Secure Coding (CSE 2010)
LAB Experiment: 9

Done by,

Aadil Mohammed

Reg.No:19BCI7052

SLOT: L23+L24

Lab experiment - Working with the memory vulnerabilities – Part III

Task

- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py) to generate the payload
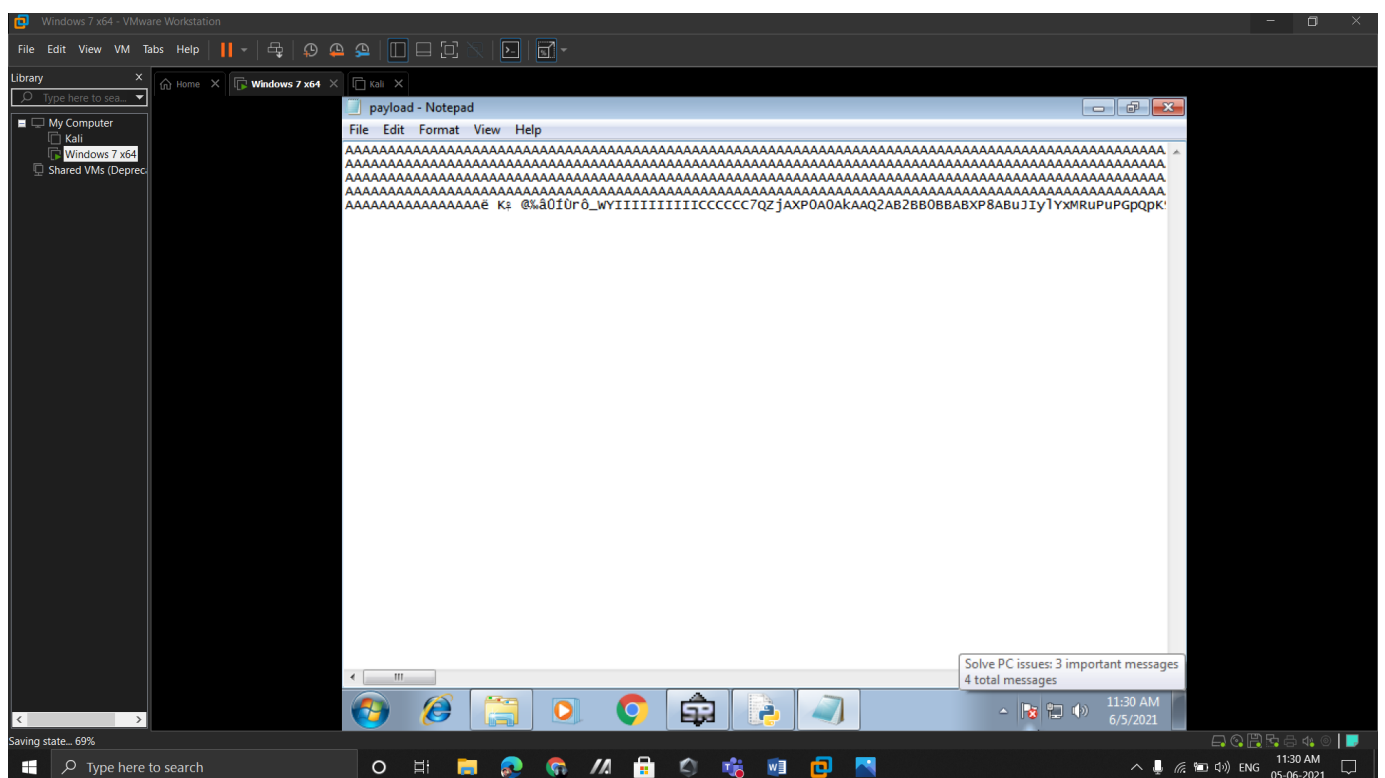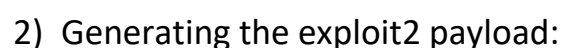- Install Vuln_Program_Stream.exe and Run the same

Analysis

- Crash the Vuln_Program_Stream program and try to erase the hdd.

