run the code by changing the trigger to control panel and execute the same process, it will display control panel.




Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Frigate3
StreamRipp...
payload_cp - Notepad
File Edit Format View Help
Windows 7
Build 7601
This copy of Windows is not genuine
Type here to search
10:53 AM
6/15/2021
Right Ctrl


Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Frigate3
StreamRipp...
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Connect to a projector
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display
Windows 7
Build 7601
This copy of Windows is not genuine
Type here to search
11:02 AM
6/15/2021
Right Ctrl