CSCI 400 Lab 3

**Name: Christopher Gonzalez**

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

**Date: September 28, 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 Perceiving Permissions: <https://pwn.college/linux-luminarium/permissions/>

**Challenge 1: Changing File Ownership**

**A screenshot of a computer

Description automatically generated**

**To attain this flag, I started the challenge and opened the terminal. This challenge introduced me to the chown command, which can be used to change the ownership of a given file. Once the terminal was running, I began by entering “/flag” to verify if I had access to the file by default. The terminal proceeded to inform me that I was denied permission from the /flag file, therefore I proceeded to enter “chown hacker /flag” so that ownership of the file was changed to my machine. After doing this, I inspected the contents of the file by entering “cat /flag” and I was given the flag.**

**Challenge 2: Groups and Files**

**A screenshot of a computer

Description automatically generated**

**To attain this flag, I started the challenge and opened the terminal. This challenge is like the first challenge, but instead of using the chown command, I was introduced to the chgrp command. This command is used to change ownership within a specified group rather than a specific user, but it is similar in function to the chown command. First, I checked if I had ownership of the /flag terminal, but I did not. I proceeded to change group ownership of the file by entering “chgrp hacker /flag” which effectively gave me ownership of the file. Finally, I checked the contents of the file by entering “cat /flag” and the flag was printed.**

**Challenge 3: Fun With Groups Names**

**A screenshot of a computer

Description automatically generated**

**To attain this flag, I started the challenge and opened the terminal. The instructions for this challenge informed me that the name of the group my machine was placed in was randomized. In the previous two challenges, I was told my machine was a part of the hacker group. Since this was no longer the case, I had to determine the randomized group name using the id command. After entering this in the terminal, I discovered the group name was “grp22028”, so I proceeded to change group ownership of the /flag file by entering “chgrp grp22028 /flag”. Once this was done, I used cat to look at the /flag file which successfully gave me the flag.**

**Challenge 4: Changing Permissions**

**A screenshot of a computer

Description automatically generated**

**To attain this flag, I started the challenge and opened the terminal. This challenge introduced me to the chmod command, which allows the user to change the permissions of a given file based on user, group, or others in one line. I began by checking the permissions set on \flag by entering “ls -l /flag”. This revealed that only the root user had read permissions to the file. I proceeded to use chmod to allow anyone complete access to the file by typing “chmod ugo+rwx /flag”. Though setting all these permissions may not have been necessary, it was done to ensure I can successfully obtain the flag. Afterwards, I entered “cat /flag” and saw the flag as the output.**

**Challenge 5: Executable Files**

**A screenshot of a computer

Description automatically generated**

**To attain this flag, I started the challenge and opened the terminal. I decided to begin by entering “/challenge/run” to see if I was allowed to execute the file by default, but the permission was denied to me. This was to be expected as the instructions for this challenge stated I needed to change execute permissions using chmod. Prior to doing this, I was curious and wanted to see what permissions were set. I entered “ls -l /challenge/run” and noted only read permissions were granted to all people. I proceeded to modify the execute permissions of the /flag file by typing “chmod ugo+x /challenge/run” and executed the file once again. Since the permissions were changed, the file was executed and gave me the flag.**

**Challenge 6: Permission Tweaking Practice**

**A screenshot of a computer

Description automatically generated**

**To attain this flag, I started the challenge and opened the terminal. This challenge required me to perform 8 rounds of changing the permissions of the /challenge/pwn file before being allowed to change permissions of the /flag file. Upon initiating /challenge/pwn, the round began, and I proceeded like so:**

