**Challenge Title: Magic**

**Challenge Description**:

There is magic associated with each file. Uncover it…

**Solution**:

In this reverse engineering challenge, participants are provided with a Windows executable that appears to be non-functional. The challenge revolves around inspecting the file signature using a hex editor. The given executable has undergone a slight modification to its signature, rendering it unable to execute. Windows typically uses the MZ and PE signatures to identify executable files, and in this case, they've been altered to PZ and ME, respectively.

NOTE: Search for magic number for file types.

Steps to find flag: FLAG{file\_signatures\_are\_important}

File Inspection:

Open the provided executable in a hex editor to inspect its contents. Look specifically for the MZ and PE signatures, which are essential components of a valid Windows executable.

Signature Modification:

Identify the altered signatures where MZ (magic number) has been changed to PZ and PE has been changed to ME. These modifications disrupt the expected file structure, causing the executable to be rejected by the operating system.

Reverse the Changes:

Use the hex editor to reverse the modifications by changing PZ back to MZ and ME back to PE. This process involves directly editing the hexadecimal values in the file.

Save the Changes:

Save the modified executable with the corrected signatures.

Execution:

Attempt to run the modified executable. With the correct signatures restored, Windows should now recognize and execute the application.

Flag Printing:

Once successfully executed, the program should print the flag to the console or provide some output that reveals the solution.