Project Proposal - G02

Like we discussed in the email our group would like to show and develop a SeedLab like guide that is able to introduce the process of reverse engineering to students taking this class.

Reverse engineering a piece of software or a program can be done with a lot of different programs but we want to focus on using those that are free and open source.

One of the most popular tools that fits these requirements is Ghidra. Ghidra is developed by the NSA (National Security Agency of the USA). It has support for many different architectures (x86, x86-64, arm, arm64, risc v, …) and is fairly easy to install because it uses Java.

Our main idea for this is as follows:

First we want to introduce the basic concepts of Ghidra and show the relevant parts of the interface. This step will allow the students that are following the guide to quickly check how to do something using the existing UI.

Then we would like to show how programs can be reversed engineered and their contents/behavior studied.

This will bring us to the actual first step that will require some student engagement.

Some software nowadays uses a License or a Password to unlock certain features. By building a simple program and giving it as a complementary file to the students (without access to the source code) we can show them a real-world case of how to reverse engineer.

This part will show them

- how to load the program in Ghidra
- how to find the subroutines
- how to bypass these License/Password checks

By itself this part will surely teach the basics however we want to also try another thing. If possible and if it does not make the guide's difficulty exponential we would also like to show how vulnerabilities are sometimes found or exploits developed.

For this last part we would like to show telnetd which allowed users to become root without knowing the password for the root account (In the email I said ssh but it was actually telnetd).