SECURE SYSTEMS ENGINEERING (CS6570), IIT MADRAS

Assignment 2

ROP.

Steps involved.

1. Download and install ROP gadget from `https://github.com/JonathanSalwan/ROPgadget`, from the given github repo.
2. Fill in your roll number(s) in the C code.
3. Compile the C code given with the following options: `gcc -m32 -O0 -static tut2.c -o tut2`. This will create a 32 bit executable with statically linked libraries.
4. Find the ROP gadgets on tut2.

Implement and Answer the following Questions:

(a) Describe the attack plan that you are going to adopt along with the vulnerabilities in the source code.

(b) List all the useful gadgets (or achieve the same result) that ROPgadget can find.

(c) Describe your complete stack size that used to compute the result.

(d) **Part 1**: Pick your gadgets, stitch them together on the stack, so that 15^{th} Fibonacci number is printed on the screen.

(e) **Part 2**: Pick your gadgets, stitch them together on the stack, to kill a process using its PID.

(f) You are done!! Submit your payloads and report.

Happy Hacking !!!