## Runningtheexploit2.pyfiletogeneratepayload

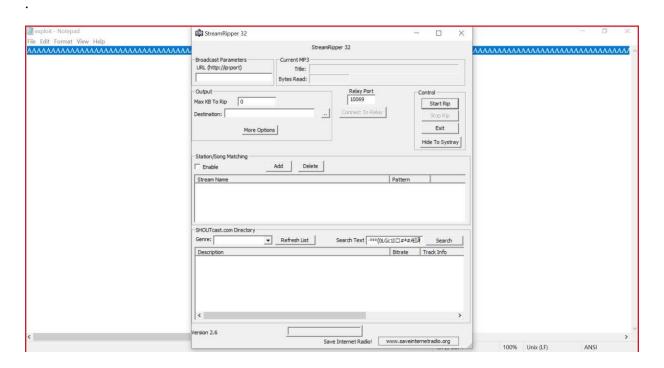
>python2exploit2.py

After successfully running the python file it will generate a.txt file along with the payload.

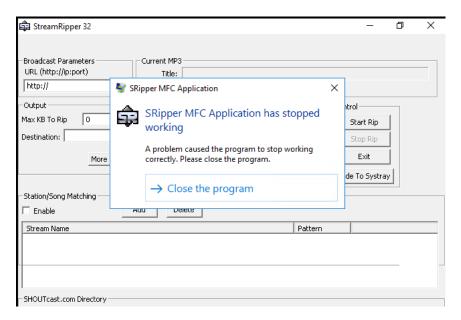
>notepadexploit2.txt

## Now,installVulnerableapplication(StreamRipper32).

After installing the application copy paste the payload in these archbox and click on Search button



By exploiting buffer overflow vulnerabilitiy we have crashed the application.



## **Tryingtoerasehdd**

```
C:\WINDOWS\system32>diskpart
Microsoft DiskPart version 10.0.19041.964
Copyright (C) Microsoft Corporation.
On computer: DESKTOP-U6VV86T
DISKPART>
DISKPART> list disk
 Disk ###
            Status
                           Size
                                     Free
                                              Dyn
                                                   Gpt
 Disk 0
            Online
                            476 GB
                                         0 B
DISKPART> select disk 0
Disk 0 is now the selected disk.
DISKPART> clean
```