CSCI 400 Lab 8

**Name: Christopher Gonzalez**

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

**Date: December 5, 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 Intro to Cybersecurity dojo:**[**https://pwn.college/intro-to-cybersecurity/**](https://pwn.college/intro-to-cybersecurity/)
* **Review short videos above challenges in Access Control:**[**https://pwn.college/intro-to-cybersecurity/access-control/**](https://pwn.college/intro-to-cybersecurity/access-control/)
* **Complete challenges level 1 through 16.**

**level1**

A computer screen shot of a computer screen

Description automatically generated

**To obtain the flag, I opened the terminal and started the challenge. These series of challenges will have me work with various access control systems to get the flag. It can be seen in the image that I, as the hacker, have read permissions to the flag file, so I simply entered “cat /flag” and it was given to me.**

**level2**

A screenshot of a computer

Description automatically generated

**To obtain the flag, I opened the terminal and started the challenge. Unlike the previous challenge, the flag file is owned by the root and I, as the hacker, have group permissions. However, since I still had easy access to the file, I did “cat /flag” once again and got the flag.**

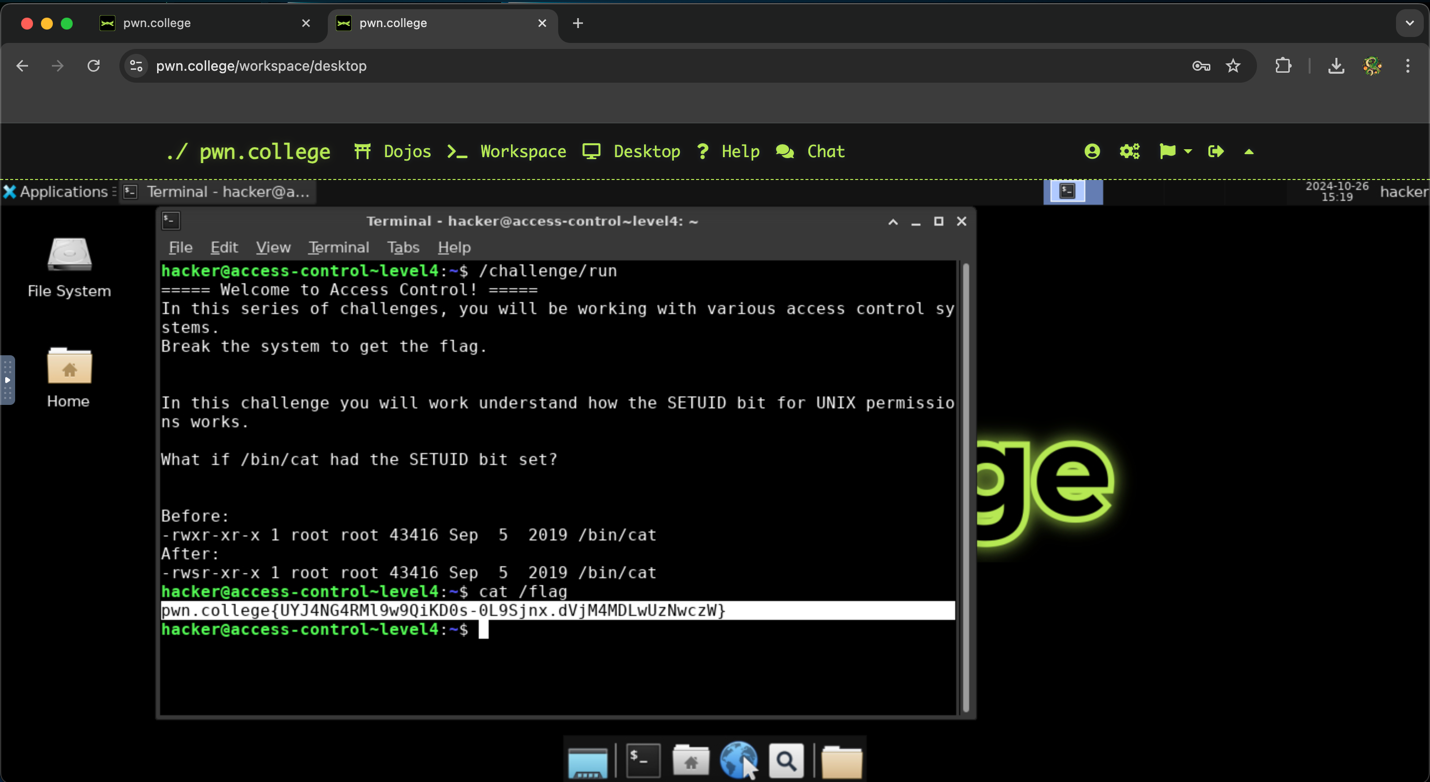
**level3**

A screenshot of a computer

Description automatically generated

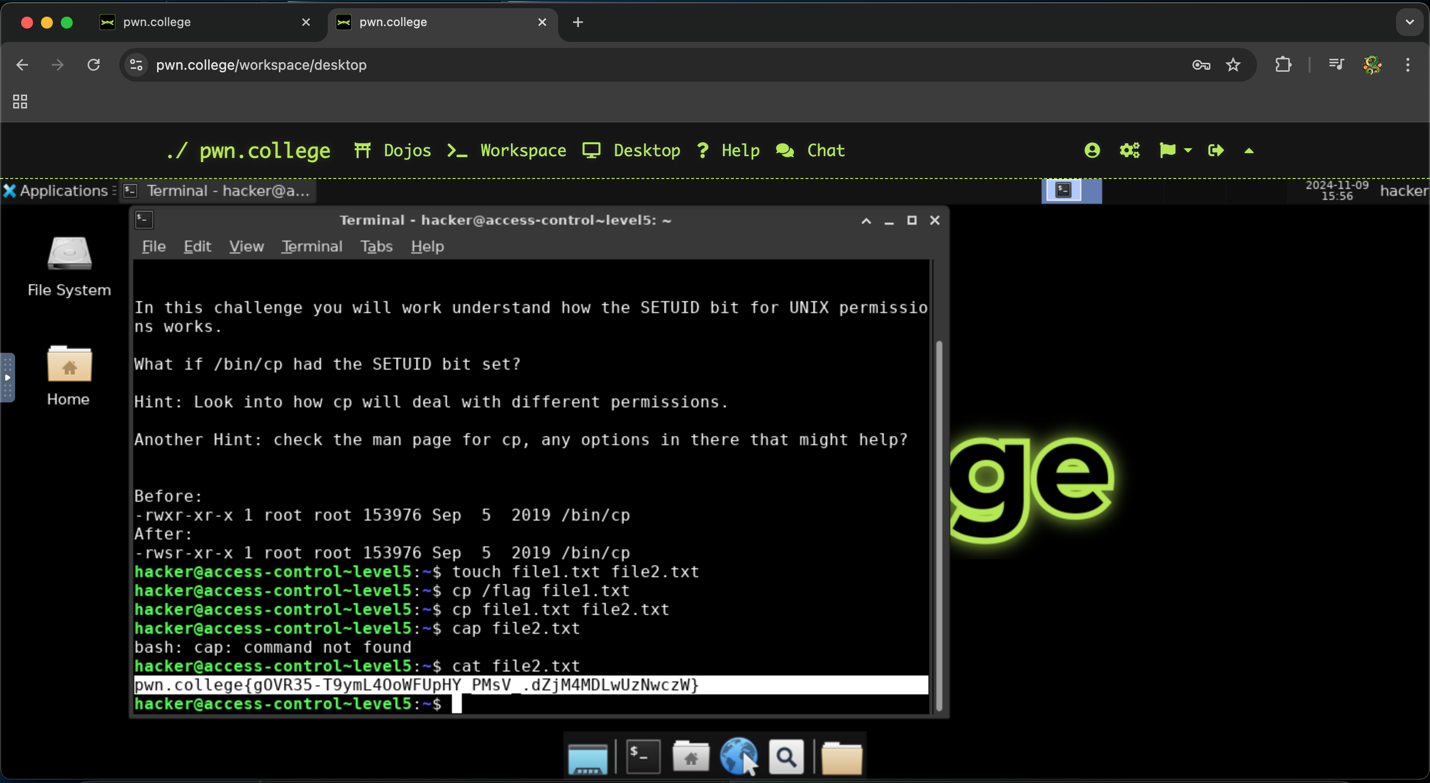
**To obtain the flag, I opened the terminal and started the challenge. This time, the file was owned by me, but all permissions were set to 0, meaning I could not read, write, or execute the file. Fortunately, I had the ability to change these permissions by entering the command “chmod ugo+rwx /flag”, which allowed me to give myself all permissions. Then I proceeded by entering “cat /flag”.**