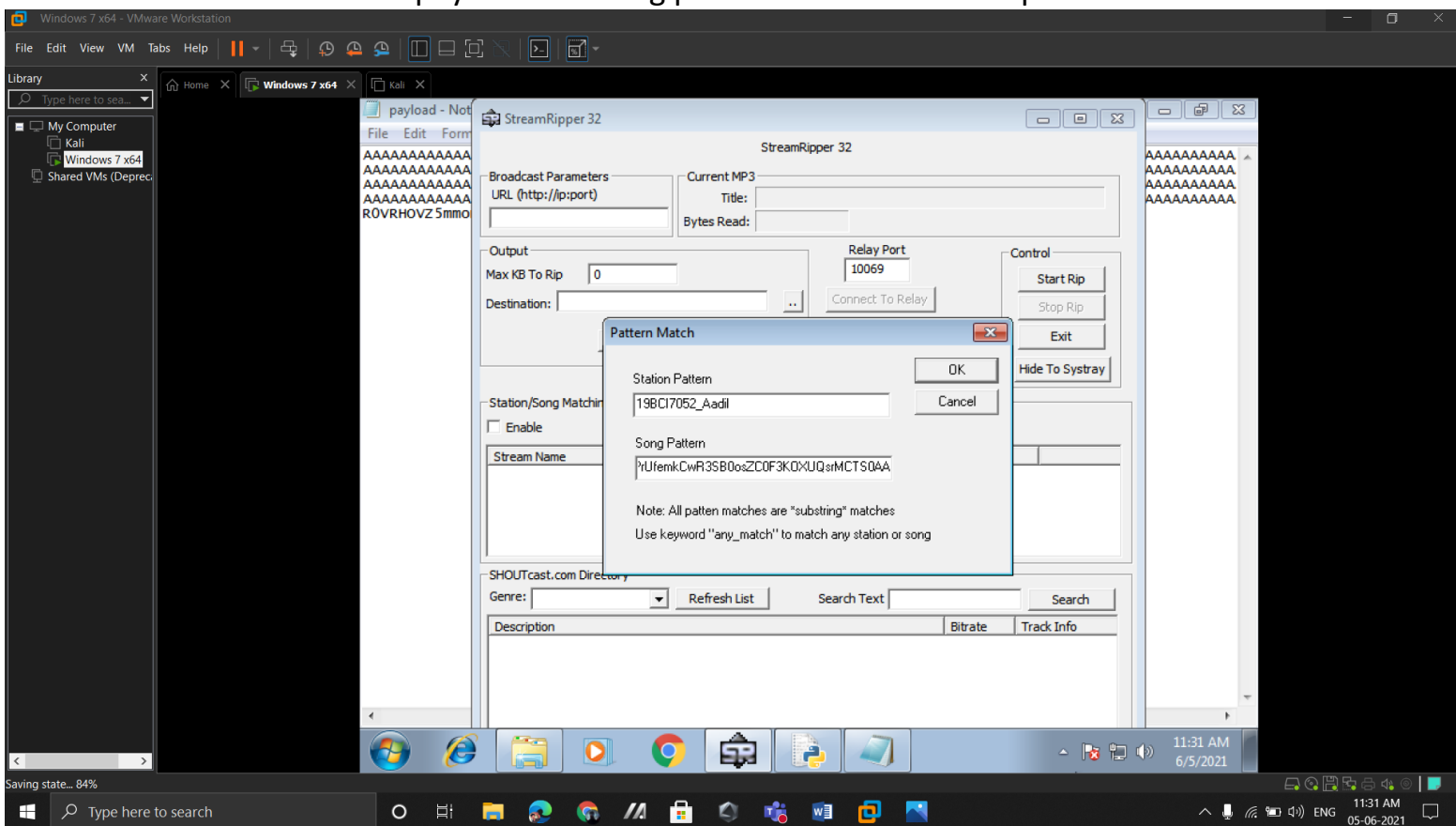Happy Learning!!!!!!

