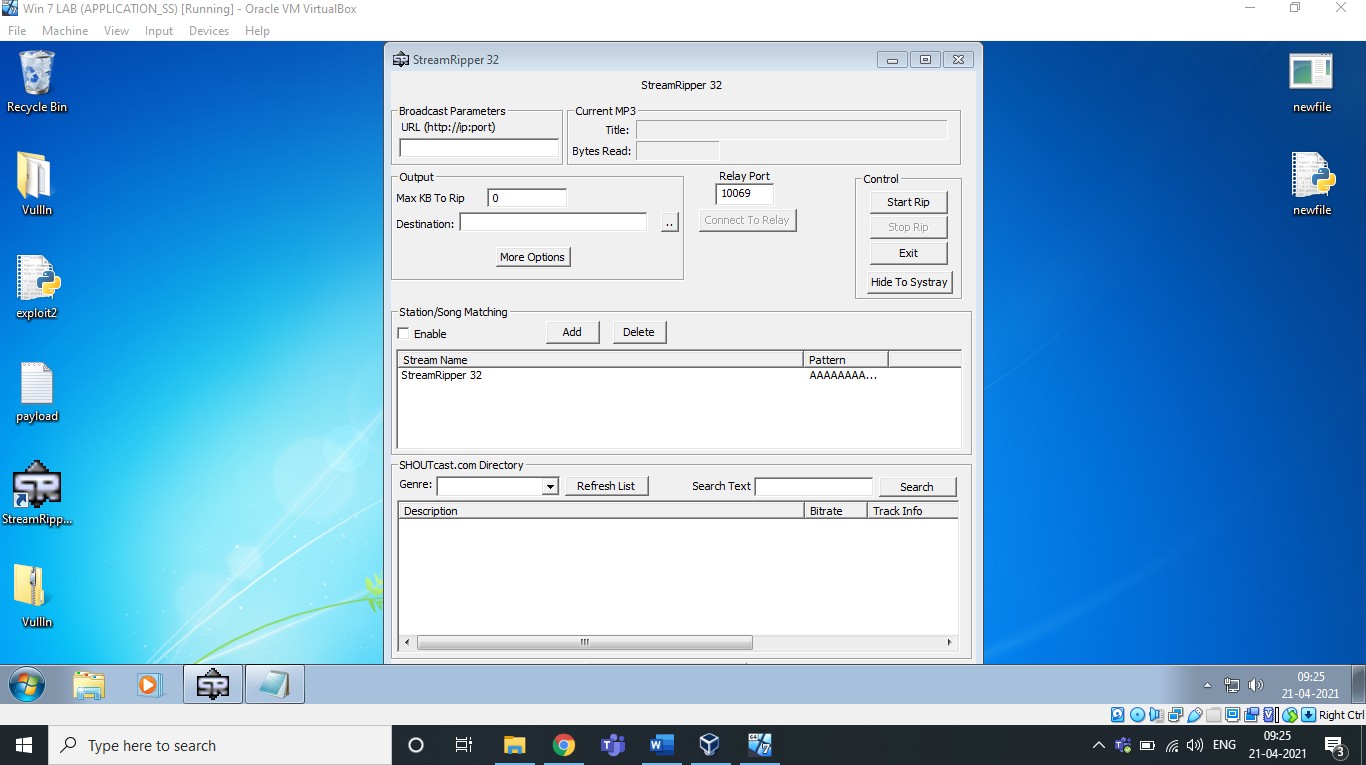
Secure Coding Lab-9

Chekuri.mahesh

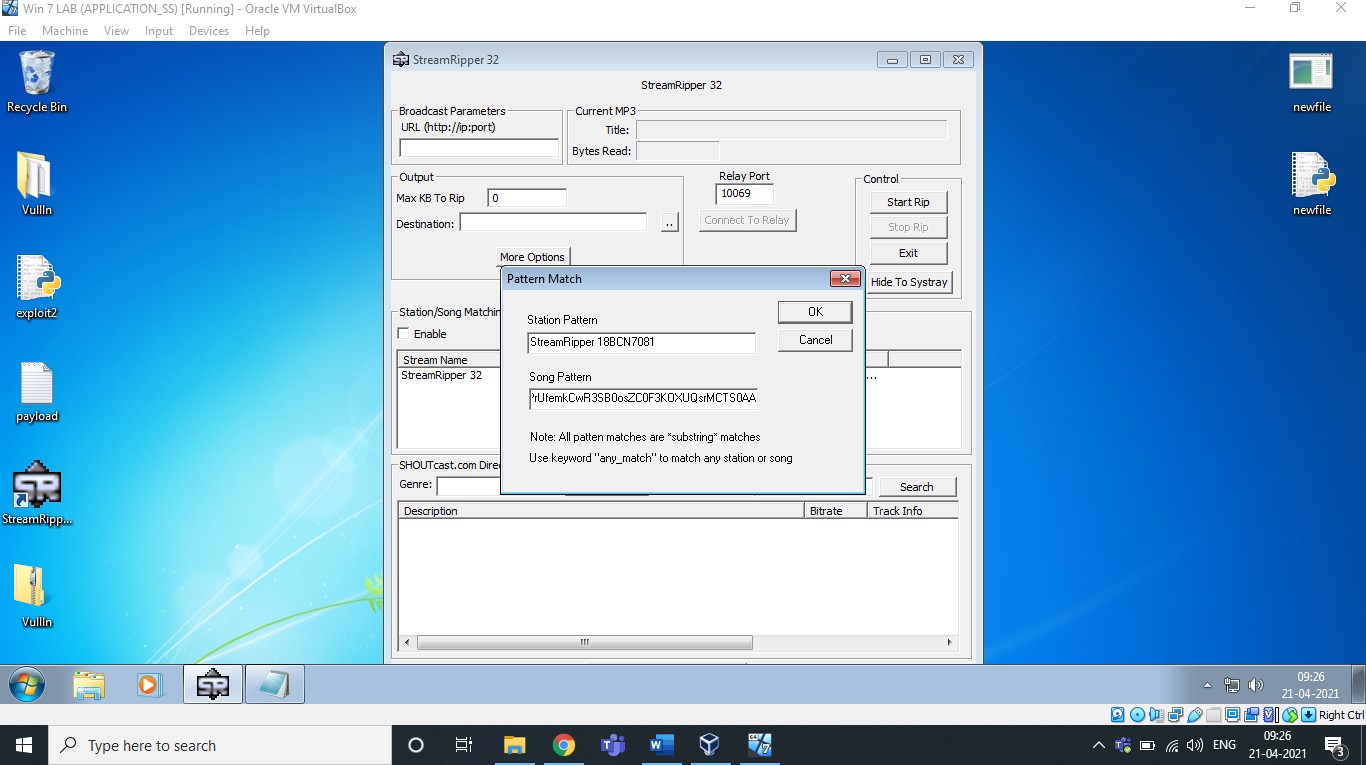
