SECURE CODING LAB-8

CSE-2010

SLOT-L23&L24

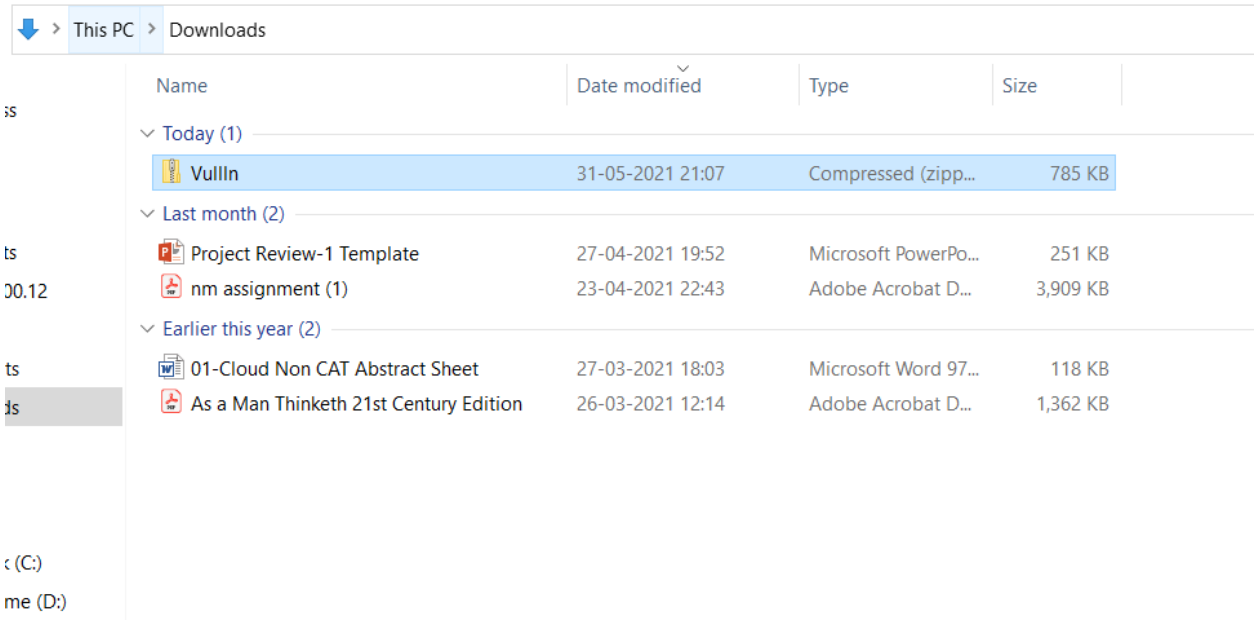
DONE BY

HEMANTH KUMAR R

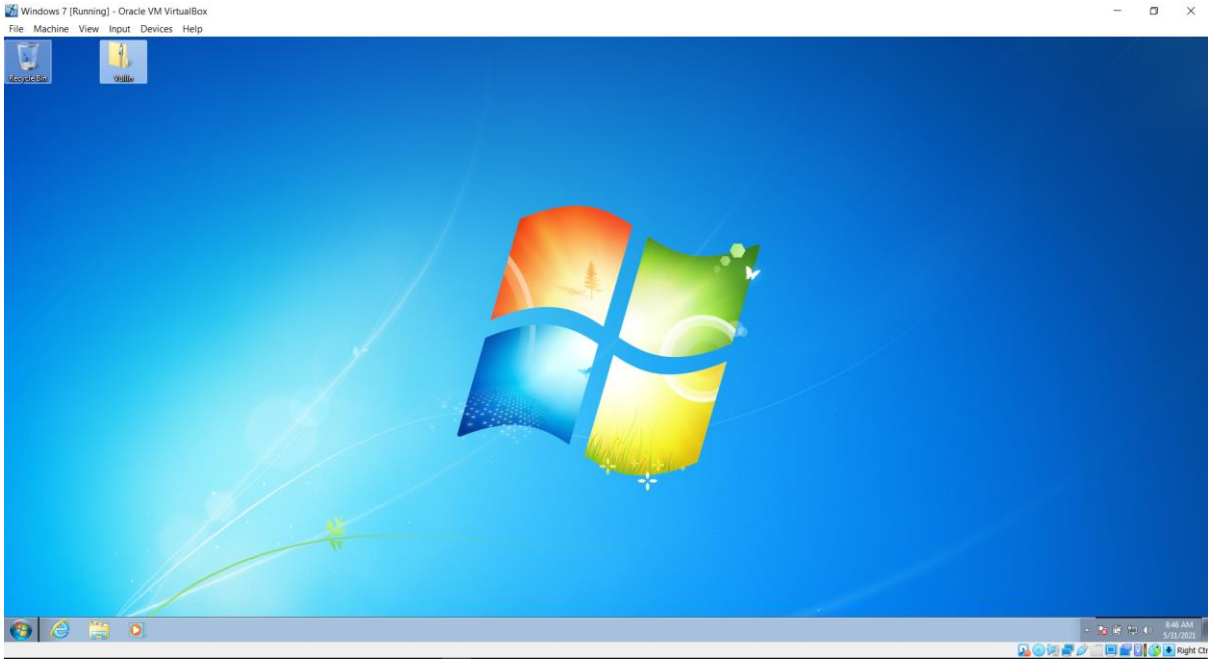
18BCN7028

Working with the memory vulnerabilities

