2PAC - BINARY 100

This space mission is based on a secret hardware component known only by the innovation team. If it was revealed to the world, it would endanger the whole mission: find the secret key before the spies do, or the 2020 mission will be compromised.

We are given of an *ELF 32-bit* file, the first thing we tried to do was to run strings on it but it led to nothing. So we started to analyze it statically.

The first thing we noticed is the presence of only the *entry0* function, that was strange to us as if it has to print something at least one function (e.g. *printf*, *write*) is usually needed.

So analyzing the *entry0* we noticed immediately the presence of many int 0x80, an instruction used to run the syscalls, so we understand the lack of function!

The firsts two syscall are a *getpid()* and a *ptrace()*, so we “nopped” them to debug the executable.

Starting to debug the program we found that it generates a function where it jumps at *0x1059*, by debugging this function we found that it generates the flag in memory.

{FLG:wHo_n33ds_1ibc}