Lab 1: Set-UID Program Vulnerability

Lab Description

`Set-UID` is an important security mechanism in Unix operating systems. When a `Set-UID` program is run, it assumes the owner's privileges. For example, if the program's owner is root, then when anyone runs this program, the program gains the root's privileges during its execution. `Set-UID` allows us to do many interesting things, but unfortunately, it is also the culprit of many bad things. Therefore, the objective of this lab is two-fold: (1) Appreciate its good side: understand why `Set-UID` is needed and how it is implemented. (2) Be aware of its bad side: understand its potential security problems.

Lab Tasks

This is an exploration lab. Your main task is to "play" with the `Set-UID` mechanism in `Linux`, and write a lab report to describe your discoveries. You are required to accomplish the following tasks in `Linux`:

1. (20 points) Figure out why "`passwd`", "`chsh`", "`su`", and "`sudo`" commands need to be `Set-UID` programs. What will happen if they are not? If you are not familiar with these programs, you should first learn what they can do by reading their manuals. Please copy these commands to your own directory; the copies will not be `Set-UID` programs. Run the copied programs, and observe what happens.

2. (20 points) Run `Set-UID` shell programs in `Linux`, and describe and explain your observations.

   (a) Login as root (in Ubuntu, you can do this by using `sudo su`", copy `/bin/zsh` to `/tmp` using command `cp` (https://www.geeksforgeeks.org/cp-command-linux-examples/), and make it a set-root-uid program with permission `4755`. Then login as a normal user, and run `/tmp/zsh`. Will you get root privilege? Please describe your observation. For example, you can write to a file that only root user has write permission on.

   If you cannot find `/bin/zsh` in your operating system, please use the following command to install it:

   - Note: in our pre-built `Ubuntu` VM image, `zsh` is already installed.
   - For `Fedora`

     ```
     $ su
       Password: (enter root password)
     # yum install zsh
     ```

   - For `Ubuntu`

     ```
     $ sudo apt-get install zsh
     ```

(b) Instead of copying /bin/zsh, this time, copy /bin/bash to /tmp, make it a set-root-uid program. Run /tmp/bash as a normal user. will you get root privilege? Please describe and explain your observation.

3. (Setup for the rest of the tasks) As you can find out from the previous task, /bin/bash has certain built-in protection that prevent the abuse of the Set-UID mechanism. To see the life before such a protection scheme was implemented, we are going to use a different shell program called /bin/zsh. In some Linux distributions (such as Fedora and Ubuntu), /bin/sh is actually a symbolic link to /bin/bash. To use zsh, we need to link /bin/sh to /bin/zsh. The following instructions describe how to change the default shell to zsh.

```
$ sudo su
  Password: (enter password)
# cd /bin
# rm sh
# ln -s zsh sh
```

4. (15 points) **The PATH environment variable.**
The system(const char *cmd) library function can be used to execute a command within a program. The way system(cmd) works is to invoke the /bin/sh program, and then let the shell program to execute cmd. Because of the shell program invoked, calling system() within a Set-UID program is extremely dangerous. This is because the actual behavior of the shell program can be affected by environment variables, such as PATH; these environment variables (stored in /etc/environment) are under user's control. For example, the user can add a new path to PATH by using export PATH=/path/to/your/dir:$PATH. Note that this change is only effective for the current terminal.vim By changing these variables, malicious users can control the behavior of the Set-UID program.

The Set-UID program below has to be created by the root user and is supposed to execute the /bin/ls command; however, the programmer only uses the relative path for the ls command, rather than the absolute path:

```
#include "stdio.h"
#include "stdlib.h"
   int main()
   {
       system("ls");
       return 0;
   }
```

(a) Can you let this Set-UID program (owned by root) run your code instead of /bin/ls by add a new directory to PATH? If you can, is your code running with the root privilege? Describe and explain your observations. The command you can use to add a new directory to PATH is export PATH=/path/to/your/dir:$PATH

(b) Now, change /bin/sh so it points back to /bin/bash, and repeat the above attack. Can you still get the root privilege? Describe and explain your observations.

Submission

You need to submit a detailed lab report with **screenshots** to describe what you have done and what you have observed; you also need to provide explanation to the observations that are interesting or surprising. Submit the final Word or PDF file to Canvas.