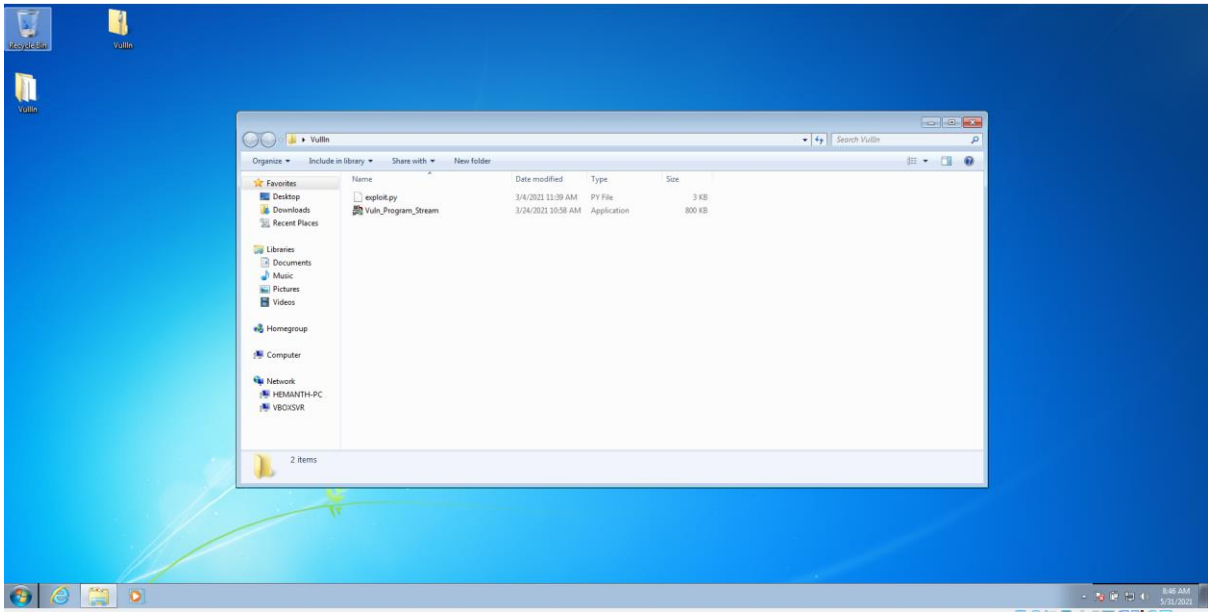
Download Vulln.zip from teams.



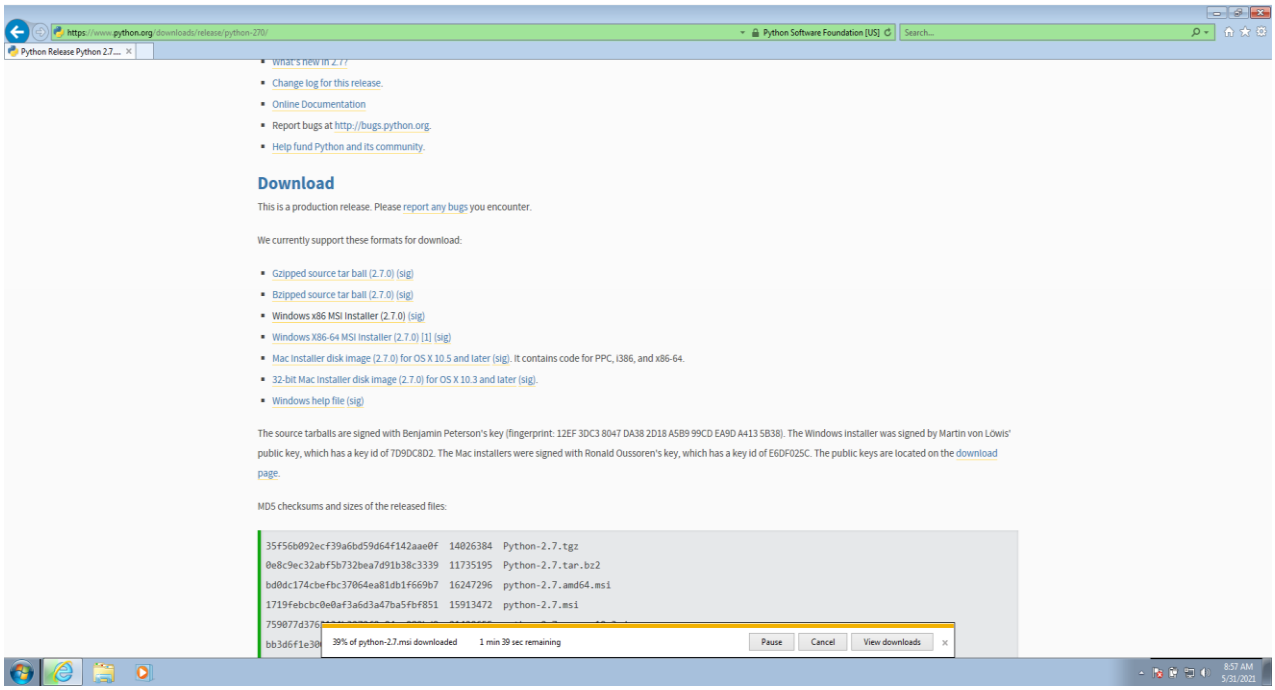
Deploy a virtual windows 7 instance and copy the Vulln.zip into it.