18BCN7101 L39+L40

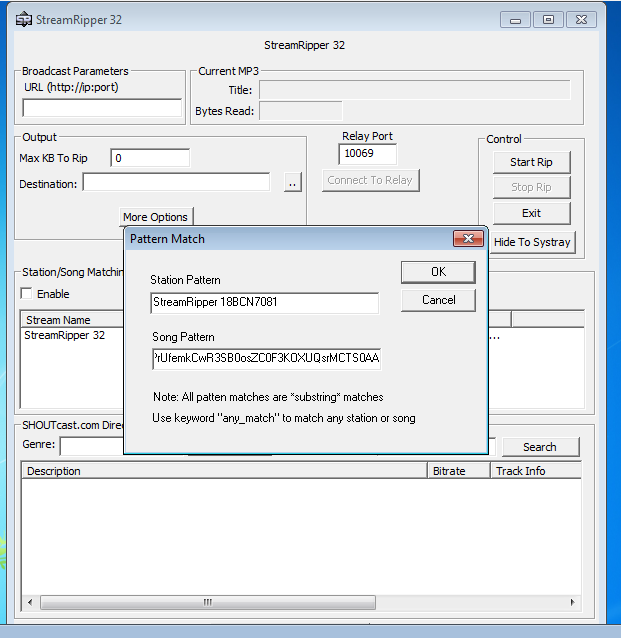
**Lab experiment - Working with the memory vulnerabilities – Part III**

