National Taiwan Normal University
CSIE Information Security: A Hands-on Approach

Instructor: Po-Wen Chi
Due Date: 10 18, 2021, AM 11:59

Assignment 1

Policies:

- Zero tolerance for late submission.
- Please pack all your submissions in one zip file. **RAR is not allowed!!**
- I only accept **PDF**. MS Word is not allowed.
- Hand-writing is not allowed.

1.1 SEED Lab (50 pts)

Environment Variable and Set-UID Lab
https://seedsecuritylabs.org/Labs_20.04/Software/Environment_Variable_and_SetUID/

Please record all your steps with screen captures and answer all questions.

1.2 ping.c (15 pts)

Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply. The program reports errors, packet loss, and a statistical summary of the results, typically including the minimum, maximum, the mean round-trip times, and standard deviation of the mean.

I will give you an example code of ping implementation. The code is from the following site:
https://gist.github.com/sfantree/dd3fb67ef86d5be69b7b72a58fd3af0d

Please answer the following questions:

1. Why there are lots of **unpack error** in this program?

2. This program should be executed with the root identity. That is, you should use **sudo** when you use this ping. Why do you need the root identity to run this program?

3. How about the ping program in your system? You may guess it is a Set-UID program. Unfortunately, it is not. Why?

1.3 setuid vs. seteuid (15 pts)

What is the difference between **setuid** and **seteuid**? Please design a lab, including the code and steps to describe the difference. I will not accept the answer copy from the manual directly.

1.4 execve (15 pts)

In our code, when we use **execve()** to execute an external program, we pass NULL in the third argument. How many environment variables will the process running has? Please design a lab to verify your answer.

1.5 ld-linux (15 pts)

In Linux, many environment variables are ignored if the program by the dynamic linker if the program to be executed is a Set-UID program. Two such examples are **LD_PRELOAD** and **LD_LIBRARY_PATH**. Please read the manual of ld-linux (https://linux.die.net/man/8/ld-linux) and explain why the following environment variables are also ignored:

1. **LD_AUDIT**
2. **LD_DEBUG_OUTPUT**

You should also design a lab to show how to use these two variables to launch attacks.