LAB 7

K.SIVA KARTHIK
19BCE7416

Lab experiment - Working with the memory vulnerabilities

Task

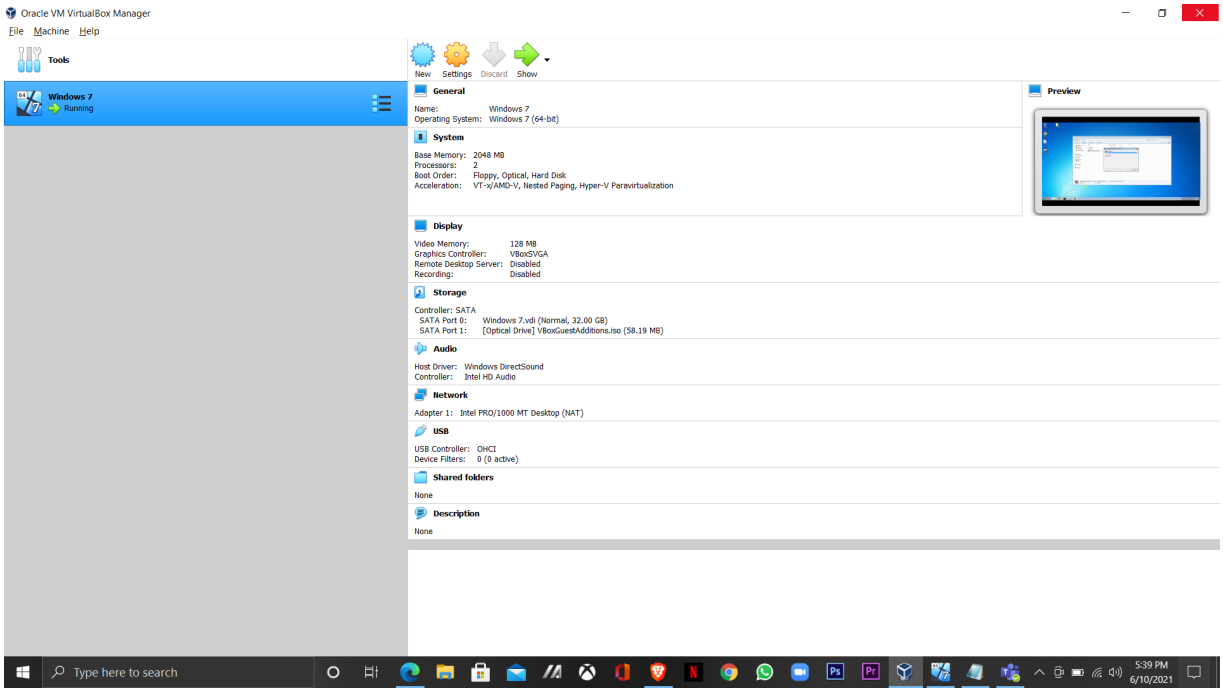
- **Download Vulln.zip from teams.**
- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**
- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**
- **Download and install python 2.7.* or 3.5.***
- **Run the exploit script to generate the payload**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