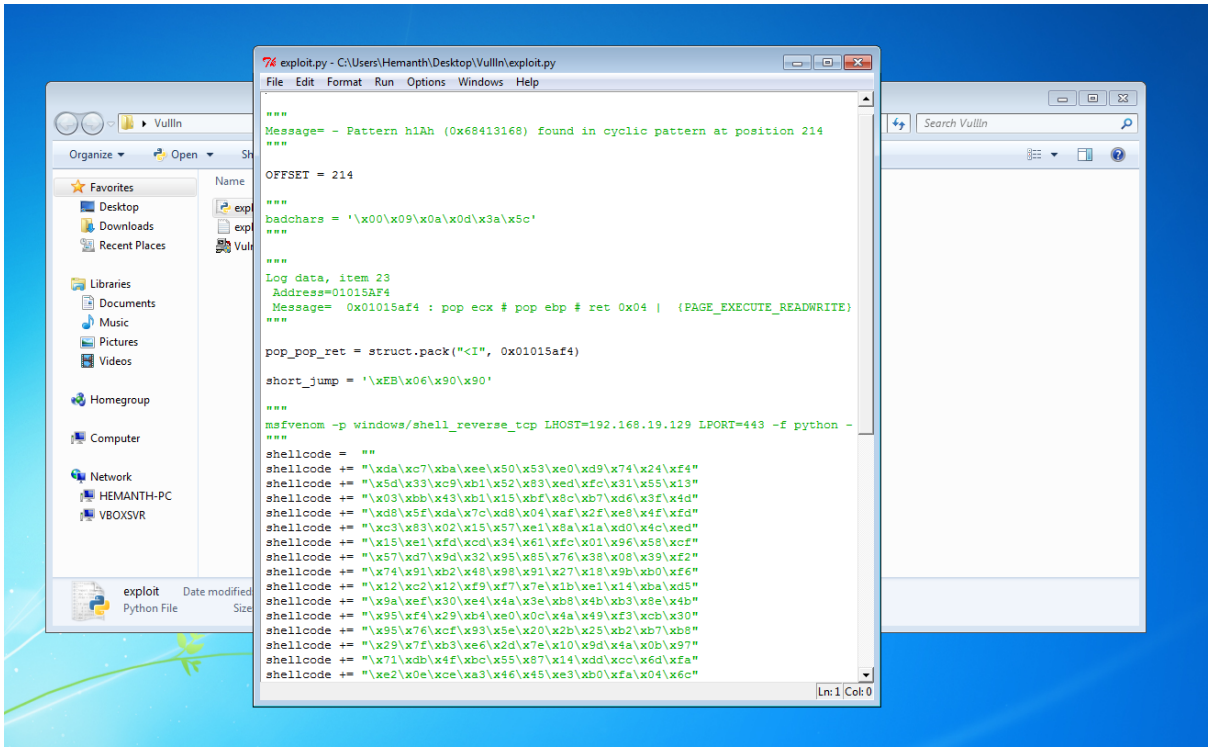
Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe



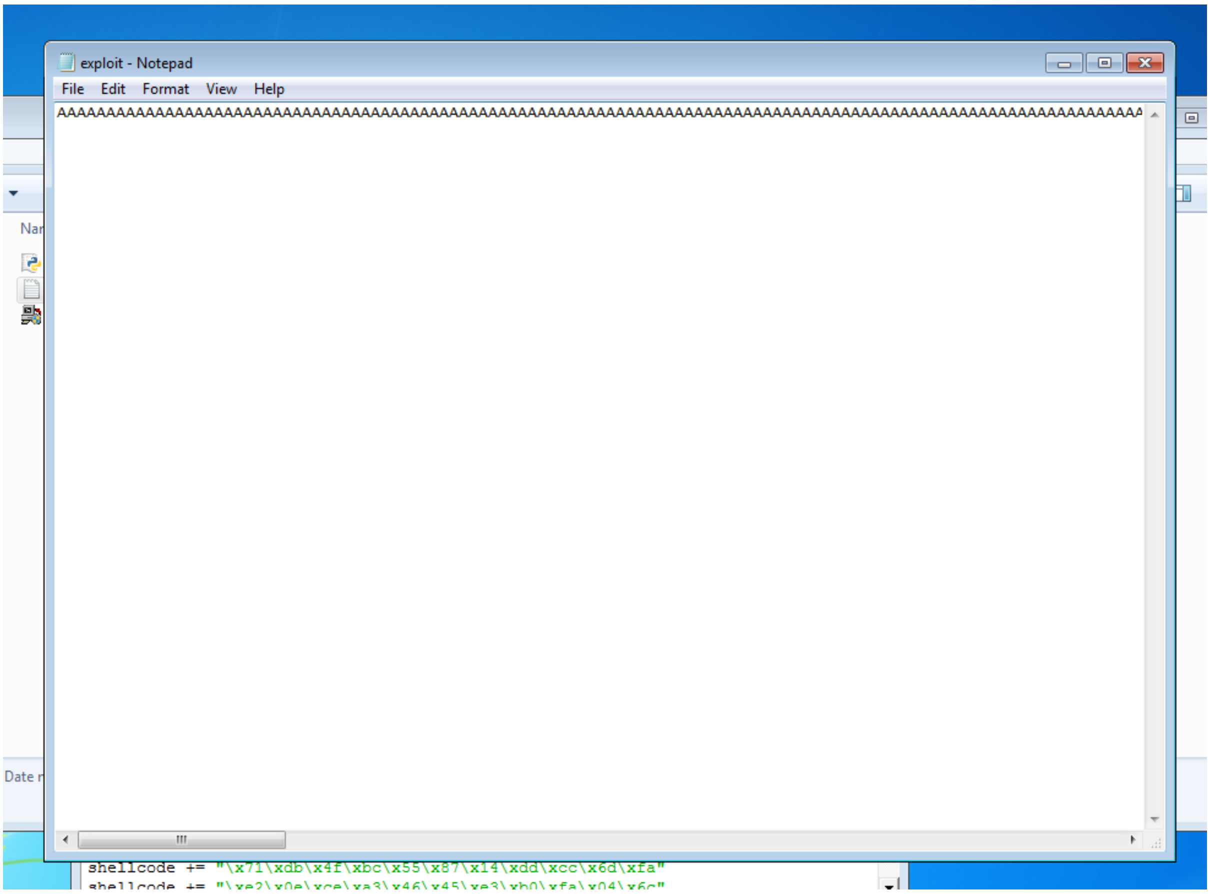
Download and install python 2.7.* or 3.5.*



