S.V.SAIVAMSI ,19BCN7258

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

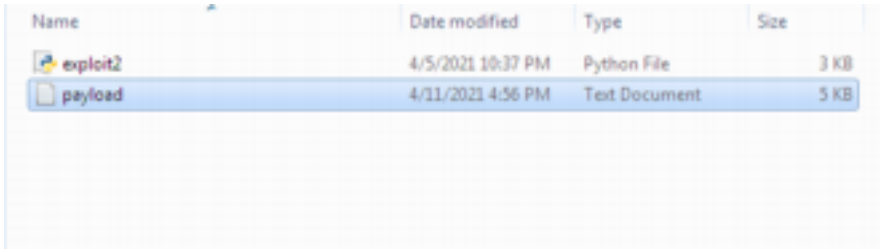
Analysis:

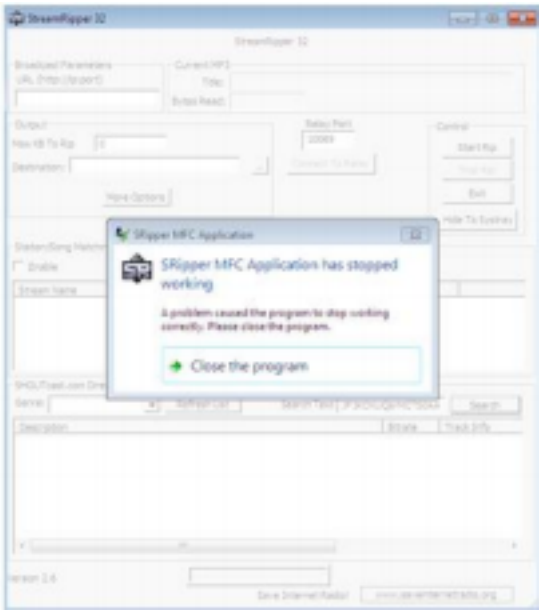
- Try to crash the Vuln_Program_Stream program and exploit it. • Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali Linux).

  Example:

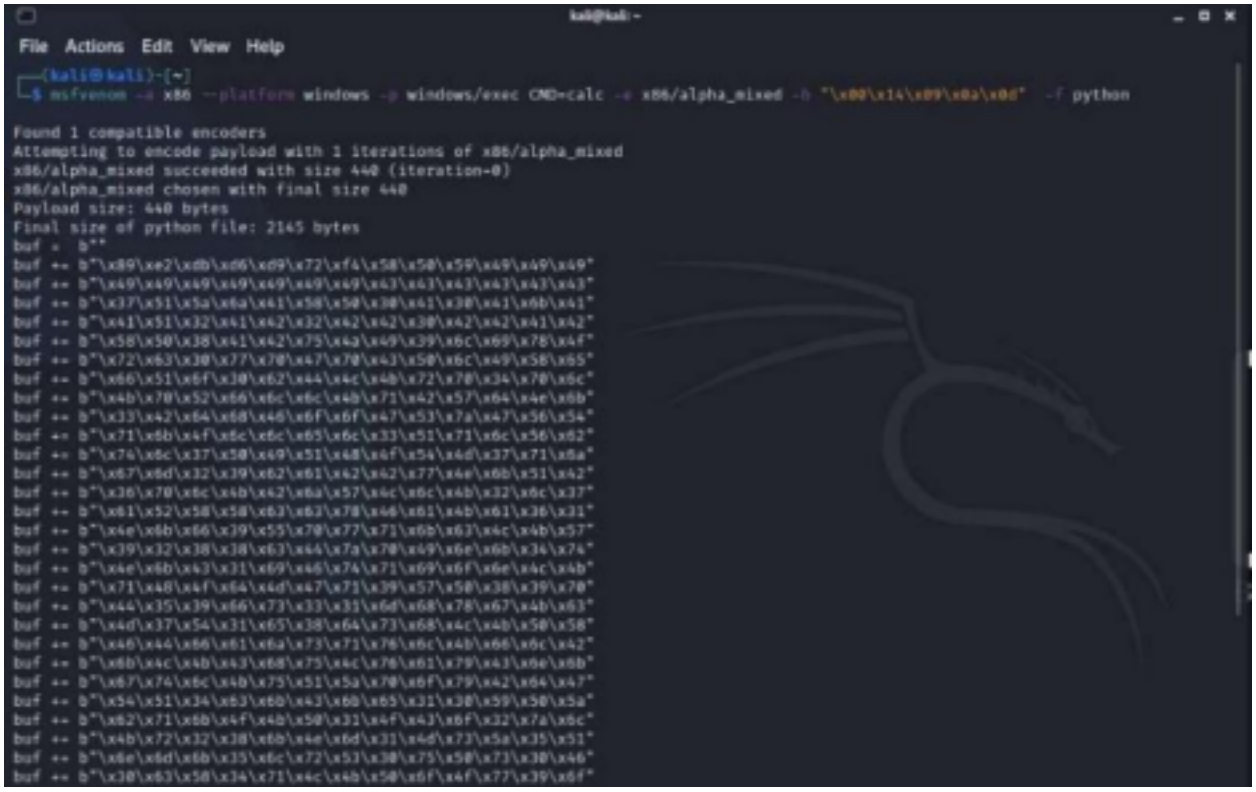
  msfvenom -a x86 --platform windows -p windows/exec CMD=calc - e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python • Change the default trigger to open control panel.

