CSCI 400 Lab 4

**Name: Christopher Gonzalez**

**Class Section: CSCI 400 02 [35583]**

**Date: October 1, 2024**

**Instructions**:

* Login to your account at <https://pwn.college/>

**pwn.college username: Chris\_B\_Gonzalez**

**A screenshot of a computer

Description automatically generated**

* Go to the Linux Luminarium dojo: <https://pwn.college/linux-luminarium/>
* Complete the challenges in Untangling Users: <https://pwn.college/linux-luminarium/users/>

**Challenge 1: Becoming Root with su**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I started the challenge and opened the terminal. This challenge introduced me to the su command, which is an older version of sudo. In short, su was a command that was used to elevate to root access. When executed successfully, the user will be able to run as the root user. The first thing I had to do was enter “su” in the terminal, which then asked for the password. The instructions for this challenge informed me the password was “hack-the-planet”, so I entered it and successfully became the root user. After this, I used “cat /flag” to print the flag, which is highlighted in white.**

**Challenge 2: Other Users with su**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I started the challenge and opened the terminal. Once, again, I was instructed to use the su command, but this time, I was instructed the command will be used to switch to the zardus user. I began by entering “su zardus” since this command specifies my objective to switch to the zardus user. I was asked to give the password (which was “dont-hack-me” and I became the zardus user. Next, the instructions informed me to execute the /challenge/run file once I became the zardus user. I did this by typing “/challenge/run” which gave me the flag.**

**Challenge 3: Cracking Passwords**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I started the challenge and opened the terminal. I was instructed the flag was in /challenge/run, but I would need to switch to the zardus user first. Unfortunately, I was not given the password for this challenge because I needed to use the john program to crack the password based on the hash value of zardus’ password. Fortunately, a leak of the hash value was in /challenge/shadow-leak, so I began by typing “cat /challenge/shadow-leak” which have me the hash of the password at the very end. Next, I entered “john /challenge/shadow-leak” to crack the password based on the hash value. After waiting for a few minutes, it was revealed to me the password was “aardvark”. Using this knowledge, I proceeded to switch to the zardus user by typing “su zardus” and entering “aardvark” as the password. After this, I successfully became the zardus user, and proceeded to execute /challenge/run, which gave me the flag.**

**Challenge 4: Using sudo**

****

**To obtain the flag, I started the challenge and opened the terminal. This challenge introduced me to the advanced version of the su command which is sudo. Unlike su, sudo relies on policies that it checks for a user’s authorization to run things as root. I began by seeing if I could check the contents of the file by typing “cat /flag”, but the permission was denied. Seeing as /flag could only be accessed by a higher entity in terms of permissions, I entered “sudo cat /flag” to read the file as the root user. Fortunately, this line of code worked and gave me the flag.**