14-741/18-631: Homework 7

All sections Due: Tuesday November 30, 2021 by 10:00am EST

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 **Optional Team Work**. For those, you can work with another student. The maximum team size is 2. In your write up, please write "completed as a team" for the designated team work problem, followed by the andrew ids of you and your teammate. **Individual CTF username and flag need to be put in the write up for CTF questions.** Please refer to the problem write up for requirements of whether to submit individual or one joint write up (this may defer from problem to problem).
- **References:** List resources outside of class material that helped you solve a problem. This includes online video tutorials, other CTF problems on other platforms, etc. Remember that source code available online (e.g. stackoverflow) also needs to be cited. A quick guide on citing source code can be found here: `https://integrity.mit.edu/handbook/writing-code`. **Omitting the references section may result in an Academic Integrity Violation(s).**

- 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 10:00am 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 any late days, 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.

- **General allowed team work** Beyond designated team questions, you are encouraged to shared resources (e.g., TA's help, online resources you found helpful); you are encouraged 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!

Using Tor

Install Tor on your machine. Download instructions are available from `https://www.torproject.org/download/`. Do **not** configure your Tor machine as a server (relay).

This exercise will make use of the Stem library (`https://stem.torproject.org/`), a Python library that allows you to directly talk to the Tor controller. If you do not have any familiarity with Python, relax: it is really an easy language to pick up, nothing in this problem requires very advanced programming skills in Python, and there are tons of online resources to help, such as the Python tutorial `https://docs.python.org/3/tutorial/`. You'll find the PycURL library of use.

Note: For students not based in US or Europe, using Tor might not be the fully in compliance with the local regulations. If you do have any concerns, make a private post on Piazza and we can make alternative arrangements.

1 Preliminaries

1. (20 pts) (Before starting Tor) What is your public IP address? Show the output of a `whois` query on that address. Google how to do this.

2. (20 pts) **Team Work. Feel free to discuss homework with your teammates. Please send in your own write up.** Provide a Python script that, using the Stem library, displays:

   (a) A list of all Tor circuits your machine currently uses, as specified by the list of three Tor relays. An entry should look like "entry node–middle node–exit node."

   (b) For each circuit:

   - The IP address of each relay in the circuit
   - The location (country) of each relay
   - The current bandwidth of each relay

   Provide both your python script **and** its output.

2 Using exits to circumvent censorship

IMPORTANT: YOU MUST INCLUDE YOUR ANDREW ID (NOT YOUR CTF USERNAME) IN ALL OF YOUR HTTP REQUESTS *AND* IN YOUR WRITEUP IN ORDER TO GET FULL POINTS

1. (20 pts) Try to connect to `http://ini741website.anishs.net:14741/flag?id=ANDREWID` If you connect directly, you will likely to get 403 error. To circumvent this "block," you will attempt to force the use of specific exit nodes. Write a Stem script to constrain Tor to specific exits in different countries. Provide your Python/Stem script in your handout. What is the flag that you get from the site (no need to submit to the CTF server)?

2. (20 pts) Use your script to find as many countries as possible (at least, five) in which the website `http://ini741website.anishs.net:14741/flag?id=ANDREWID` is *not* blocked. Provide a list of these countries, the IP address of the exit node that you used, as well as the exact date/time at which you made each request verifying that each of these countries was not blocked.

3. (20 pts) You could also access the blocked site using a VPN. VPN also encrypts traffic and provides some level of anonymity. Explain why one would prefer Tor over VPN. Please base your explanation on security properties that users aim to achieve and/or TCB of the system to achieve those properties.

   Important note: We are logging all requests to the server and have reasonably good fingerprinting techniques. So, we can probably tell whether or not you are cheating on the exercise, so don't cheat! (One program per person, and don't run your program for friends). Also try to be considerate of others and do not flood the server with requests. (Attempting to hack into the server, it goes without saying, would be a major academic integrity offense, and would be treated as such). This should also act as incentive for you to start this problem early.