Man Tik Li

CS 377 - 001

September 28, 2020

**Lab 1**

1. First use “env | grep PWD” to find the value of PWD. Then use “export” to change the value of PWD to bob and use “printenv PWD” to print out the value of PWD has changed to bob. After that, I used “unset” function to delete the variable and used “printenv PWD” to check that no value in PWD.Text

   Description automatically generated
2. Step1 1: When completing the program, I got an error on printenv() because of the Line ➀ sign that after the printenv statement.

Text

Description automatically generated

Step 2: After commenting out the Line ➀ and Line ➁, the program successfully compiles and run. The code prints the values of the specified environment variables that part of environment.

Text

Description automatically generated

Output: I captured the first and the last part of the output.

Text

Description automatically generatedText

Description automatically generated

1. After compile and run the code, the program didn’t print out any value from environment variables.

Text

Description automatically generated

After change the third arguments in execve from NULL to environ, the program prints all the environment variables.

Conclusion: The execve() has three parameters: filename, array contains the arguments, and the envp array contains the environment variables. If set the third arguemnts in execve() to NULL, the process does not pass any environment variable. If change it to environ, it passing all the environment variables.

1. Output:Text

   Description automatically generatedText

   Description automatically generated
2. The program will change the value for PATH, LD\_LIBRARY\_PATH, and the user defined variable to what I defined in screenshot. The reason we can change the value and create new variable because of the ownership permission of the file has change to root. When the file is under root, any non-root user cannot access the file. In this case, all the new process will be fork with root permission.Text

   Description automatically generatedText

   Description automatically generatedText, chat or text message

   Description automatically generated
3. Yes, you can let set-uid program that is owned by root to run the code. However, it is unsafe.

Text

Description automatically generated

1. Text

   Description automatically generatedText

   Description automatically generated
2. Step1:

Text

Description automatically generated

Step 2: Comment system() and uncomment execve()

Text

Description automatically generated

Yes, attacks in Step 1 still work, I can read the file content.

1. Text

   Description automatically generated