14-741/18631: Homework 3

Due: Thursday, March 18, 2021 (by 10:39am Eastern)

Name:

Andrew ID:

Total (100 pts max):

Guidelines (Please read before starting!)

- Be neat and concise in your explanations.
- You must use at most one page for your explanation for each Problem (code you wrote may be on additional pages). Start each problem on a new page. You will need to map the sections of your PDF to problems in Gradescope.
- To access the CTF problems, create the SSH proxy as per the guide on Canvas.
- For CTF problems, **you must use the following format in your explanation**:
  - CTF Username
  - Flag
  - Explain the vulnerability in the program, and explain conceptually how that vulnerability can be exploited to get the flag.
  - How did you exploit the vulnerability? List the steps taken and the reasoning behind each step. The TA grading should be able to replicate the exploit following the steps. Feel free to make references to your code! **Note that *”use XYZ online solver”* is not sufficient - you must explain how the online solver derived the answer for full credit.**
  - Append your source code in the same writeup. Your source code should be readable from the writeup PDF itself. Note that this does not count towards the page count above.

  Omitting any of the above sections would result in points being deducted.
- Some questions are marked as **Team work**. For those, you will be asked to come up with a joint write up/solution. Only one needs to put the solution in the write up, and the other simply write ”*see [teammate andrewid]*”. However, individual CTF username and flag still need to be put in the write up for CTF questions. This only applies to questions marked as ”Team work”.
- It is highly recommended that you use Python for your assignment. You may use other languages that you are familiar with, but the teaching team will not be able to support or debug language specific errors.
- Please check your English. You won’t be penalized for using incorrect grammar, but you will get penalized if we can’t understand what you are writing.
- Proofs (including mathematical proofs) get full credit. Statements without proof or argumentation get no credit.
- There is an old saying from one of my math teachers in college: “In math, anything partially right is totally wrong.” While we are not as loathe to give partial credit, please check your derivations.

- Write a report using your favorite editor. Note that **only PDF submissions will be graded.**
- Submit to Gradescope a PDF file containing your explanations and your code files before 10:39am Eastern Standard Time on the due date. You can find the timing for EST here: `https://time.is/EST`. Late submissions incur penalties as described on the syllabus (first you use up grace credits, then you lose points).
- If you choose to use a late day, you do not have to inform the instructors. We will calculate the number of late days used at the end of the semester based on the time of submission on Gradescope.
- Post any clarifications or questions regarding this homework to Piazza.
- **Team work** As a team, beyond designated team questions, you are encouraged to shared resources (e.g., TA's help, online resources you found helpful); you are encourages to set up virtual study sessions with your teammate(s) to check each other's progress and discuss homework assignment solutions.
- **This is not a group assignment. Beyond your teammate, feel free to discuss the assignment in general terms with other people, but the answers must be your own.** Our academic integrity policy strictly follows the current INI Student Handbook `http://www.ini.cmu.edu/current_students/handbook/`, section IV-C.
- Good luck!

Access Control

University C's instructors of class X decide to set up the assignment submission system using the file system of X. LJ and HH are instructors, Alice and Bob are TAs, and ST$_1$, .., ST$_n$ are n students enrolled in this class. Files of interest include assignment handouts, submitted assignments, and grade reports. The desired access control policies are as follows.

1. Only instructors and TAs are allowed to write to the assignment handouts.
2. All instructors, TAs, and students can read the assignment handouts.
3. Instructors and TAs can read students' assignment submissions.
4. A student can read his or her own assignment submissions, but not other students' submissions.
5. A student can write (modify) his or her own assignment submissions, but not other students' assignment submissions.
6. Instructors and TAs are not allowed to write to students' assignment submissions.
7. Instructors can read and write the grade reports.
8. TAs can read the grade reports, but not write any grade reports.
9. A student is allowed to read his or her own grade report, but not other students' grade reports.
10. A student is not allowed to write any grade reports.
11. During the semester, a TA can be fired. If that happens, the TA user account will be removed from the TA group and lose any permissions when accessing the file system.

Your task is to implement this submission system according to above policies using ACL under x64 Ubuntu 18.04 (in your own VM or Docker image). For simplification, we assume that there are only 2 students in class. You need to submit both an archive and a write-up (*missing write-up will result in a 0 score*). The following paragraphs specify the requirements of the two submissions.

In your ACL submission, please submit a "HW3.tar" file, which is an archive that satisfies the following folder structure (please do not create any files inside the folders):

```
HW3.tar
└─assignments/
   ├─handouts/
   ├─submissions/
   │  ├─st1/
   │  └─st2/
   └─grade_reports/
      ├─st1/
      └─st2/
```

Please use the `uid`, `gid`, *and the name* given below to create your users and groups, and setup permissions for each folder. The name you use when creating users and groups *will affect* grading.

```
group: instructors (gid: 20001)
├─user: lj (uid: 10001)
└─user: hh (uid: 10002)
group: tas (gid: 21001)
├─user: alice (uid: 11001)
└─user: bob (uid: 11002)
```

```
group:  students (gid:  22001)
 └─user:  st1 (uid:  12001)
 └─user:  st2 (uid:  12002)
```

In your write-up submission, please in detail describe how you setup the permissions (can be in code) and explain your design.

Hint1 Directly using `tar` to archive files and folders will discard permission information, you need arguments to preserve both Unix and ACL permissions.

Hint2 When giving a user/group the read/write permission on a folder, you also want to give execute permission, so that shell utils can access the folder.