

SECURE CODING

CSE-2010

LAB ASSIGNMENT -8

Name :HARSHA VARDHAN

Reg.No : 18BCN7133

Slot : 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- check today's folder) to generate the payload.**
 - **Replace the shellcode in the exploit2.py**
- **Install Vuln_Program_Stream.exe and Run the same**

Analysis

- **Try to crash the Vuln_Program_Stream program and exploit it.**
- **Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).**

Example:

```
msfvenom -a x86 --platform windows -p windows/exec  
CMD=calc -e x86/alpha_mixed -b  
"\x00\x14\x09\x0a\x0d" -f python
```

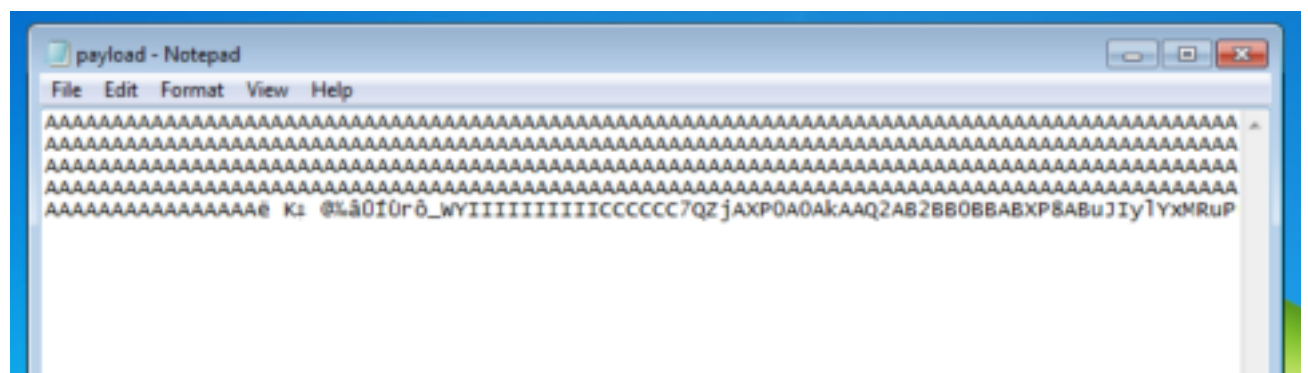
- **Change the default trigger to open control panel.**
- Analysis- • Try to crash the Vuln_Program_Stream program and exploit it.

```

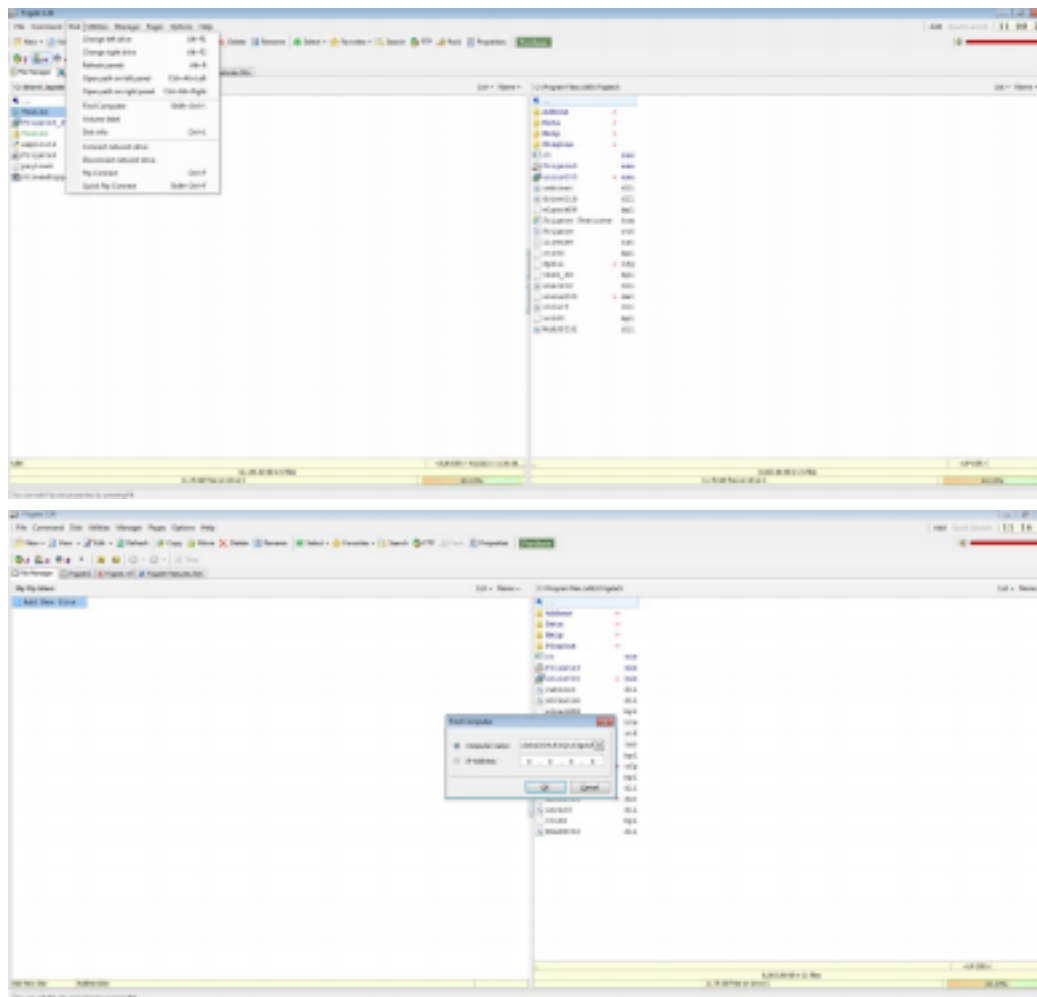
1  #include <stdio.h>
2  #include <string.h>
3  #include <stdlib.h>
4  #include <unistd.h>
5  #include <sys/types.h>
6  #include <sys/stat.h>
7  #include <fcntl.h>
8  #include <sys/mman.h>
9  #include <sys/time.h>
10 #include <sys/wait.h>
11 #include <sys/resource.h>
12 #include <sys/param.h>
13 #include <sys/uio.h>
14 #include <sys/sysmacros.h>
15 #include <sys/unistd.h>
16 #include <sys/ioctl.h>
17 #include <sys/mount.h>
18 #include <sys/procfs.h>
19 #include <sys/proc.h>
20 #include <sys/procfs.h>
21 #include <sys/procfs.h>
22 #include <sys/procfs.h>
23 #include <sys/procfs.h>
24 #include <sys/procfs.h>
25 #include <sys/procfs.h>
26 #include <sys/procfs.h>
27 #include <sys/procfs.h>
28 #include <sys/procfs.h>
29 #include <sys/procfs.h>
30 #include <sys/procfs.h>
31 #include <sys/procfs.h>
32 #include <sys/procfs.h>
33 #include <sys/procfs.h>
34 #include <sys/procfs.h>
35 #include <sys/procfs.h>
36 #include <sys/procfs.h>