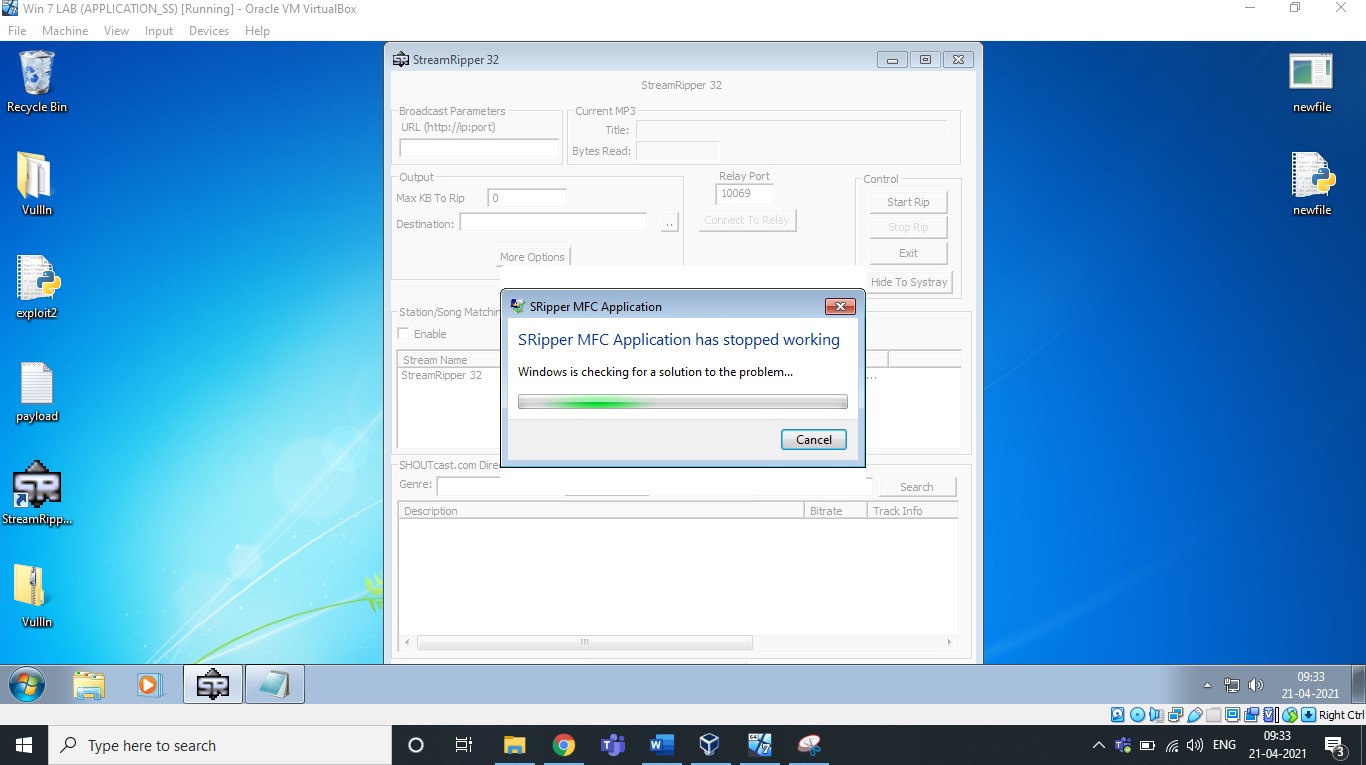
1) Crashing the StreamRipper32 with exploit2.py

After opening the application, Click on the ADD button under the Station/Song Matching Section.

Then, Give some Name in Station Pattern as per your wish and Copy the payload text and Paste it in Song Pattern. Now click on Ok, as you can see below.