**level4**



**To obtain the flag, I opened the terminal and started the challenge. This challenge reintroduced me to the SETUID bit, which allows a user to execute a program with the permission of another user. However, I noted that /bin/cat allowed for all other users to execute the command (as seen by the final x), so all I had to do was type “cat /flag”.**

**level5**

****

**To obtain the flag, I opened the terminal and started the challenge. The description of the challenge hinted at me the cp command would be significant to obtaining the flag. This command is short for copy, so I concluded that I would need to copy and transfer the flag file to a separate document. To begin, I created two files by entering “touch file1.txt file2.txt”. The reason I created two files was simply as an extra step to ensure success of copying the contents. Then, I copied the flag by typing “cp /flag file1.txt” which copied the information to the first file. Then I did “cp file1.txt file2.txt” which copied the flag again to the second file that was created. Finally, I looked at file.txt by typing “cat file2.txt” which contained the flag.**

**level6**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. The instructions for this challenge informed me the flag was owned by the root and a group (group\_afoeqfst). Since it would be far easier to access the flag file through group permissions, I used the sg command, which allows me to run a process with the privileges of the specified group. After specifying the group name and the command I wanted to run (cat /flag), I was asked to provide the password, which is given in the directions. The password was qxhwpcxn, and after providing this, I was given the flag.**

**level7**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. This challenge is like the previous level, but this time permissions were given to a specific user rather than a group. I was instructed to use the su command for this challenge, which allows me to switch to the user account given (user\_rjfesjbx) and run commands with their privileges. I began by typing “su user\_rjfesjbx” which them required me to give the password. It was given to me that the password for this user was svykkxql, so I entered this, and I was running as that user. Then I simply did “cat /flag” and the flag was mine.**

**level8**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. This challenge is essentially identical to level8, but the only difference is that I had to sudo to a different user (user\_siqgvxzj) and provide the respective password (siewcuvg). Once I was running as this user, I did “cat /flag” once again and completed the challenge.**

**level9**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. This challenge was once again identical to level8 and level9, where the only difference was the user (user\_znucucpr) and their password (fhzmllk). I began by entering “su user\_znucucpr” and provided the appropriate password. Once I was running as this user, I did “cat /flag” and got the flag.**

**level10**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. This challenge provided me with a list of users; however, it was informed to me that only one user belonged to group\_yrg, which has permissions to the flag file. There are two ways one could proceed. The user can either sudo into each account and check if they have permissions to the flag file or use getent. This command helps a user determine the number of accounts associated with a given group. I began by entering “getent group group\_yrg” and the output was user\_aejadbld. This informs me that user\_aejadbld is the only user in group\_yrg, meaning I had to sudo into this account. I proceeded by entering “su user\_aejadbld” and entered the password provided (kytmckfl). Then I did “cat /flag” and got the flag.**