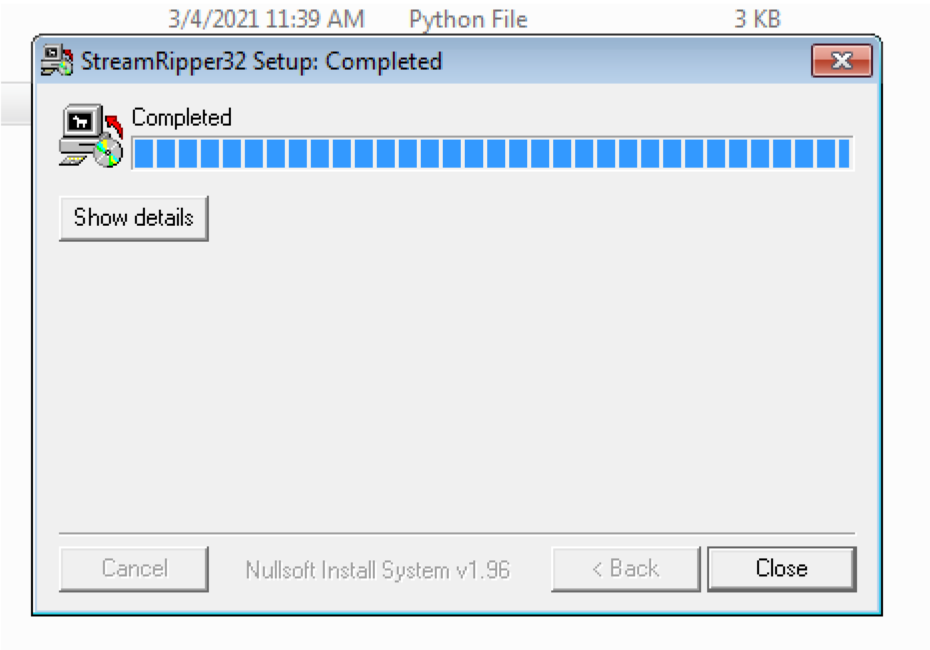
Run the exploit script to generate the payload