Analysis

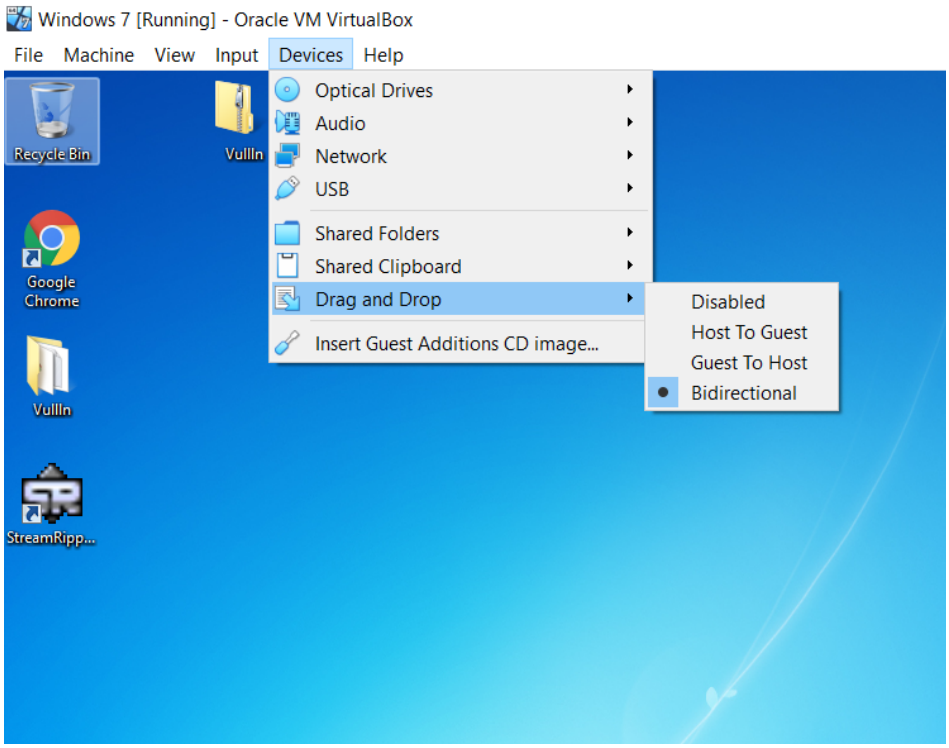
- **Crash the Vuln_Program_Stream program and report the vulnerability.**

ANS:-

1) **Windows 7 virtual machine deployment is done by using Oracle's Virtual box and windows_7_ultimate_n_x64 was downloaded from raddle.me**



2) Then the Vullln.zip was shared to the virtual machine by using Devices option on the top bar and changing changing drag and drop to bidirectional. The the zip file file is dragged and dropped to the windows 7 virtual machine.

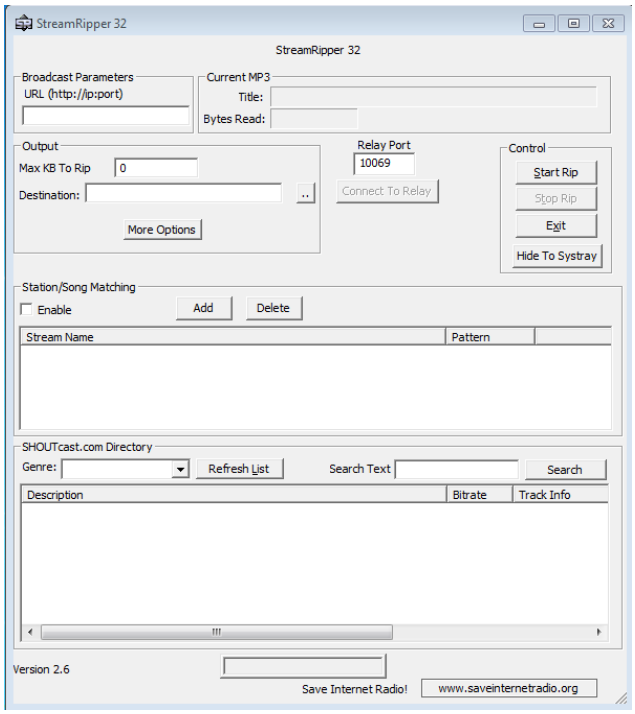


3) **Then extracted the Vullln.zip file and compiled exploit.py script in python 2.7 then the exploit payload text file is created in the same directory.**