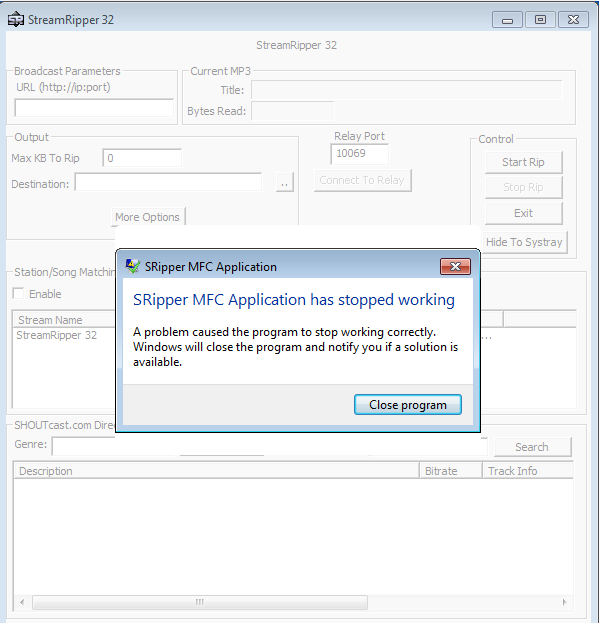






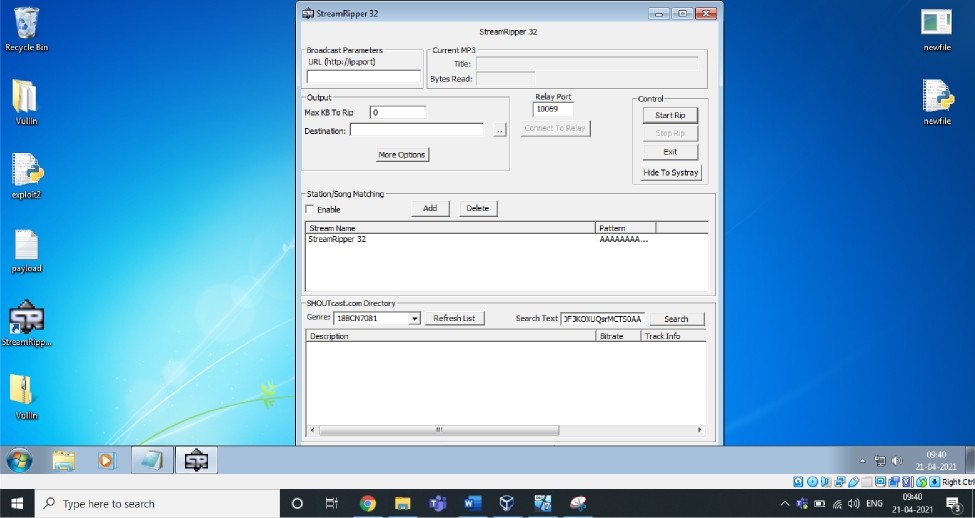
Exploit used above:

Payload text created using Exploit2.py given



As we can see, it’s crashed.

Also, Let us exploit the search box of this software, Stream Ripper 32,



StreamRipper 32

Broadcast Parameters Current MP3

URL (http ' |D '|DOFt) Tide:

Bytes Read:

Output

Max GB To Rip 0

Destination:

More Options



Qtr eamRipper 3 2

Relay Port Conbol



5 rtRi



Exit

Hide To Systray

5tation/Song Matching Enable

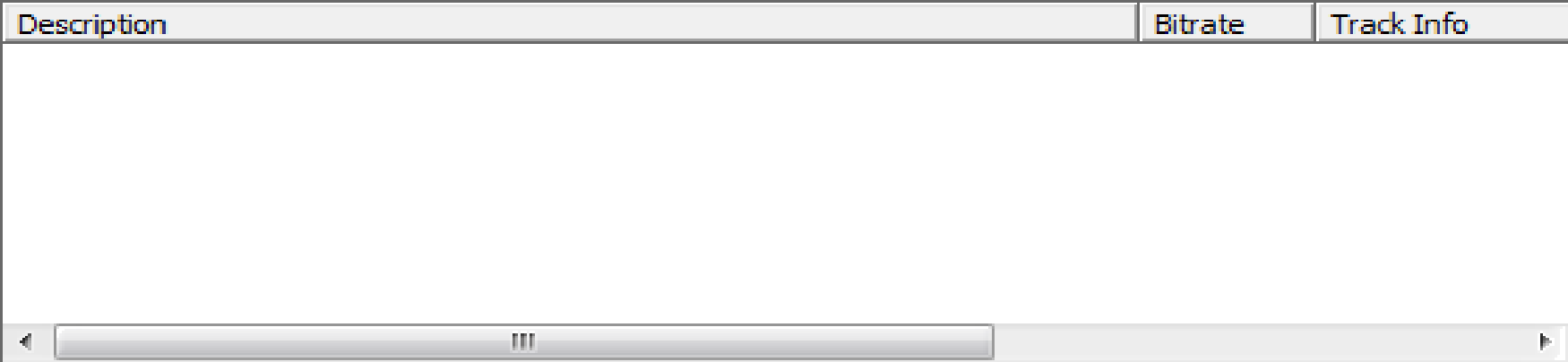
Add Delete

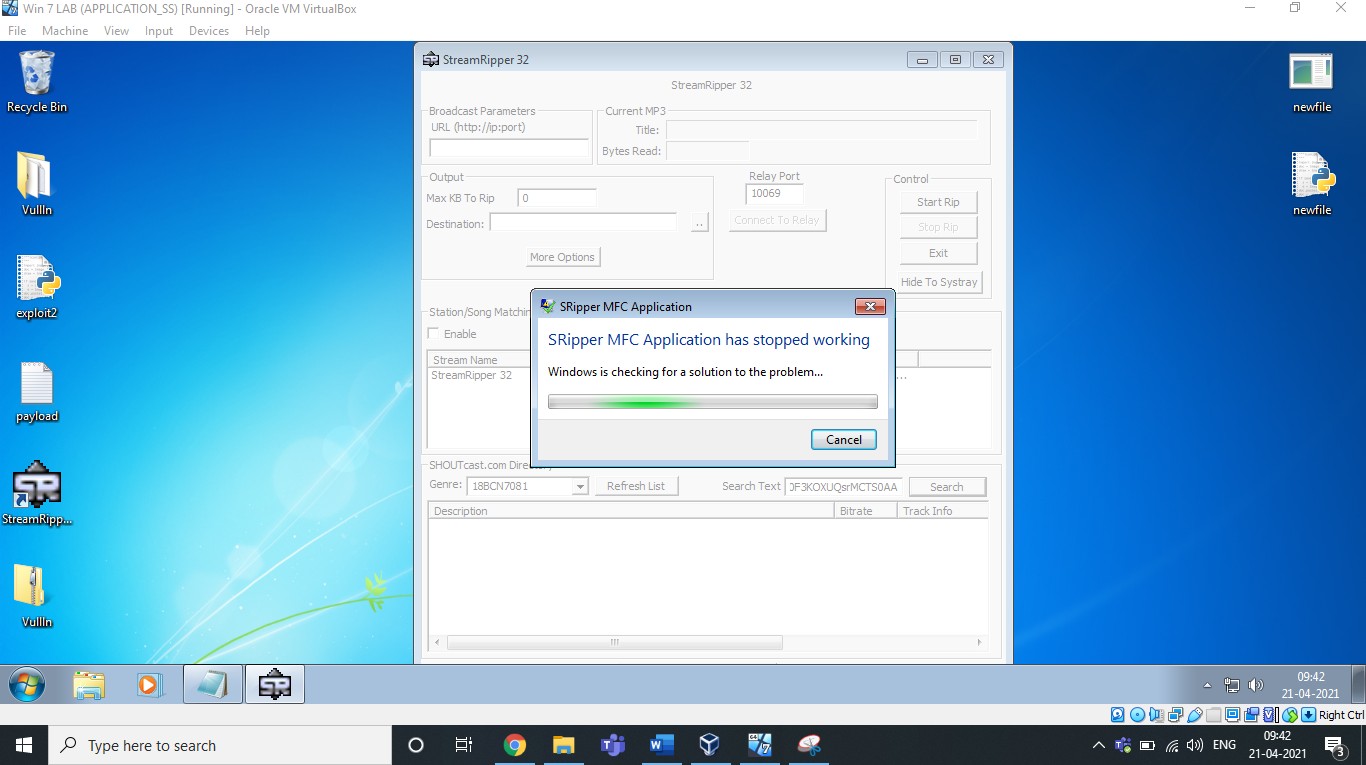


5HOUTcast. com Directory

Genre: BB B 1 Refresh List

Bearch Text F KO UQ rM 50 Search





Enter the same payload in the search as above… As you can see, it crashed..

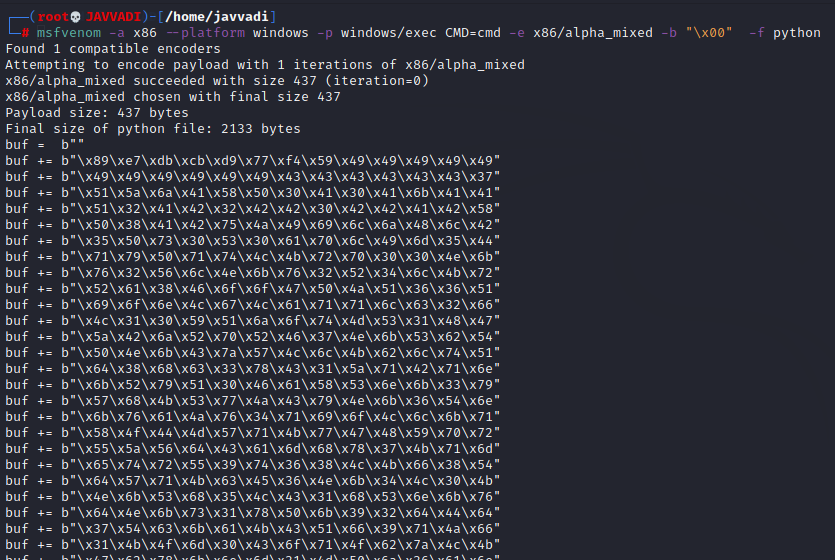
# Changing the Trigger:

Necessary Prerequisite steps to be done:

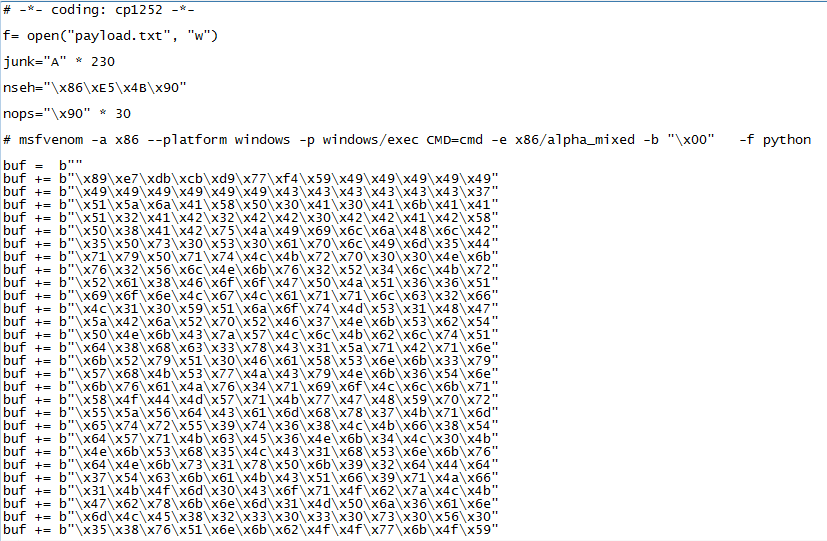
1. Crashing the Application
2. Find EIP
3. Control ESP
4. Identify Bad Characters
5. Find JMP ESP

We have already carried out these steps in last experiment i.e. Part II So let's continue trigger cmd to erase our HDD.