37 #include <sys/procfs.h>
38 #include <sys/procfs.h>
39 #include <sys/procfs.h>
40 #include <sys/procfs.h>
41 #include <sys/procfs.h>
42 #include <sys/procfs.h>
43 #include <sys/procfs.h>
44 #include <sys/procfs.h>
45 #include <sys/procfs.h>
46 #include <sys/procfs.h>
47 #include <sys/procfs.h>
48 #include <sys/procfs.h>
49 #include <sys/procfs.h>
50 #include <sys/procfs.h>
51 #include <sys/procfs.h>
52 #include <sys/procfs.h>
53 #include <sys/procfs.h>
54 #include <sys/procfs.h>
55 #include <sys/procfs.h>
56 #include <sys/procfs.h>
57 #include <sys/procfs.h>
58 #include <sys/procfs.h>
59 #include <sys/procfs.h>
60 #include <sys/procfs.h>
61 #include <sys/procfs.h>
62 #include <sys/procfs.h>
63 #include <sys/procfs.h>
64 #include <sys/procfs.h>
65 #include <sys/procfs.h>
66 #include <sys/procfs.h>
67 #include <sys/procfs.h>
68 #include <sys/procfs.h>
69 #include <sys/procfs.h>
70 #include <sys/procfs.h>
71 #include <sys/procfs.h>
72 #include <sys/procfs.h>
73 #include <sys/procfs.h>
74 #include <sys/procfs.h>
75 #include <sys/procfs.h>
76 #include <sys/procfs.h>
77 #include <sys/procfs.h>
78 #include <sys/procfs.h>
79 #include <sys/procfs.h>
80 #include <sys/procfs.h>
81 #include <sys/procfs.h>
82 #include <sys/procfs.h>
83 #include <sys/procfs.h>
84 #include <sys/procfs.h>
85 #include <sys/procfs.h>
86 #include <sys/procfs.h>
87 #include <sys/procfs.h>
88 #include <sys/procfs.h>
89 #include <sys/procfs.h>
90 #include <sys/procfs.h>
91 #include <sys/procfs.h>
92 #include <sys/procfs.h>
93 #include <sys/procfs.h>
94 #include <sys/procfs.h>
95 #include <sys/procfs.h>
96 #include <sys/procfs.h>
97 #include <sys/procfs.h>
98 #include <sys/procfs.h>
99 #include <sys/procfs.h>
100 #include <sys/procfs.h>

