CSE 2010- Secure Coding

WIN 20-21

NAME:S.BHAVYA SREE

REG.NO:19BCN7257

Lab experiment - Working with the memory vulnerabilities

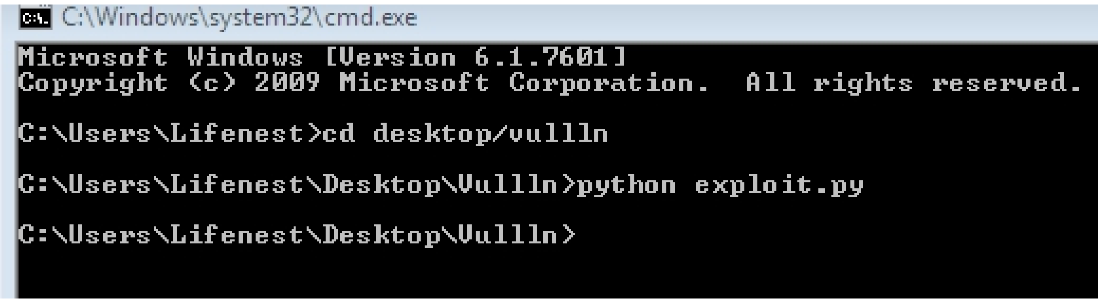
Task

- 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.

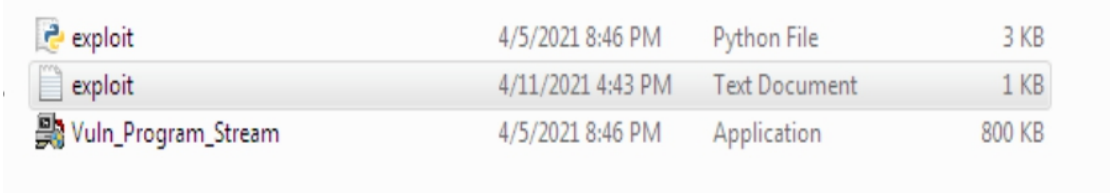
- Run the python script to generate payload.



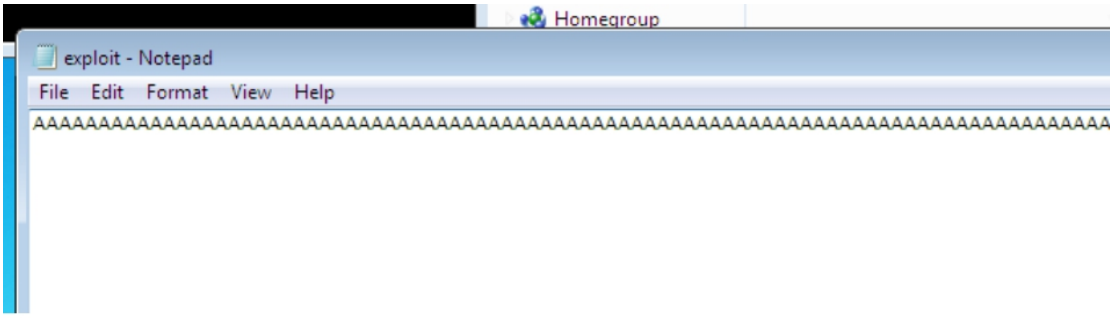
C:\Windows\system32\cmd.exe

```
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>
```

- Payload gets generated.

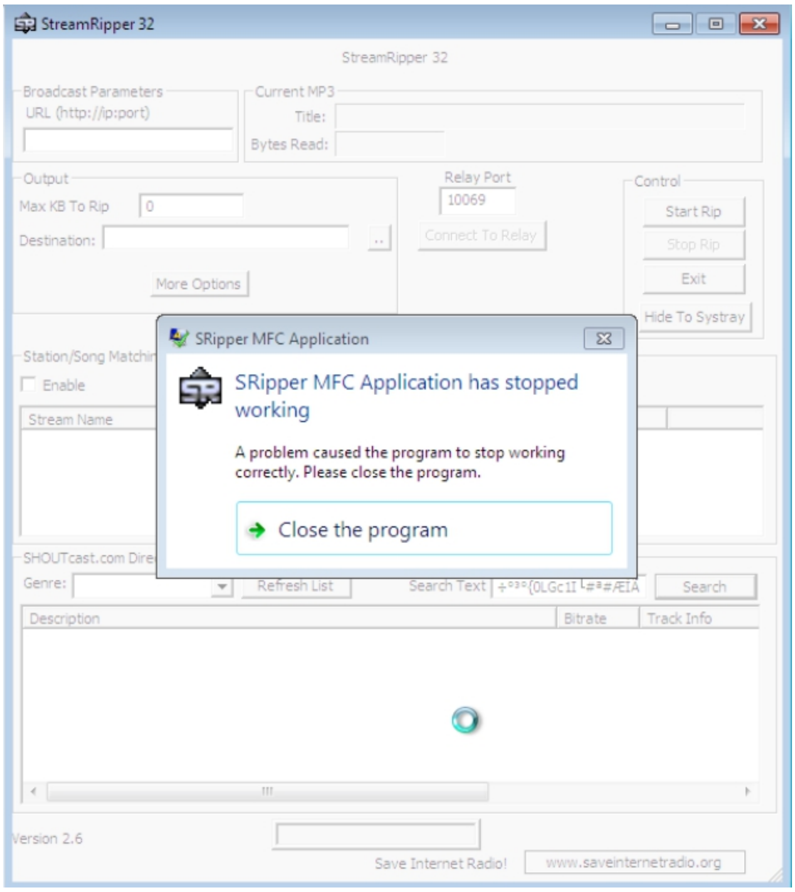


exploit	4/5/2021 8:46 PM	Python File	3 KB
exploit	4/11/2021 4:43 PM	Text Document	1 KB
Vuln_Program_Stream	4/5/2021 8:46 PM	Application	800 KB



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

-
- Open stream ripper and generate payload into intake search bar that has vulnerability.
- Then stream ripper crashes and cmd will open.



SRipper MFC Application has stopped working

A problem caused the program to stop working correctly. Please close the program.

-

Now this is because of buffer overflow, a vulnerability that is an anomaly where a program, while writing data to a **buffer**, **overruns** the **buffer's** boundary and overwrites adjacent memory locations.