A payload is generated as

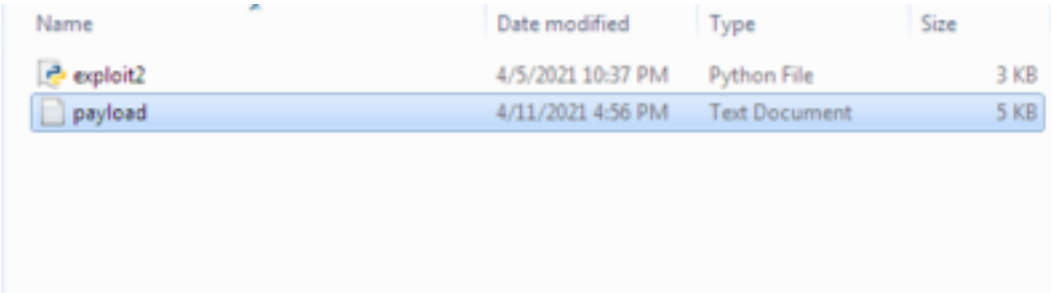




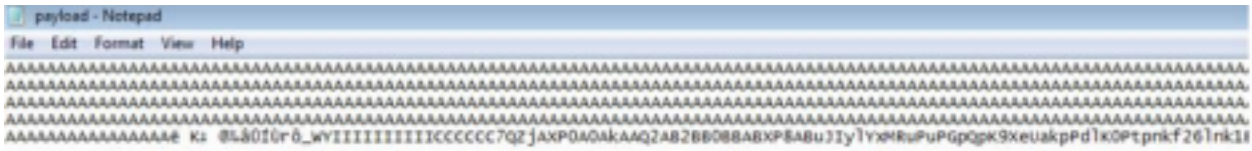
Now we crashed the vuln program with payload successfully
Now we generate code in kali linux



Payload for changed code:

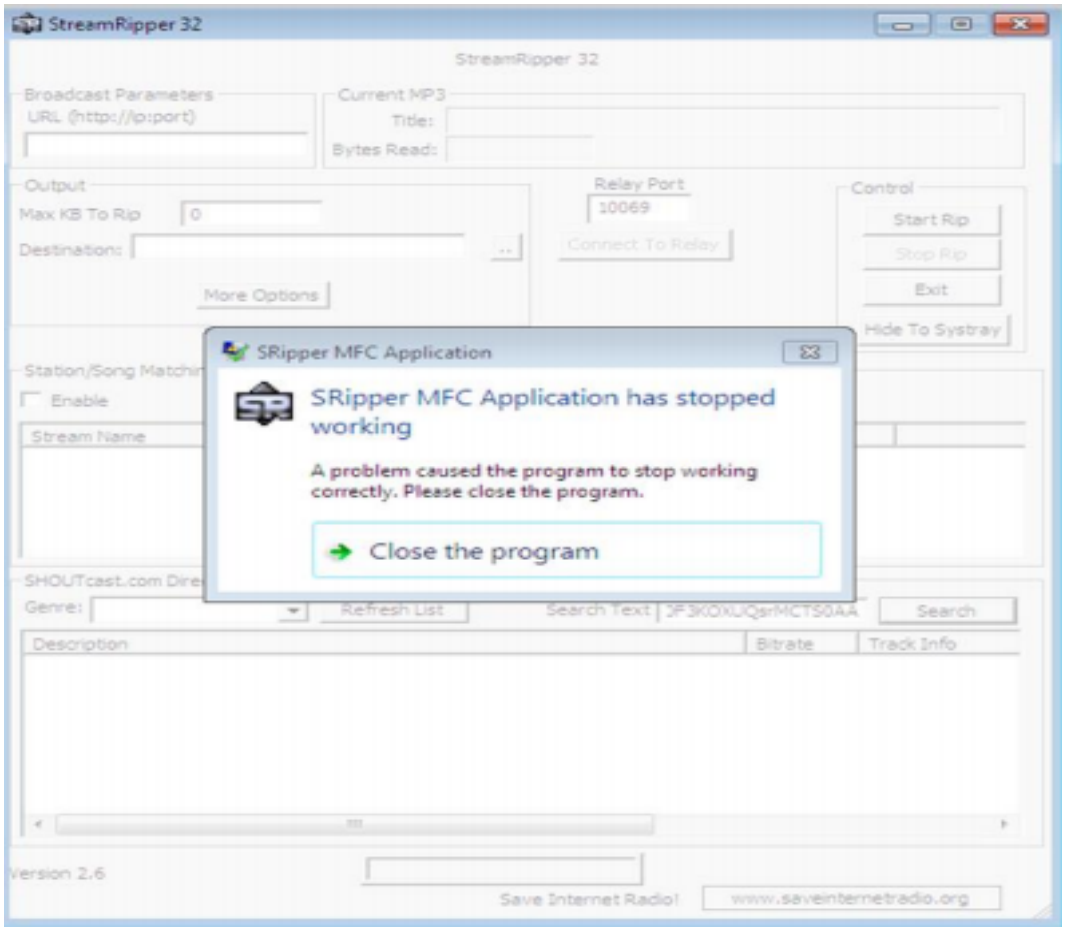


Payload after executing exploit2.py script for calculator:



After running it in the vlun:

Vuln program crashed



After crashing calculator opened