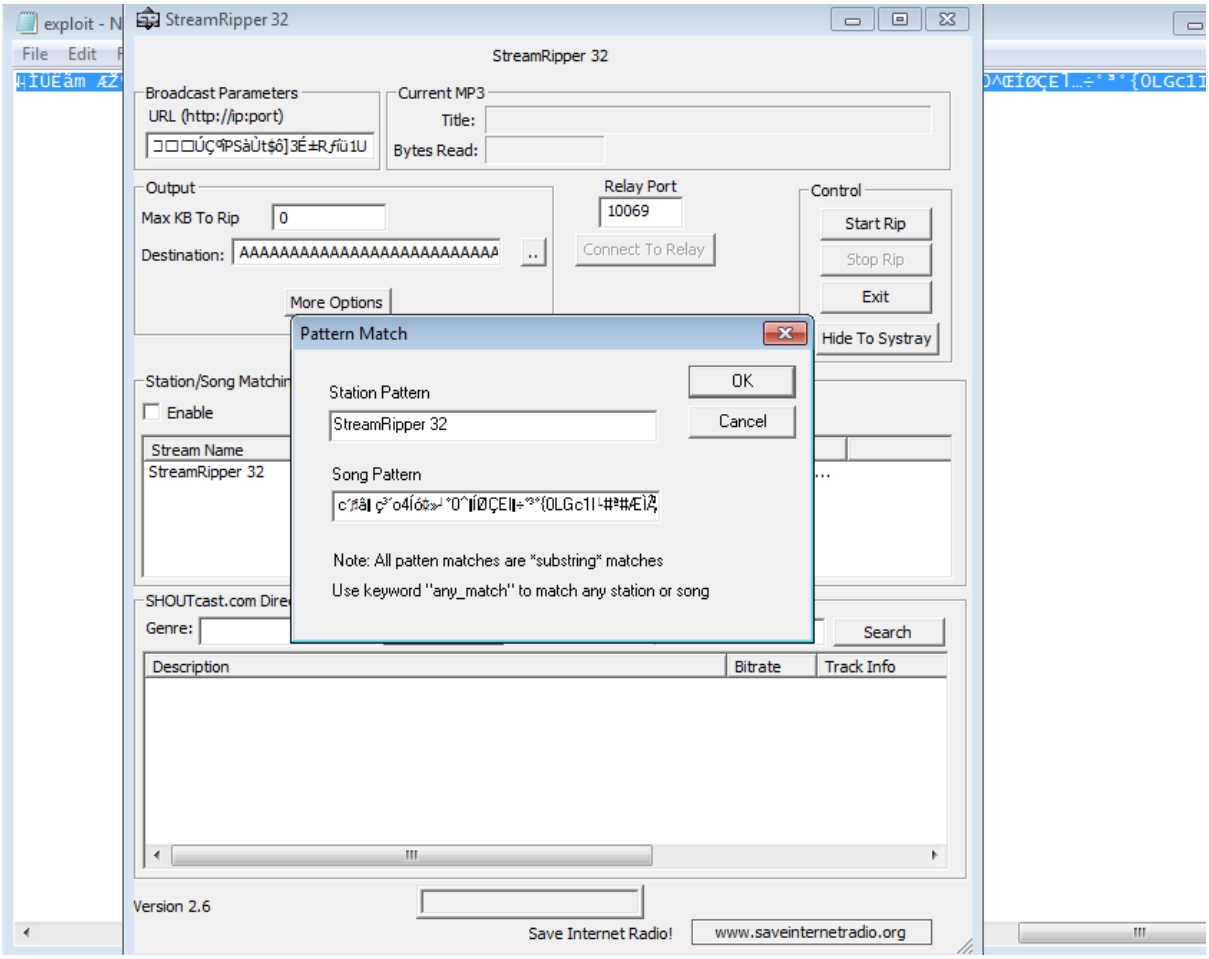


Generated the payload by running exploit.py



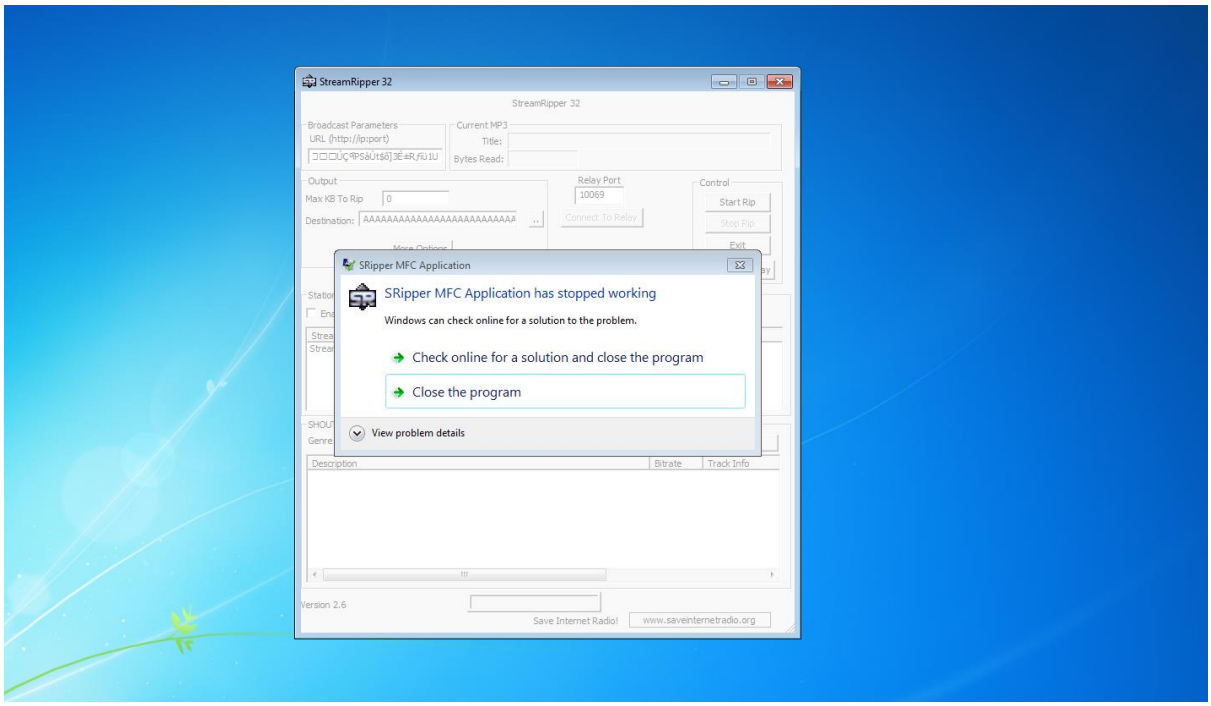
Install Vuln_Program_Stream.exe and Run the same





