**Lab experiment - Working with the memory vulnerabilities – Part II**

**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 II (exploit2.py- check today’s folder) to generate the payload**
* **Install Vuln\_Program\_Stream.exe and Run the same**

**Analysis**

* **Try to crash the Vuln\_Program\_Stream program and exploit it.**
* **Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).**

**Example:**

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

* **Change the default trigger to open control panel.**

**Happy Learning!!!!!!**