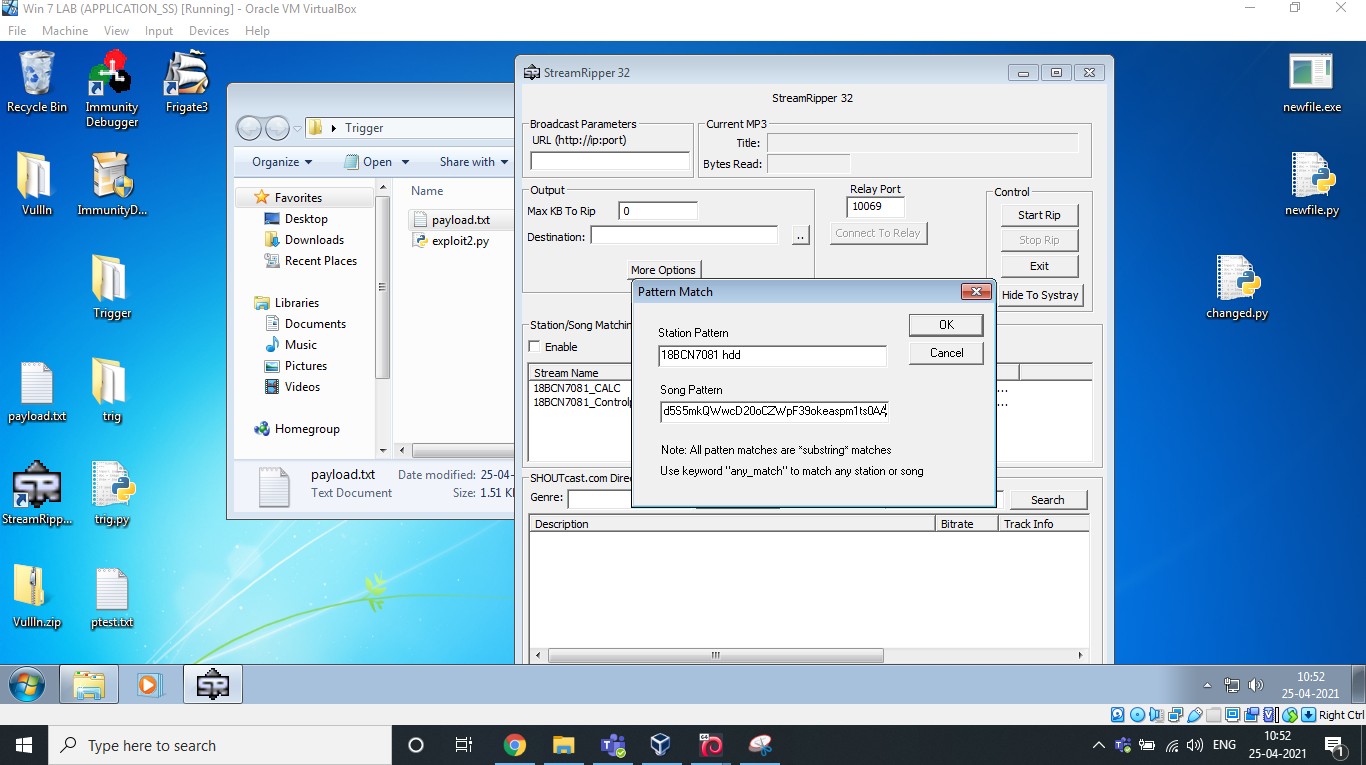
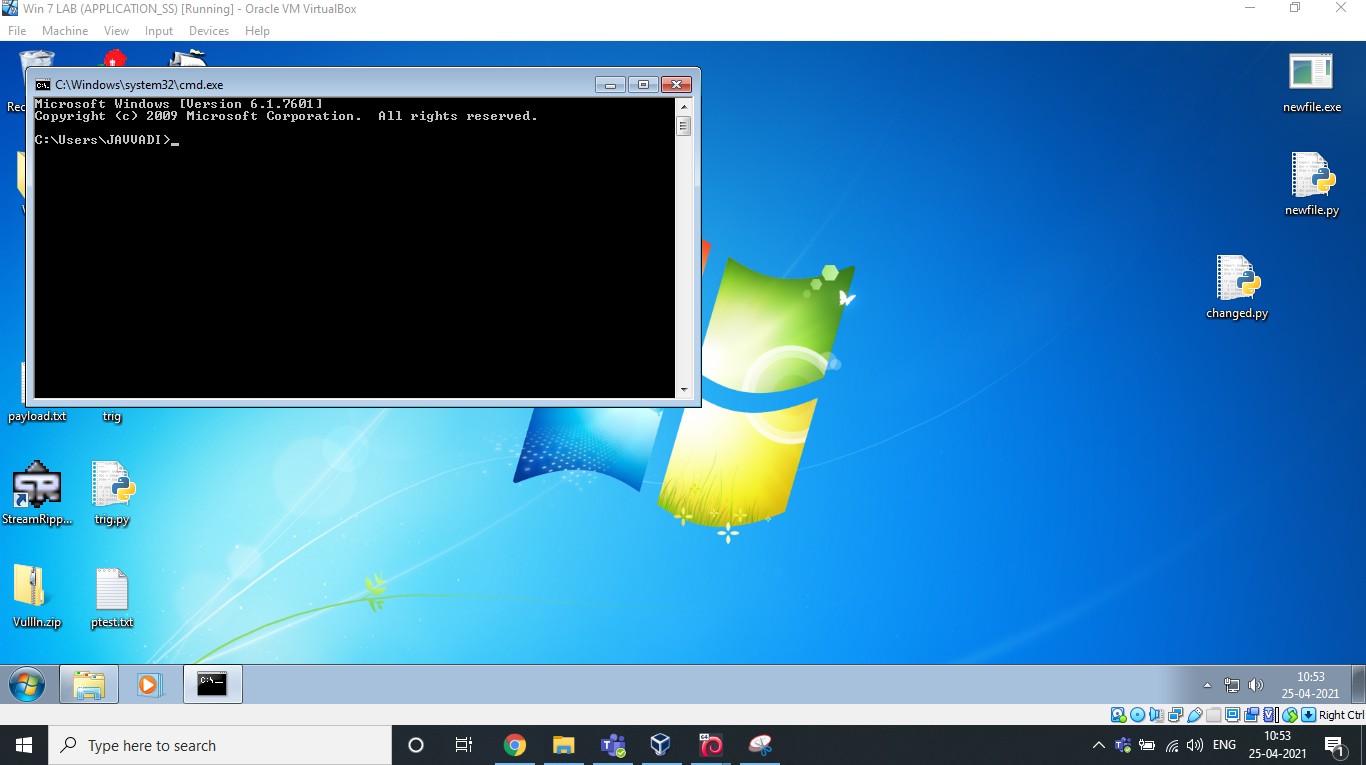
# Generating ShellCode