```

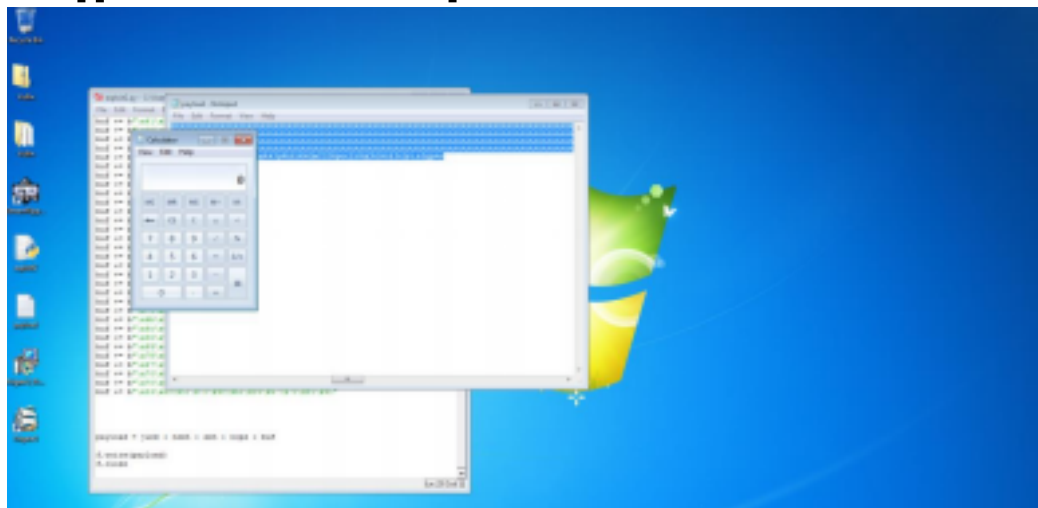
Payload Generated



App Crashes



The app crashes and calculator opens



Similarly using payload for cmd



```
Microsoft Windows [Version 10.0.18363.1440]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\harib>
```

- Change the default trigger to open the control panel.