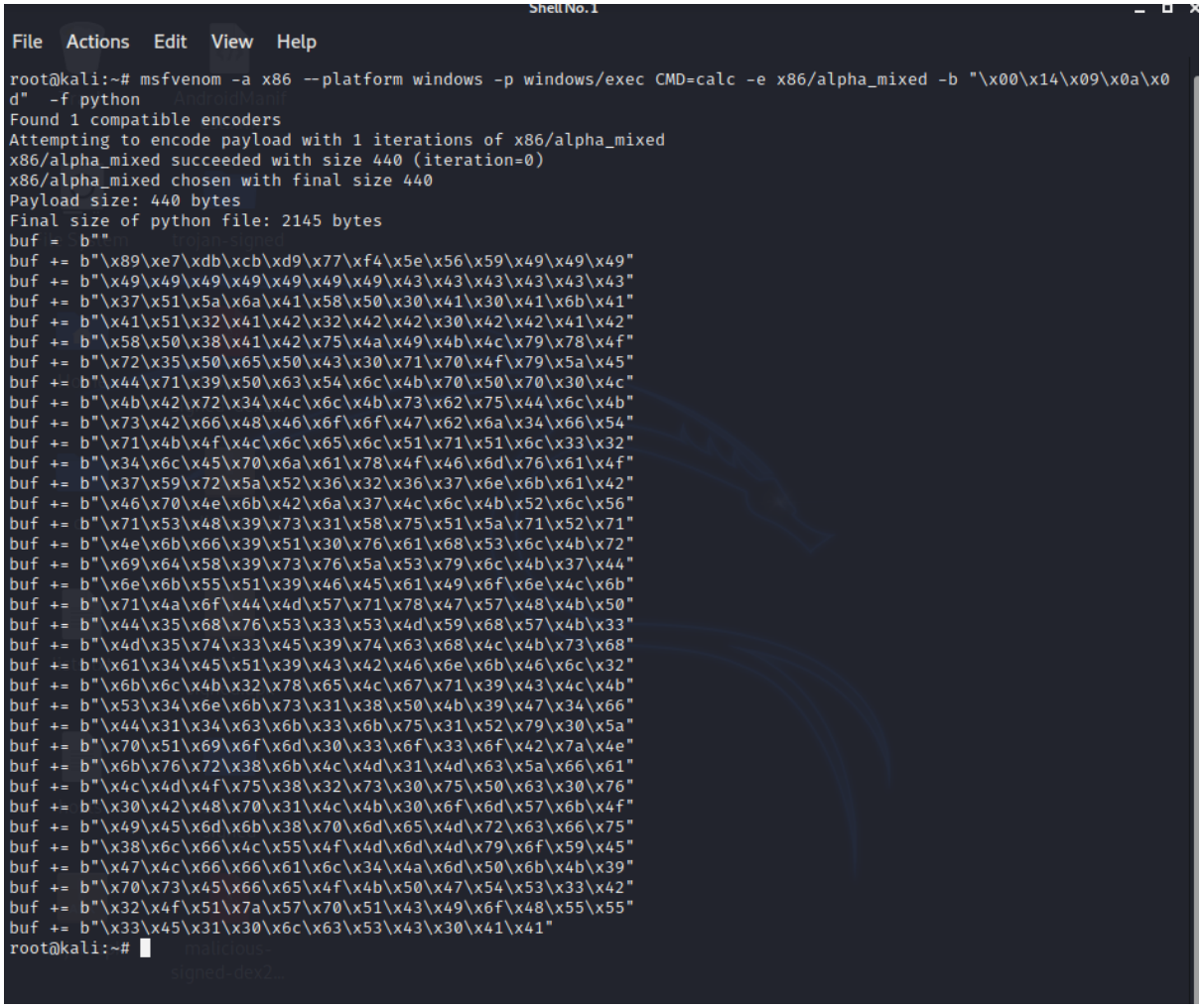
Vulnerability found

Try to crash the Vuln_Program_Stream program and exploit it

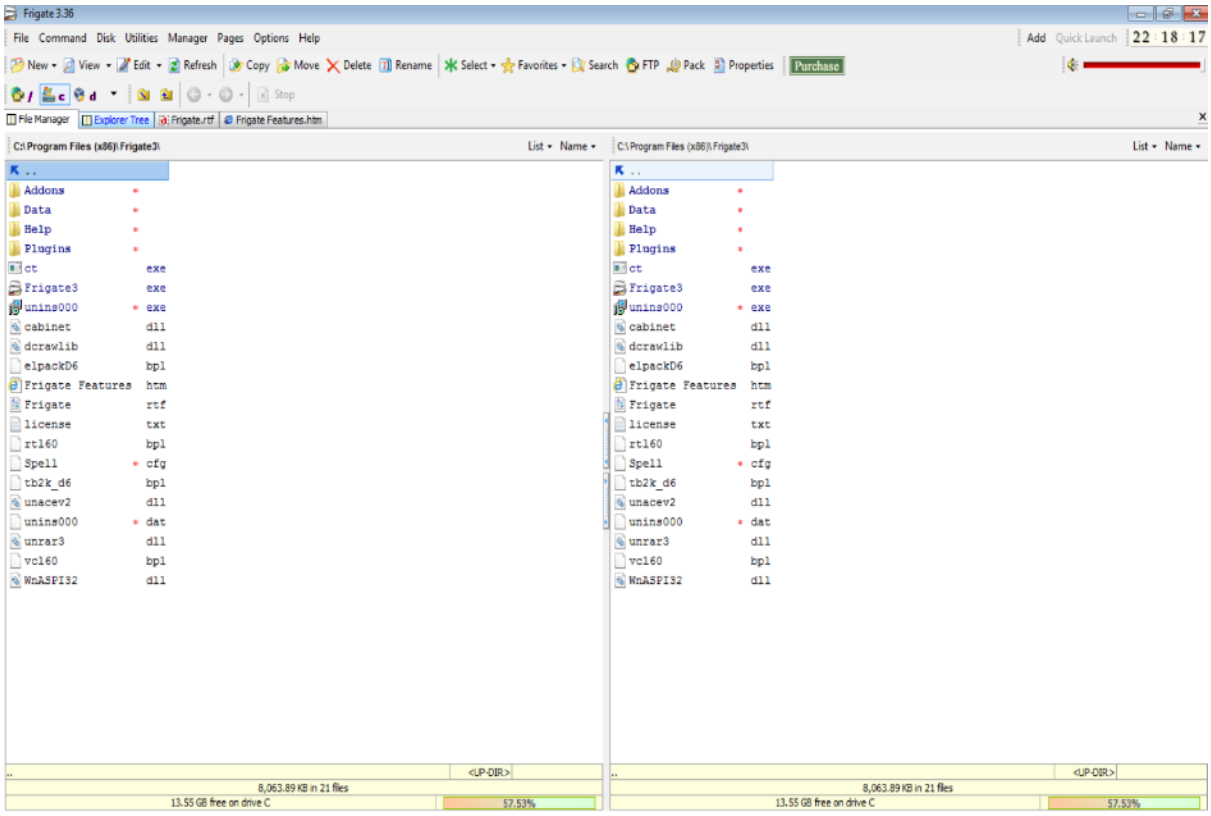