**level11**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. To capture this flag, I was instructed that I would need to switch between two accounts (user\_ggcgrvip and user\_bbszfmud) using the su commad. I began by sudoing to the first account and entering the appropriate password (xahnukuv). Once I was running as user\_ggcgrvip, I typed the command “cd /tmp” because it was also given to me that the flag was placed somewhere in /tmp. Then, I did “ls -l” to list all the files/directories. I noted the last directory (tmp8xzwdpd6) and did “cd tmp8xzwdpd6”. I repeated to to “ls -l” and saw that a file titled tmp6x0a77w1 could be read by the other user (user\_bbszfmud). I proceeded by sudoing to user\_bbszfmud and entered its password (xhtnpnjg). Finally, I did “cat tmp6x0a77w1” which contained the flag.**

**level12**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. This challenge is identical to level11, but this time I would need to switch between three accounts (user\_yguxcxau, user\_sqonwyye, and user\_jjdgecho). Since it wasn’t as obvious which account I needed to sudo to first, I did “cd /tmp” which informed me user\_sqonwyye had permissions to tmpmp2hvnih. I sudoed to user\_sqonwyye first and entered the password. Then, I did “ls -l” as the user and changed to the tmpmp2hvnih directory using cd. Once again, I did “ls -l” and saw user\_jjdgecho had permissions to tmp38nsnmze. I proceeded to sudo to user\_jjdgecho and entered the password. Then, I did “ls -l” as this user and changed to the tmp38nsnmze directory using cd. I did “ls -l” and saw user\_yguxcxau had permissions to tmps26i9w13. I sudoed to this account and did “cat tmps26i9w13” which finally gave me the flag.**

**level13**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. Unlike all the previous challenges, I had to obtain this flag by answering trivia correctly. Fortunately, I had 120 seconds to answer a single question. The question can be seen in the image, where I was given 4 levels in a MAC system: TS, S, C, and USC. It was given to me that TS was the most sensitive, which also means it is the most powerful. The question asked if a subject with level C can write to an Object with level C. Since the object will be written within the same level, I entered “Yes” and got the flag for being correct.**

**level14**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. This challenge was another trivia with the same 4 levels in a MAC system: TS, S, C, and USC (with TS being the most sensitive/powerful). However, I had to answer 5 questions correctly within 120 seconds. The first question was if a subject with level S can read an Object within level S. I entered “Yes” because it was within the same class. The next question was if a subject with level UC (lower) can read an object with level C (higher). I put “No” because it would raise security issues. The third question was if a subject with level US (lower) can read an object with level TS (higher). I entered “No” again for the same reason. The fourth question was if a subject with level UC (lower) can write to an object with level C (higher). In this case, the answer is Yes. Finally, the last question asked if a Subject with level S can write an object with level S, which the answer is also Yes. After this, I got the flag.**

**level15**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. This challenge was another trivia with the same levels, but it also incorporated the use of 4 categories (NUC, UFO, NATO, ACE). In short, these categories place extra restrictions as it becomes necessary for levels to also be in the same categories to perform read/write actions. The question was if a subject with level TS and categories {NUC, UFO} can read an object of the same level and categories. The answer is Yes because it is within the same level and category, and I got the flag.**

**level16**

**A screenshot of a computer

Description automatically generated**

**To obtain the flag, I opened the terminal and started the challenge. This challenge is another trivia regarding the 4 levels of MAC and the 4 categories. The first question asked if a subject with level C and no categories can write an object with the same level and categories {ACE, NATO}. Because it is within the same level, the answer is yes. The next question asked if a subject with level TS and categories {UFO, NUC, NATO} can read an object with the same level and categories {UFO, NATO}. Because it is within the same level and both share the UFO and NATO, the answer is also yes. After that, I was asked if a subject with level S and category {UFO} can read an object with the same level and category {NUC}. Because reading abilities require subjects to be in the same categories with objects, the answer for this is no. Then, I was asked if a subject with level TS (higher) and categories {ACE, UFO, NUC} can read an object with level UC (lower) and category {NUC, NATO}. Although TS is higher than UC, they do not share all categories, so the answer is no. Finally, the last question asked if a subject with level TS (higher) and category {UFO} can read an object with the same level and all categories. The answer for this question was no, and I got the flag.**