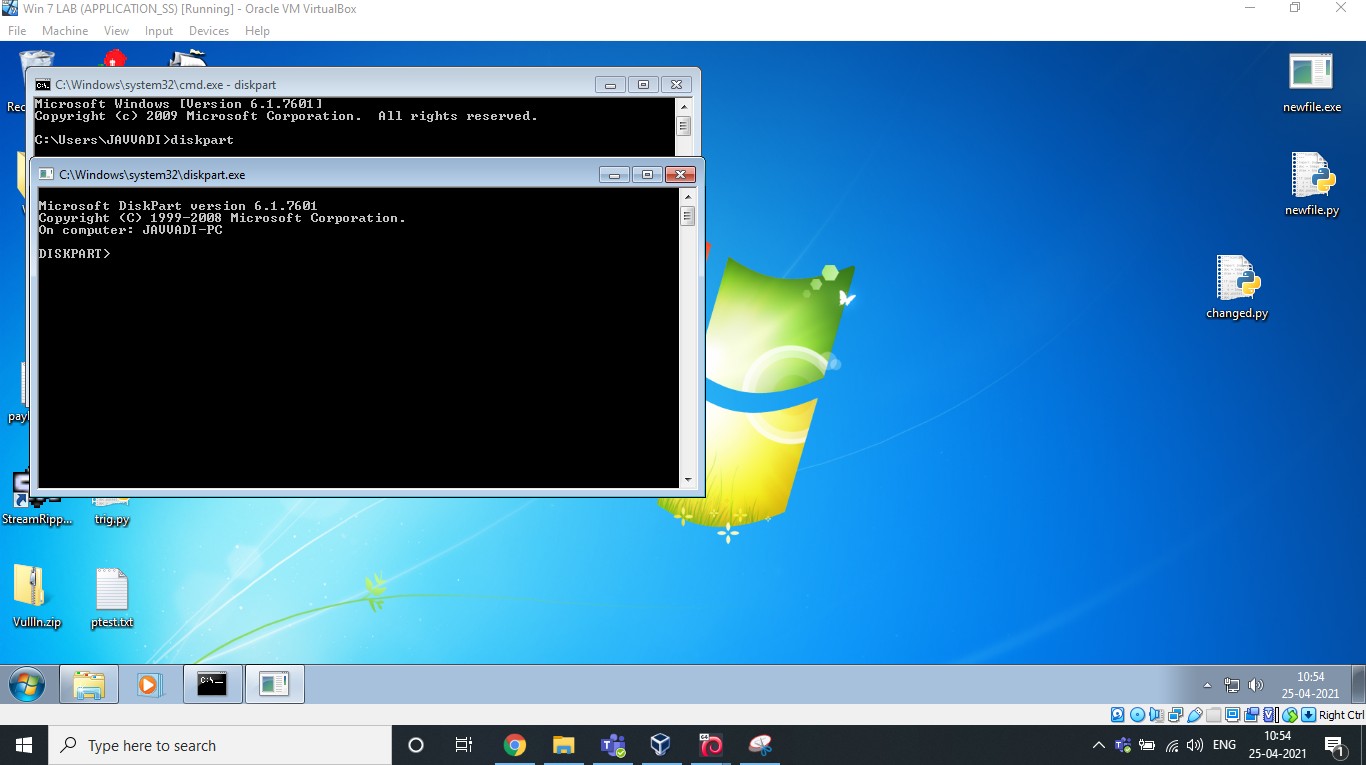


**Exploit**



Paste the payload generated using above script in any user interaction field, Like shown below.





By using DiskPart, you can erase your 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.

Stack overﬂow is when a function or program uses more memory than is in the stack. As it grows beyond its allocated space, the dynamic stack contents begin to overwrite other things, such as critical application code and data. Because of this, we are able to pop up cmd