Trying to crash Vuln_Program_Stream program:
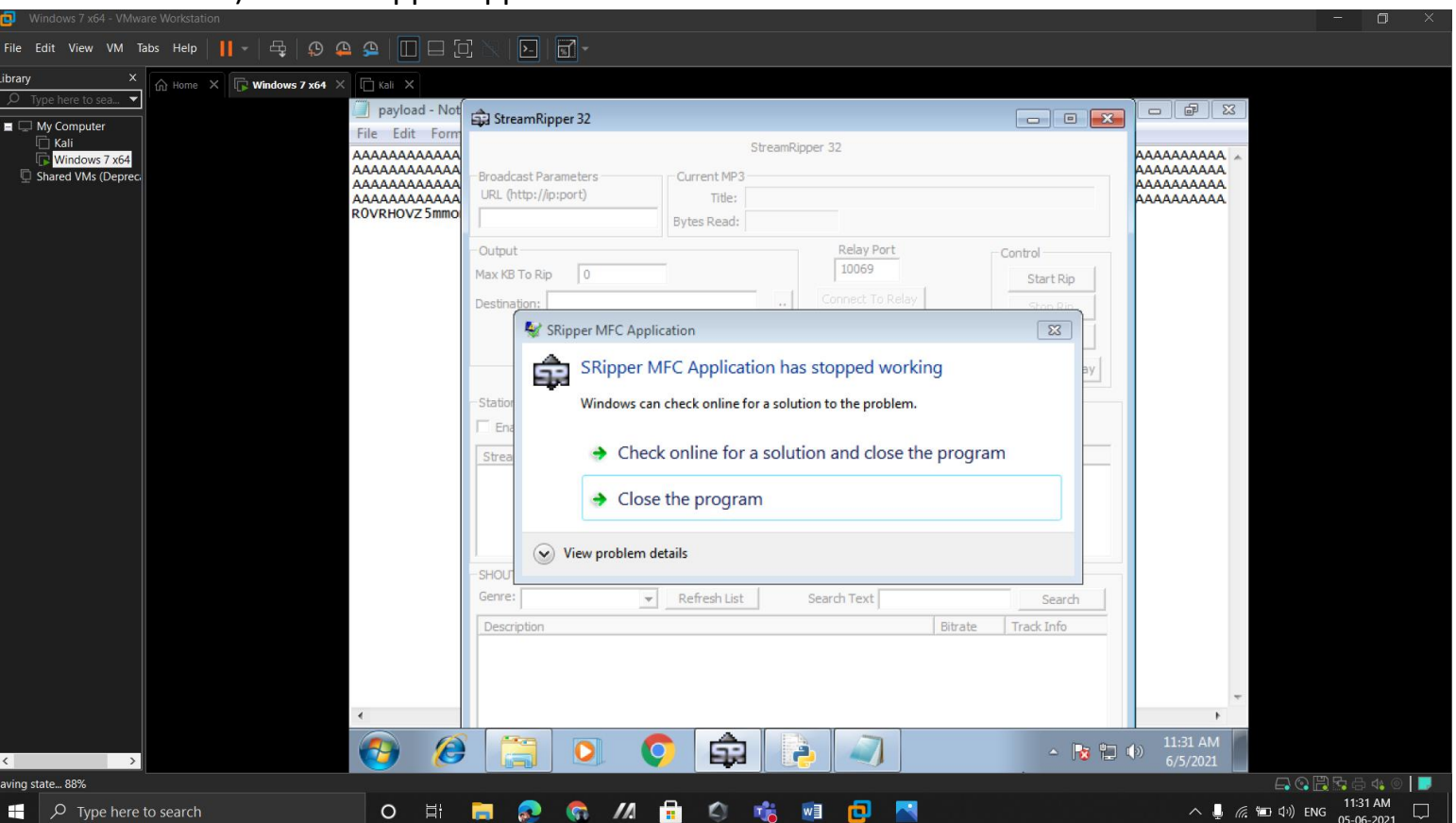
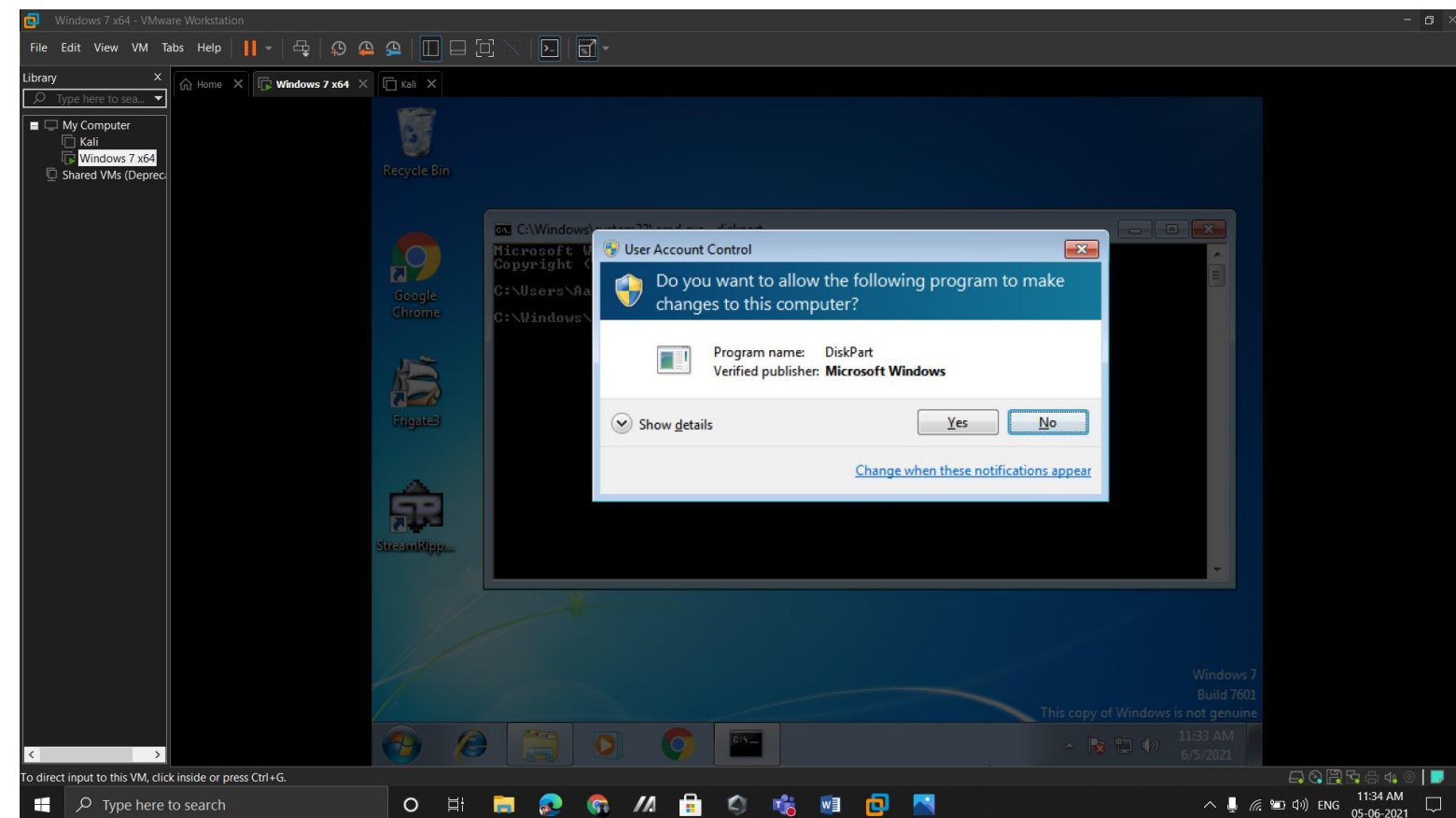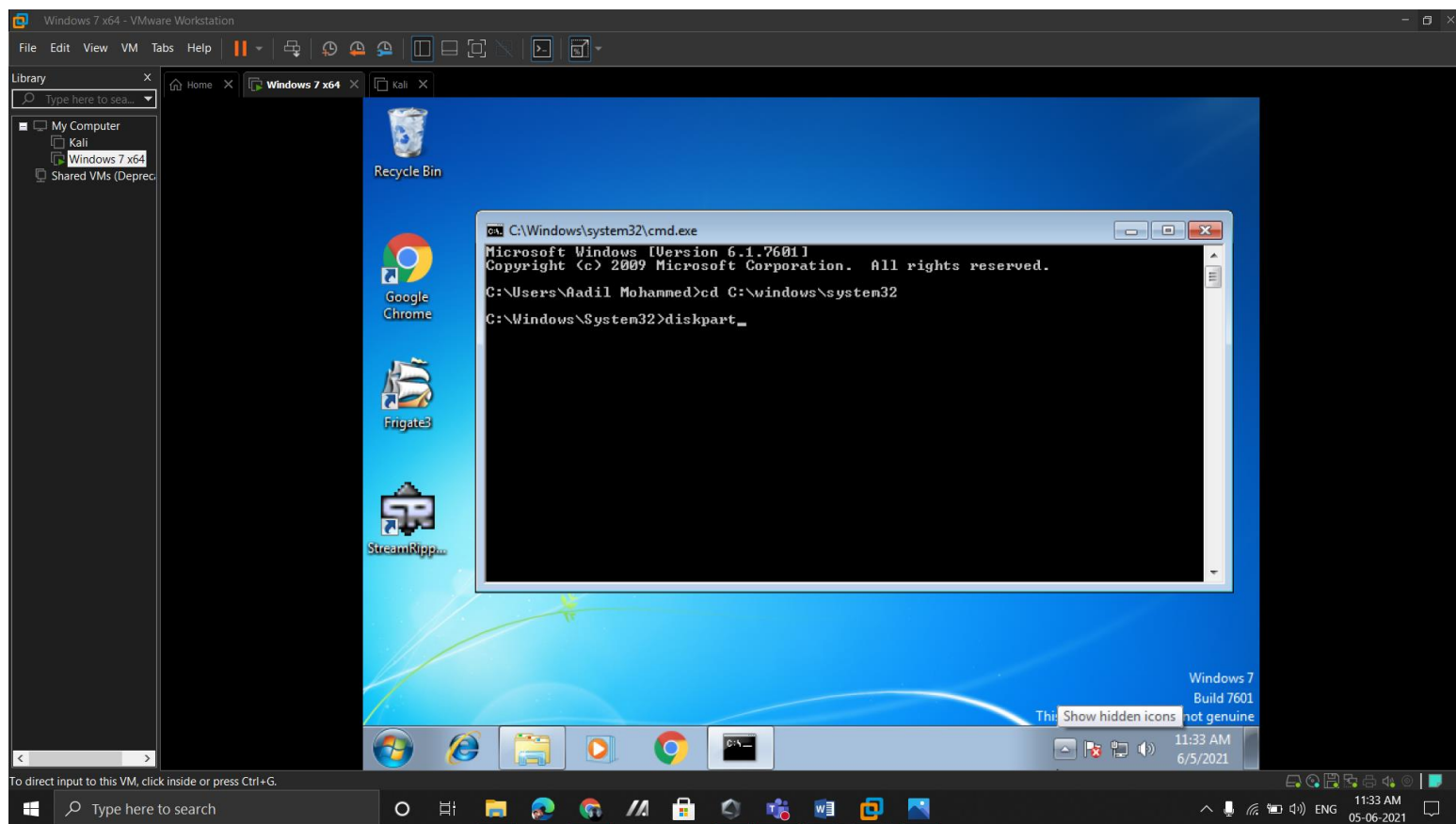1) Explot2 program script:

2) Generating the exploit2 payload:

3) In the StreamRipper32 Applications using the above generated payload to add the payload as a song pattern and select add option:

4) StreamRipper application crashes:

Trying to erase the HDD:

- Couldn't delete the HDD as, in the VM I haven't yet partitioned the Hard disk. AS all the System, windows, current boot loader along with the user files are in the same directory C, that's why I wasn't able to clear the HDD.