* **Round 0: Needed permissions of "/challenge/pwn": rw-r—rwx**

**What I entered: chmod o+wx /challenge/pwn**

* **Round 1: Needed permissions of "/challenge/pwn": rw-rw-rwx**

**What I entered: chmod g+w /challenge/pwn**

* **Round 2: Needed permissions of "/challenge/pwn": rw-rwxrwx**

**What I entered: chmod g+x /challenge/pwn**

* **Round 3: Needed permissions of "/challenge/pwn": rw-rwxr-x**

**What I entered: chmod o-w /challenge/pwn**

* **Round 4: Needed permissions of "/challenge/pwn": -w-rwx---**

**What I entered: chmod uo-rx /challenge/pwn**

* **Round 5: Needed permissions of "/challenge/pwn": -w-rwxr—**

**What I entered: chmod o+r /challenge/pwn**

* **Round 6: Needed permissions of "/challenge/pwn": -w-rw-r—**

**What I entered: chmod g-x /challenge/pwn**

* **Round 7: Needed permissions of "/challenge/pwn": ---r--r—**

**What I entered: chmod ug-w /challenge/pwn**

* **(Round 8): Change the permissions of /flag to access the file**

**What I eventually entered: chmod ugo+rwx /flag**

**After all of this was completed, I looked at the contents of the file using “cat /flag” and was given the flag.**

**Challenge 7: Permissions Setting Practice**

**A screenshot of a computer

Description automatically generated**

**To attain this flag, I started the challenge and opened the terminal. This challenge operated similarly to the previous one, however the key difference between the two was the way I was changing permissions. In the previous challenge, I was changing permissions in in the following format: “chmod ugo+/-rwx /filename”. For this challenge, I had to change permissions differently like so: chmod u=rwx,g=rwx,o=rwx /filename. This different approach is longer than the previous technique but had greater specificity. Upon initiating /challenge/run, a set of 8 rounds for changing permissions began, and I proceeded like so:**

* **Round 0: Needed permissions of "/challenge/pwn": -w-r--r—**

**What I entered: chmod u=w /challenge/pwn**

* **Round 1: Needed permissions of "/challenge/pwn": rw-rw-r-x**

**What I entered: chmod u=rw,g=rw,o=rx /challenge/pwn**

* **Round 2: Needed permissions of "/challenge/pwn": r-x-wxr-x**

**What I entered: chmod u=rx,g=wx /challenge/pwn**

* **Round 3: Needed permissions of "/challenge/pwn": rwxrwxrw-**

**What I entered: chmod u=rwx,g=rwx,o=rw /challenge/pwn**

* **Round 4: Needed permissions of "/challenge/pwn": --xrw-rwx**

**What I entered: chmod u=x,g=rw,o=rwx /challenge/pwn**

* **Round 5: Needed permissions of "/challenge/pwn": -wx---r--**

**What I entered: chmod u=wx,g=-,o=r /challenge/pwn**

* **Round 6: Needed permissions of "/challenge/pwn": -wxrw—wx**

**What I entered: chmod g=rw,o=wx /challenge/pwn**

* **Round 7: Needed permissions of "/challenge/pwn": rwx---rw-**

**What I entered: chmod u=rwx,g=-,o=rw /challenge/pwn**

* **(Round 8): Change the permissions of /flag to access the file**

**What I entered: chmod a=rwx /flag**

**Afterwards, I used cat to view the contents of /flag, giving me the flag information.**

**Challenge 8: The SUID Bit**

**A screenshot of a computer

Description automatically generated**

**To attain this flag, I started the challenge and opened the terminal. The instructions for this challenge introduced me to the concept of the SUID bit which is an additional permission bit that allows the user to run a program as the owner of that file. To begin, I checked if I could execute the /flag by default, but I could not (which was expected). Next, I listed all the permissions of /challenge/getroot file as I can access the flag file through this program. I noted that user permissions were set to rwx, so I proceeded to use chmod to add the SUID bit by typing “chmod u+s /challenge/getroot”. Afterwards, I executed /challenge/getroot, which spawned a root shell for me to use to access the /flag file I couldn’t before (meaning I was essentially running as the root user). Finally, I looked at the contents of the /flag file by typing “cat /flag” and I was given the flag.**