Change the default trigger from cmd.exe to calc.exe

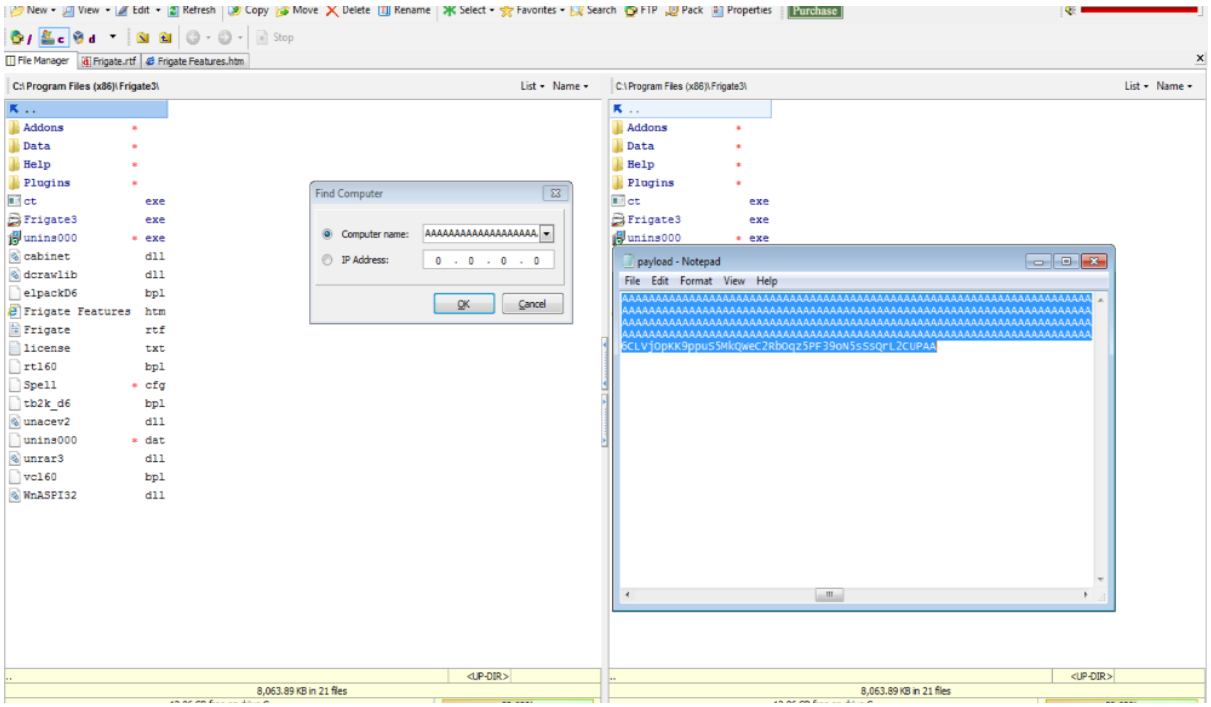
msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python



