

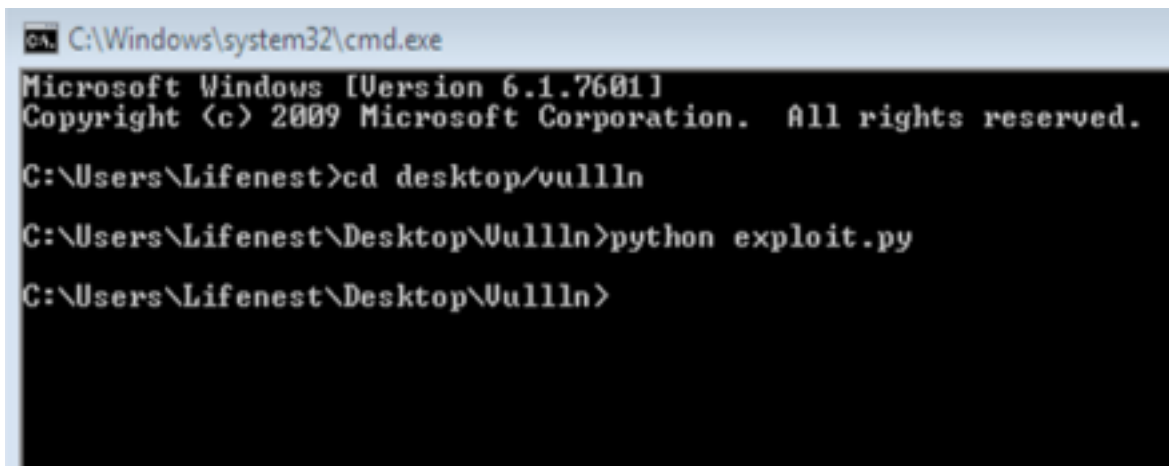
S.V.SAIVAMSI,19BCN7258

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




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

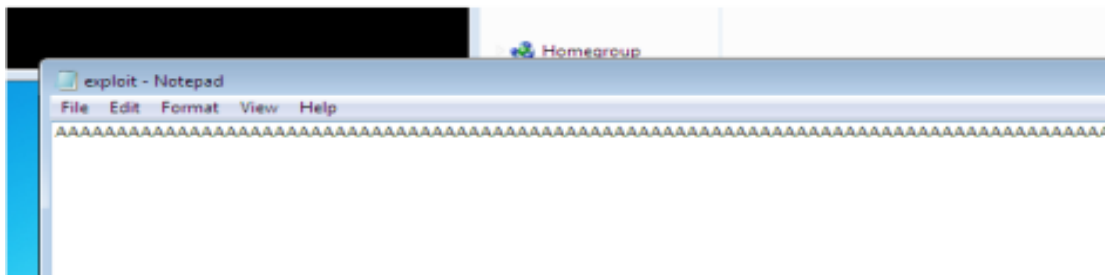


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

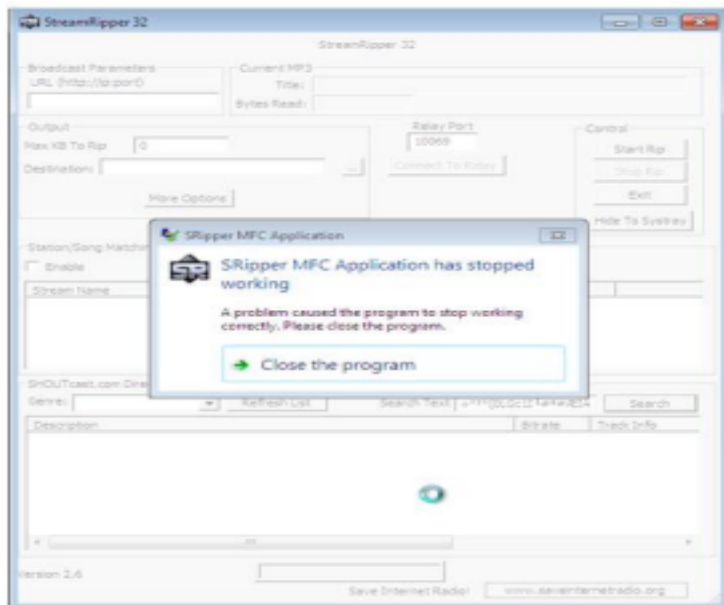
C:\Users\Lifenest>cd desktop/vullln
C:\Users\Lifenest\Desktop\Vullln>python exploit.py
C:\Users\Lifenest\Desktop\Vullln>
```

Now a payload will generate as shown,

 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



Now we open stream richer and insert payload then it crashes and command prompt will open



This happens because of the buffer overflow vulnerability

A buffer overflow occurs when the volume of data that is to be stored exceeds the storage capacity of the memory buffer. So, as a result the program attempting to write the data to buffer overwrites adjacent memory locations then as the data that to be stored in a particular memory location is stored in the adjacent memory locations also there occurs buffer overflow.