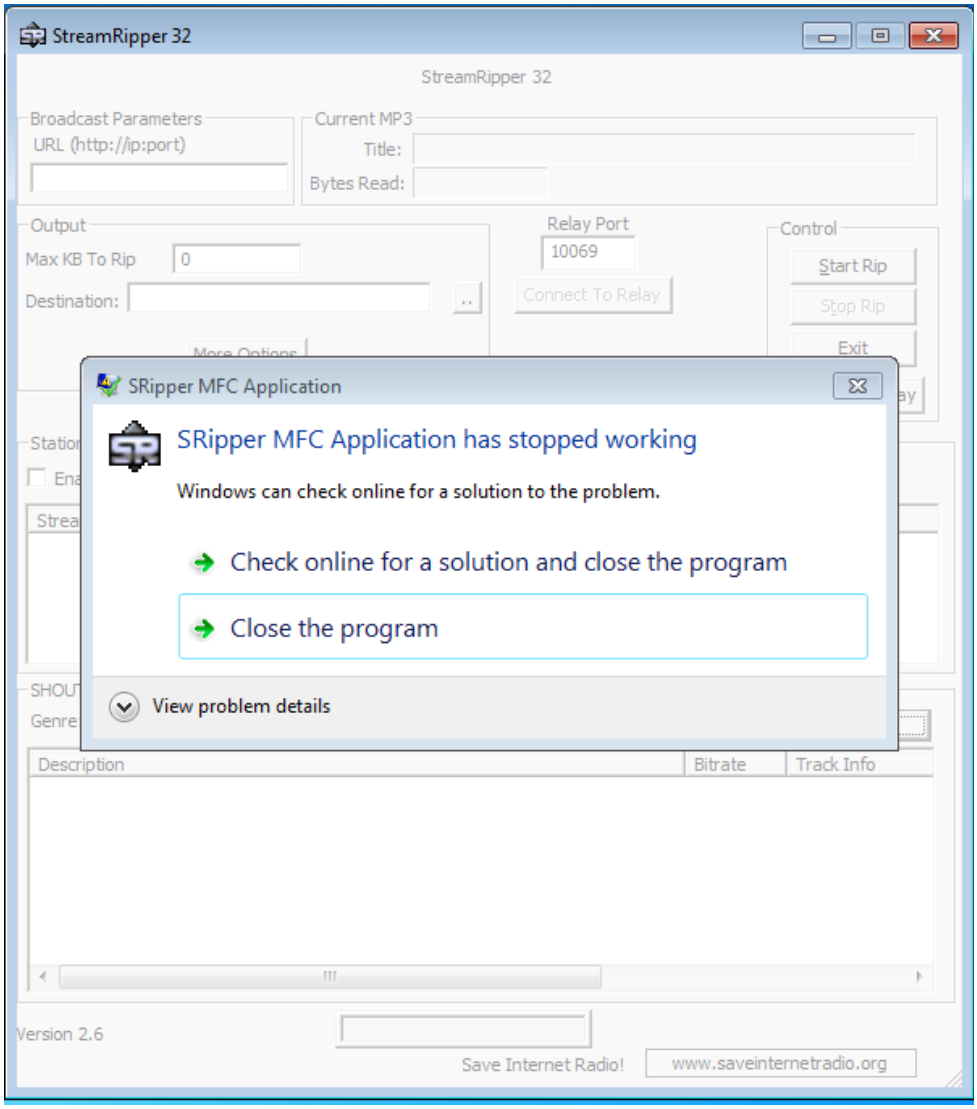
PAYLOAD:

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAë ôZ ÚÇºîPSàÙt$ô]3É±Rƒíü1U »C± ¿Œ·Ö?MØ_Ú|Ø ¯/èOýÃƒ WáŠ ÐLí áýÍ4aü –XÏW× 2•…v8 9òt‘²H˜" ›°ö Â ù÷~ á ºÕšï0äJ>¸K³ŽK•ô)´àJIóË0•vÏ“^ +%²·¸) ³æ-~ J —qÛO¼U‡ ÝÌmúâ Î£FEã°ú lt7¶l @Å^½úAÓ6%– m‘ ëŽâ (Ú²9™cY¹&¶Îéˆî¯YiÚG³f w¼¬. G''KT6yŽZ9Á ¼S%N ÌÜËãm ÆŽ®ªåo`[ƒc «ÞÙ°´ôu^&“…)[Ò~E¶”ÿ¤n@Çlµ±Æm8 ì}„ ©)XYg‡ 3ÉqÉèƒ ŒÂ c‘ â‹ ç³´ o4Íó » °0^ŒÍØÇEl…÷°³°{0LGc1l #ª# ÆÌ Ã

4) **Then install the Vuln_Program_Stream from the extracted folder then open the StreamRipper 32 application in the virtual machine.**



5) **Then paste the exploit payload in the search section of StreamRipper 32. Click on the search then we see the application crashes and error promt appears on the screen.**



ANALYSIS :

StreamRipper 32 crashes because it is with for 32-bit architecture and supports/handles 32-bit files. The payload we entered in the search field is of 64-bit. When the search button is clicked the application crashes the field we exceeds 32-bits of alloted memory during the compile time.So the application crashes and prompts error message.