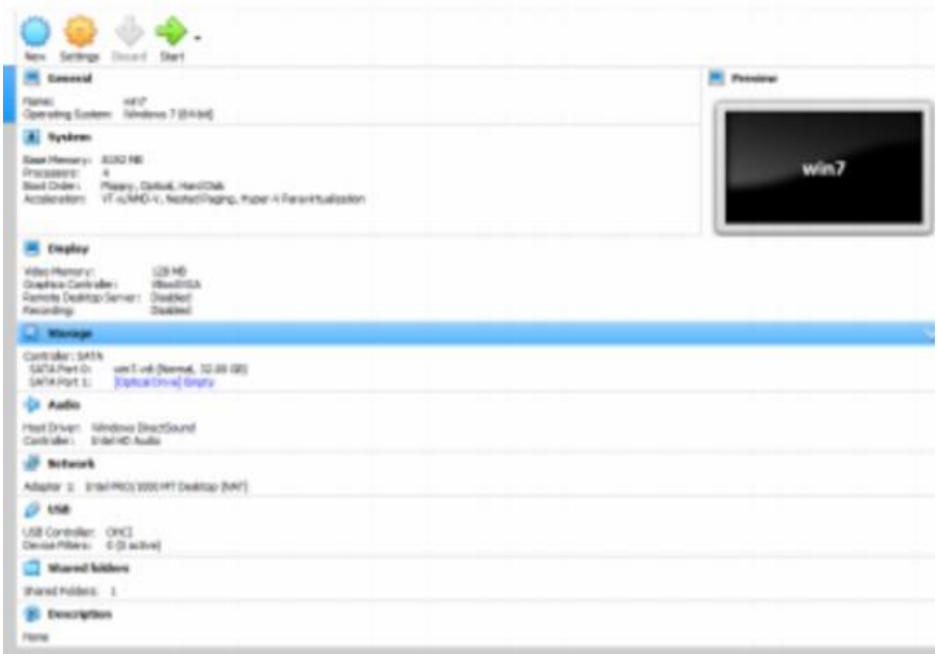
Secure Coding Lab-7

S.Poojith
18BCN7032

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



General
Name: win7
Operating System: Windows 7 (64-bit)

System
Base Memory: 8192 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: SATA
SATA Port 0: win7.vdi (Normal, 32.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio
Host Driver: Windows DirectSound
Controller: Intel HD Audio

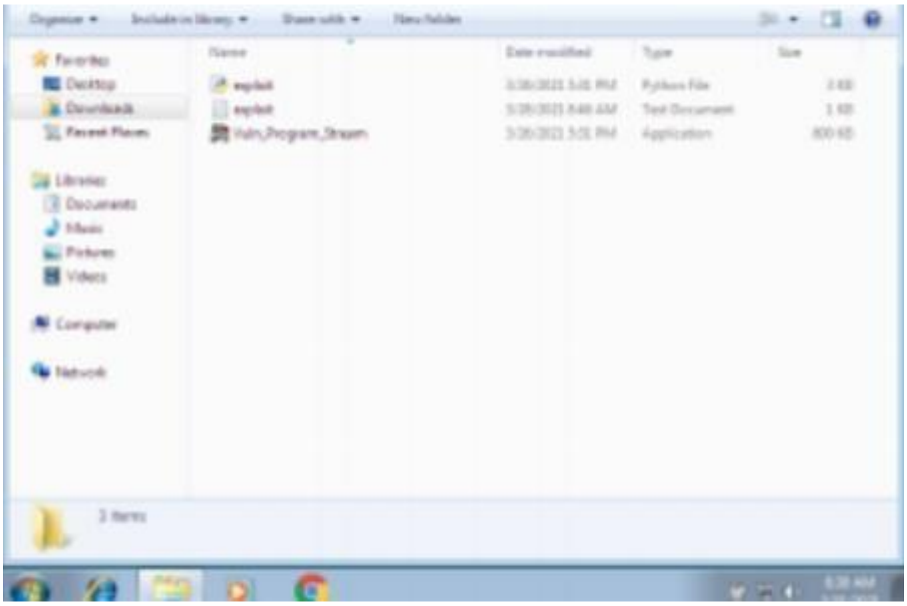
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders
Shared Folders: 1

