SECURE SYSTEMS ENGINEERING (CS6570), IIT MADRAS

Total Time : 1 week **Capture the Flag 2 (ROP)**
Max Marks : 20 **23/8/2017**

This is a take home assignment, which can be done in groups of atmost two.

For the C code (with similar bugs as in the previous tutorial), use buffer overflows and ROP gadgets to print the factorial of 10.

These are the steps involved.

1. Download and install ROP gadget from https://github.com/JonathanSalwan/ROPgadget. This may require you to also install capstone. Please see the readme file in the git hub.
2. Turn off ASLR for your Linux kernel (refer class slides).
3. Fill in your roll number(s) in the C code.
4. Compile the C code given with the following options: gcc -m32 -O0 -fno-stack-protector –static tut2.c -o tut2. This will create a 32 bit executable with statically linked libraries.
5. Execute ROP gadget on tut2 using the command python ROPgadget.py –binary tut2. Have a look at –help in ROPgadget.py for many more interesting options.
6. Pick your gadgets, stitch them together on the stack, so that 10! is printed on the screen. One way is to fill the result in the glb global variable, which gets printed in main.
7. Implement and answer the following questions.
   (a) Implement NOPs in ROP and verify that they indeed work. What does the stack containing 10 NOPs look like.
   (b) The most favorite gadget looks like pop X; ret. This gadget lets you easily fill registers without any restrictions. List all such gadgets (or achieve the same result) that ROPgadget can find. The more number of registers that you can manipulate this way, the easier it would be build your payload.
   (c) Implement a multiplication gadget that multiplies two integers (imul instruction). The integers could be present in either memory or registers. Describe the gadget that you used here.
   (d) Use the above multiplicaion gadget that you found to compute 10!. Describe the gadget here.
   (e) Use glb and find a gadget that will display the factorial of 10. Describe the gadgets that you had used.
   (f) Describe your complete stack that computes 10!.
   (g) You are done!! Submit the document and the payload through moodle.