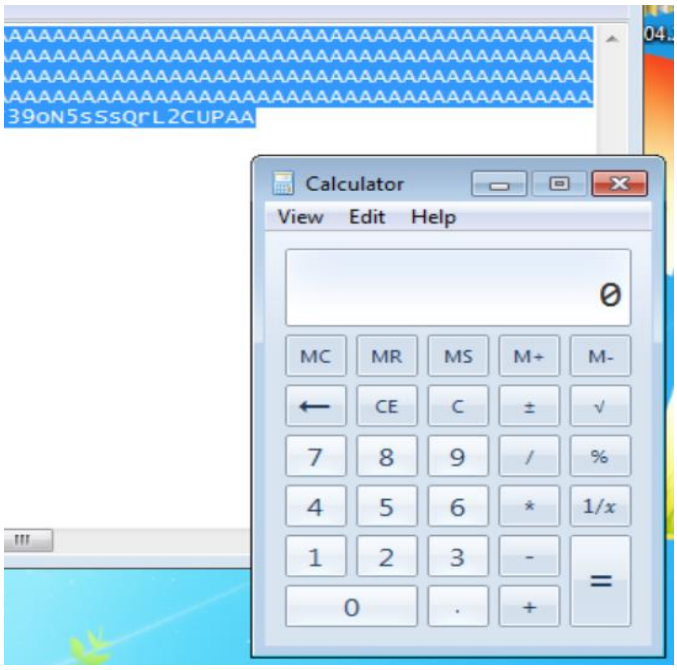
Install frigate.exe and run the same



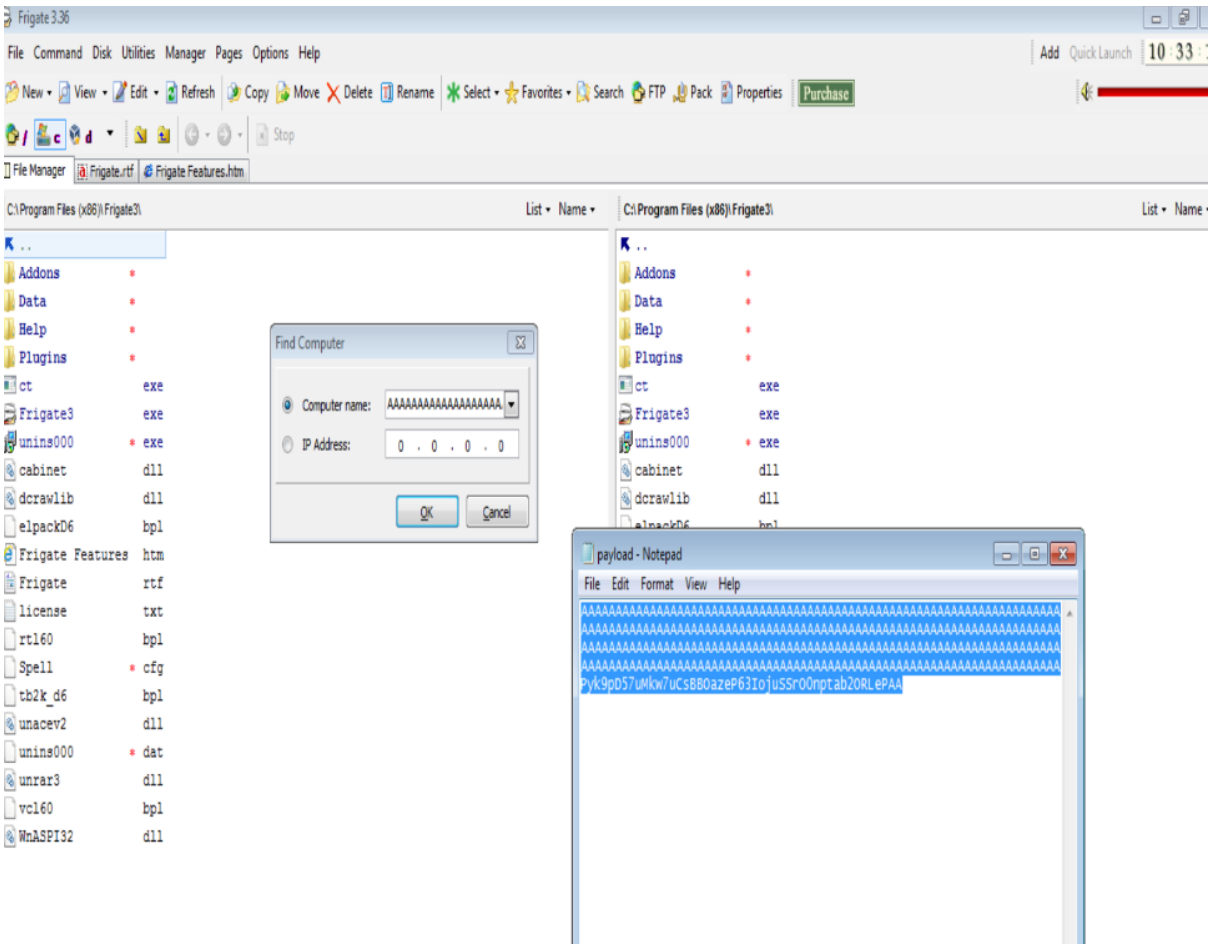
Vulnerability found by generating the calculator payload



Application crashes and opens the calculator



Vulnerability found by generating the calculator payload



The app crashes and opens control panel.