**Challenge Title: NSA\_hid\_dragon**

**Challenge Description**:

If you can’t see it, then try feeding it to the Dragon head.

**Solution**:

In this reverse engineering challenge, participants are introduced to the Ghidra tool, a powerful open-source software for analyzing binary code. The goal is to guide participants through using Ghidra to explore the provided Windows executable and uncover the flag. The flag is hidden within the main program logic.

**FLAG : FLAG{ghidra\_is\_useful}**

Steps to find flag:

Download and Install Ghidra for windows:

If participants don't have Ghidra installed, instruct them to download and install it from the official website: Ghidra Official Website

Open Ghidra:

Launch Ghidra and create a new project. Load the provided Windows executable into the project.

Navigate to Entry Point:

In the Symbol Tree window, locate and click on the entry point of the executable under label section. This is typically labeled as "entry".

Explore Functions:

Look for a function that starts with "FUN..." in the decompiler window.

Locate \_main Function:

Within the chosen function, find the "\_main" function. This is where the main program logic resides.

Inspect Code:

Explore the decompiled code within the "\_main" function using the decompiler window. Look for any references, conditions, or operations that might lead to the flag.

Flag Identification:

Identify the flag within the "\_main" function. The flag may be present as a string or as part of a conditional statement.