Flipnote

Category: Pwn
Difficulty: Hard
Author: Localo
Writeup by: argator

Description

I was unable to come up with an interesting vulnerability, so instead I just cheated like all the hardware hackers do and used a laser instead. Have fun ;)

Summary

The challenge provides the source code together with the compiled binary and the Dockersetup.
We don't get a port and a domain to connect to the service 'vuln' but instead we get a ssh connection to some server.
Exploring the server and also through looking into the Dockerfile, we see, that we are on a standard Ubuntu setup, while we are really restricted in the installed commands, as wget, curl and python etc. aren't installed, we see three "unusual files":

- ynetd
- /flag
- /vuln

ynetd will come in handy later.
/flag is obviously not accessible to non-root users.
And /vuln has the suid bit set, allowing to run the binary with root rights.

As it is a pwn chall, let's check the libc version installed on the system:
`ldd /vuln` and `/lib/x86_64-linux-gnu/libc.so.6 --version` reveales, that GLIBC 2.35 is installed.

Binary

Running `checksec` on the binary, we can see that all common security features are activated but for some reason the binary is compiled with debug symbols.

Program features

Running the binary shows, that the program implements a notes server with the following abilities:

Input : Action

- a : add a note
- e : edit a note
- f : flip a note
- r : remove a note
- q : quit the program

The flip a note ability is quite unique and teasered from title and description.
It allows you to use a "laser" to flip (xor with 1) one single bit of the first 8 bytes of the note.
Unfortunately the "laser will break and terminate the program" after the second time, so this feature can be used only twice.

Source Code

The first thing to note are the last two lines in the main function: