**9.Malicious Archive Execution**

1.Execute the extracted file

Run the extracted calc.exe:

& "$env:USERPROFILE\Desktop\calc\calc.exe"

This will launch the Calculator app (harmless payload, but useful for testing).

2. Monitor logs with Sysmon or Windows Defender

If Sysmon is installed:

* Open Event Viewer:
* eventvwr.msc
* Navigate to:
* Applications and Services Logs > Microsoft > Windows > Sysmon > Operational
* Look for Event ID 1 (Process Create), filtering for calc.exe and see:
  + Parent process (likely 7z.exe or explorer.exe)
  + Image path (C:\Users\Aarti\Desktop\calc\calc.exe)
  + Command line used
  + Hash of the executable (Sysmon can log this if enabled)

3. Check the file hash

Run PowerShell to get SHA256 hash of extracted file:

Get-FileHash "$env:USERPROFILE\Desktop\calc\calc.exe" -Algorithm SHA256

Save this hash for correlation with Sysmon or antivirus logs.

4. Check Windows Defender Logs

In Event Viewer, check:

Applications and Services Logs > Microsoft > Windows Defender > Operational

for any alerts triggered by the file execution.