

SECURE CODING LAB REPORT:

DATE: 24 MARCH 2021

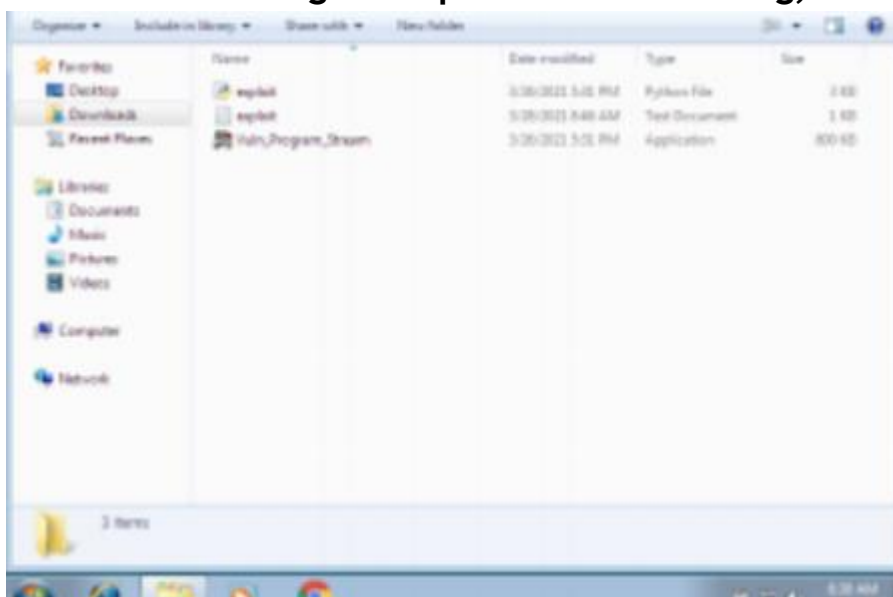
SUKHMANI SANDHU

18BCE7155

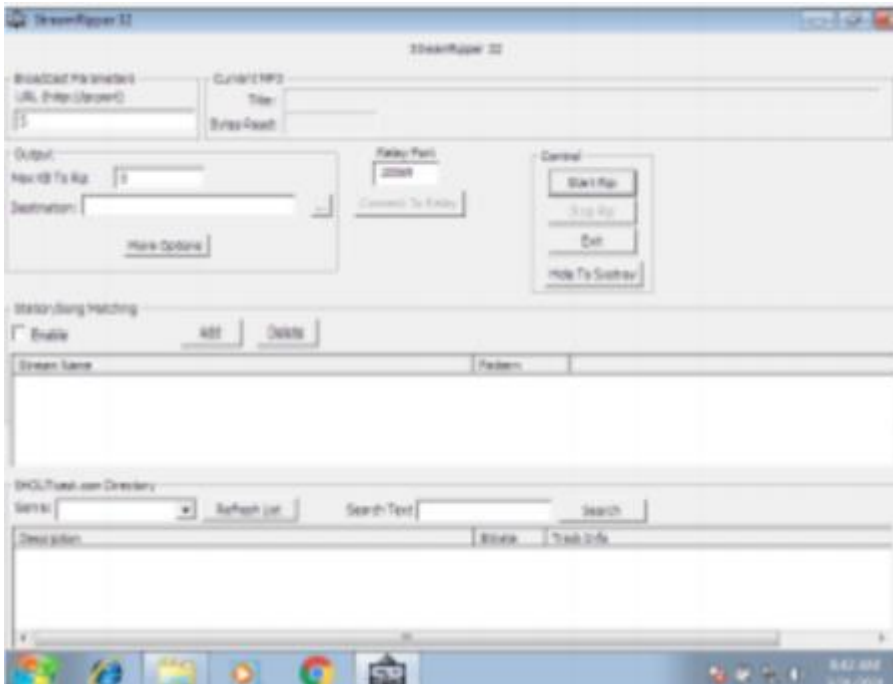
The first thing we start with is the setup of our Windows 7 virtual instance and then the download and installing of Python



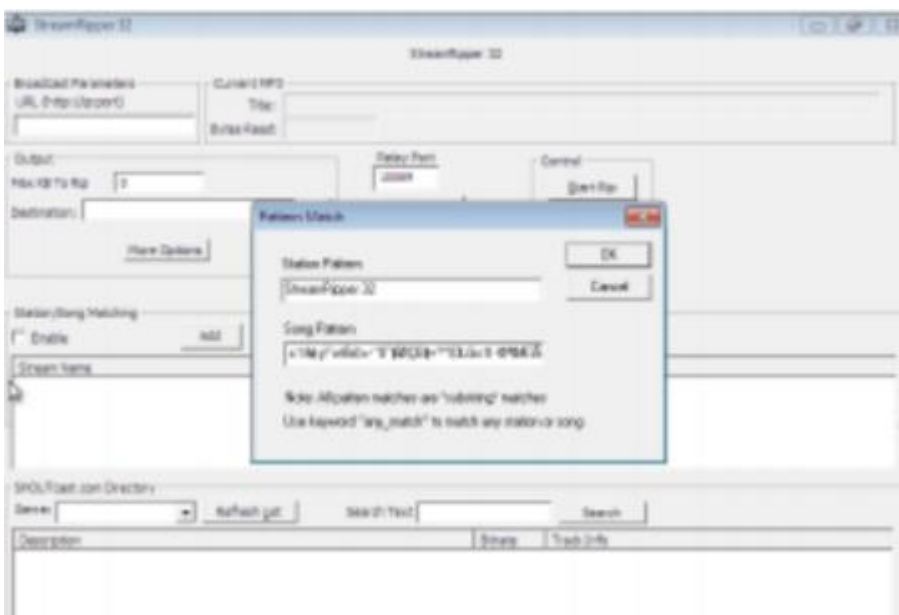
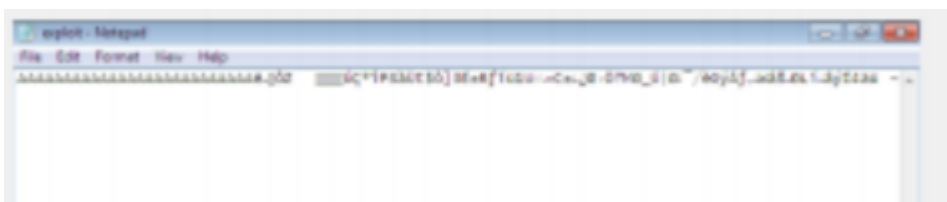
After downloading the zip file and extracting,



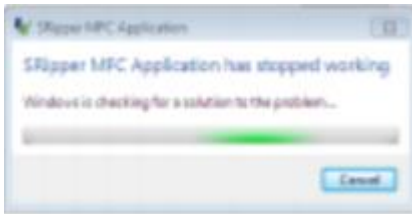
From the app, we are trying to find a malicious vulnerability file, StreamRipper32



Now, we execute the file we get a an executable which contains the attack payload



When we copy and paste it, there will be a crash in the system



Now, the reasons for this crash,:

The input field has no restrictions on the number of characters allowed, not on user side. So when it exceeds 256 characters, there will be a buffer overflow. That will cause the application to crash- especially if there is no proper exception handling method. This vulnerability can be fixed in two ways.

Creating a restriction on the number of characters in the field and validating the input.

And creating proper methods to handle exceptions that will avoid the total shutdown of the application