Description
None

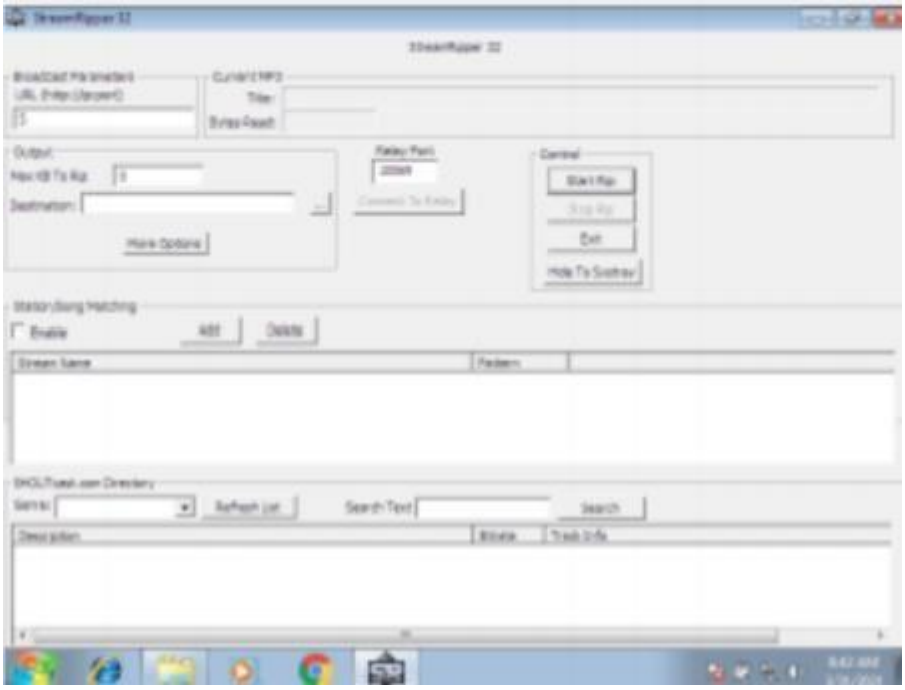
After downloading the zip file and extracting,



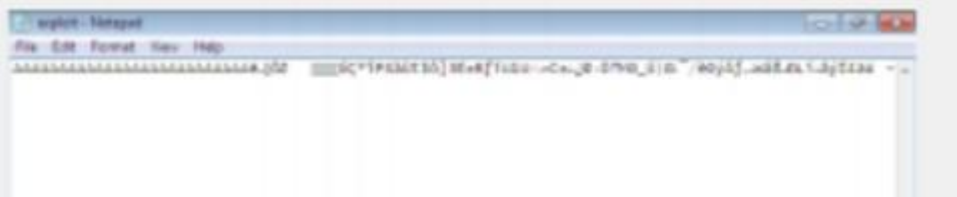
Name	Date modified	Type	Size
exploit	3/26/2021 5:01 PM	Python File	3 KB
exploit	5/28/2021 8:48 AM	Text Document	1 KB
Vuln_Program_Stream	3/26/2021 5:01 PM	Application	400 KB

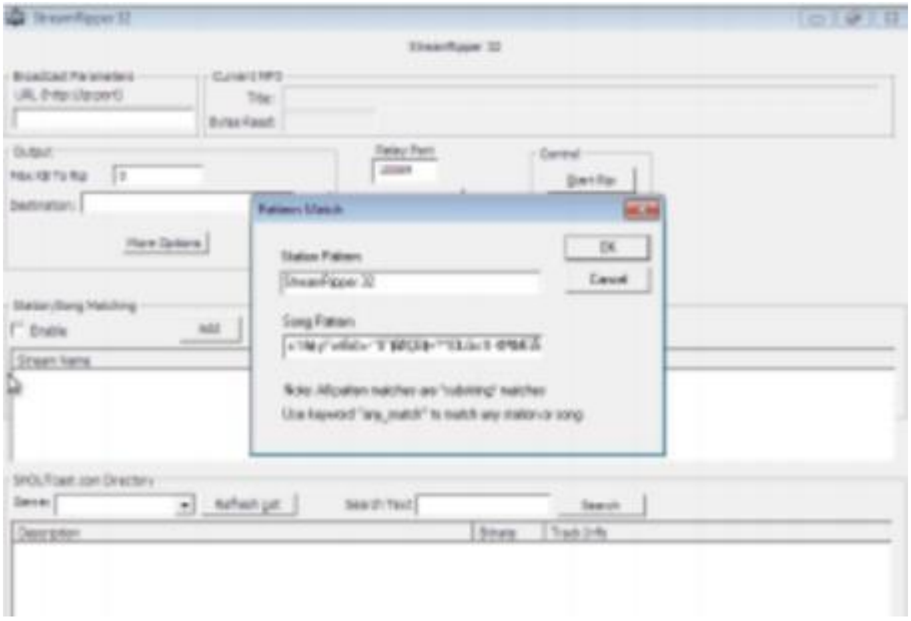
3 items

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 attackpayload





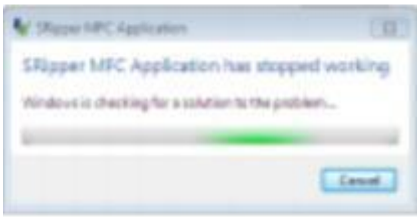
Station Pattern: StreamRipper 32

Song Pattern: [illegible]

Note: All pattern matches are "substring" matches

Use keyword "any_match" to match any station or song

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



SRipper MFC Application

SRipper MFC Application has stopped working

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

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 validatingthe input.
And creating proper methods to handle exceptions that will avoid the totalshutdown of the application