**3. Persistence via Registry Run Keys**

Step-by-Step Guide

1. Create a Malicious or Benign Payload

Example harmless script (hello.ps1):

Start-Process notepad.exe

Save it at:  
C:\Users\<Username>\hello.ps1

2. Add a Registry Key for Persistence

Registry location:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

You can use PowerShell to add this:

Set-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" `

-Name "MyScript" `

-Value "powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -File C:\Users\<Username>\hello.ps1"

Or use Command Prompt (as Admin):

reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v MyScript /t REG\_SZ /d "powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -File C:\Users\<Username>\hello.ps1" /f

This ensures the script runs every time the user logs in.

3. Test Persistence

* Restart the VM or log off and back in.
* Notepad should launch automatically.

4. Verify Registry Entry

Manually:

* Run regedit
* Go to HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
* You should see MyScript with the payload path.

|  |  |
| --- | --- |
| Component | Example |
| Registry Path | HKCU\...\Run |
| Value Name | MyScript |
| Value Data | powershell.exe -ExecutionPolicy Bypass ... |
| Payload Location | C:\Users\<User>\hello.ps1 |