

CSE 2010 || Secure Coding

WIN 20-21

Lab: 7

Name: R B Ch S Tarun

RegNo: 19BCN7122

Topic: Working with the memory vulnerabilities

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

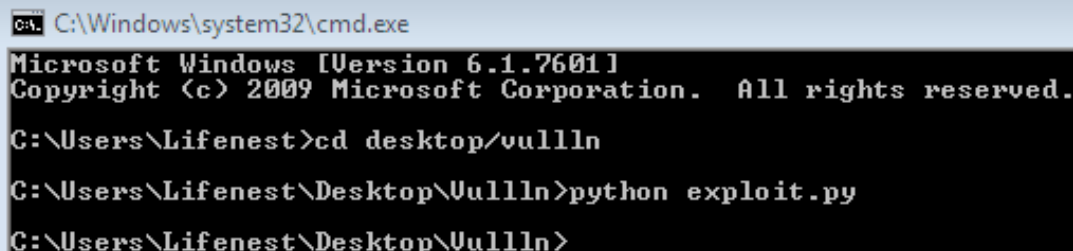
Analysis

- Crash the Vuln_Program_Stream program and report the vulnerability.

→

First we have to run the python script to generate payload.




Here the step1, iam running the python script which generates the payload

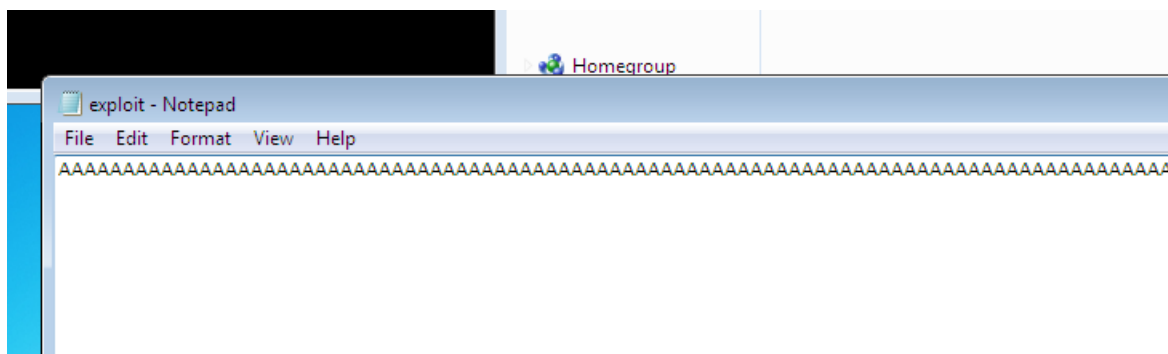


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Lifenest>cd desktop/vullln
C:\Users\Lifenest\Desktop\Vullln>python exploit.py
C:\Users\Lifenest\Desktop\Vullln>
```

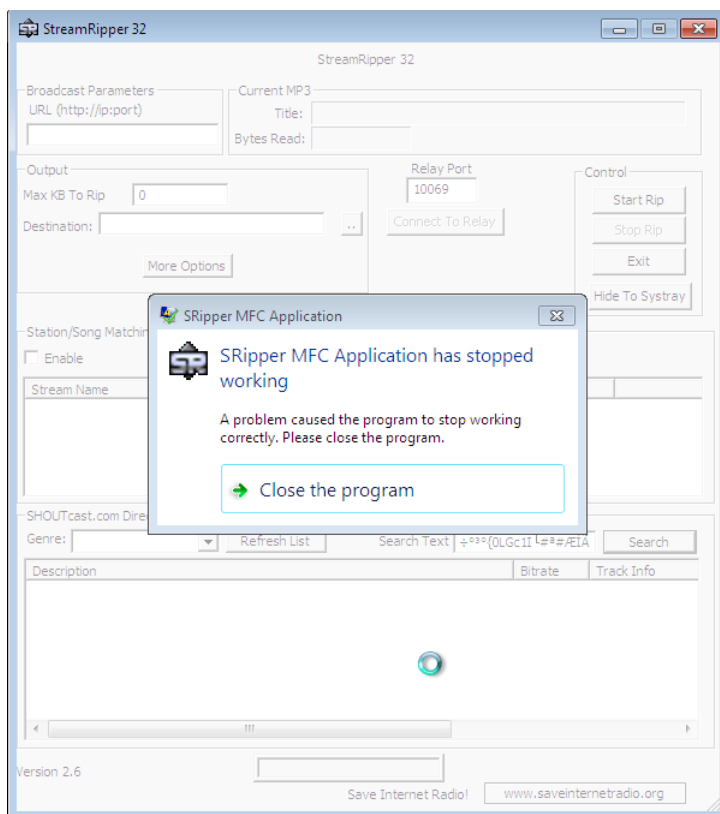
Now, after running the python script the payload will be generated

 exploit	4/5/2021 8:46 PM	Python File	3 KB
 exploit	4/11/2021 4:43 PM	Text Document	1 KB
 Vuln_Program_Stream	4/5/2021 8:46 PM	Application	800 KB



After the payload is generated we have to open the stream ripper and we have to insert the payload into a intake search bar which poses vulnerability.

Then the stream ripper application crashes and cmd opens.



This happens because of buffer overflow vulnerability.

A buffer overflow occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

After the stream ripper application crashes CMD didn't open in the stream ripper but as in frigate it opened. (Security of Windows 7 isn't disabled).