Labs 8-10: CTF Challenge

50.042 Foundations of Cybersecurity

November 7, 2019

1 Timeline

Hand-out: November 7
Hand-in (all are hard deadlines):

- 11:59 pm November 28 (challenge draft, ungraded, for comments only);
- 11:59 pm December 5th (finalized challenge, graded as 2 labs); all challenges will be open at 5pm of December 6th for other teams to solve.
- 11:59 pm December 12th (solutions to your peer teams' challenges, graded as 1 lab), 2019.

2 Objective

- This year, we will have a CTF as part of the 50.042 FCS class!
- This is your chance to design a security-related (more specifically, cryptography related) challenge for your classmates.
- Your objective for the next three weeks:
  - Form a team of four(4). It's ok if your team size is smaller than 4, but please be noted that grading criteria apply to all the teams (regardless of team size).
  - Get familiar with CTF challenges
  - Select a topic to work on for your challenge
  - Prepare a first draft of your challenge and writeup (i.e. solution)

3 Familiarize yourself with CTFs

- Capture the Flag (CTF) is a special kind of information security competitions. Our CTF will be a Jeopardy-style event for students of the 50.042 FCS class.

  Jeopardy-style CTFs has a couple of questions (tasks) in range of categories. For example, Web, Forensic, Cryptography, or something else.
- `https://ctftime.org/writeups` provides writeup of CTF challenges from recent online competitions
- For general instructions on how to organize a CTF and structure challenges, see here: `https://github.com/pwning/docs/blob/master/suggestions-for-running-a-ctf.markdown`

4 General CTF setup

- Each group will prepare one challenge. The groups should not disclose those challenges to other students before the main event, and in particular not share solutions. Groups should not collaborate with external parties.
- Instructors will be the jury overseeing the event to coordinate the technical part, and arbitrate conflicts
- Detected attempts to cheat will lead to disqualifications. Decision of the jury on such matters is final.
- All challenges will be made open/available from 5 pm Friday Week 12 (December 6th) until 11:59 pm Thursday Week 13 (December 12th), during which time your fellow students will attempt to solve your group's challenge.
- Teams gain some points for every solved task
- The CTF will count towards your lab grade in 50.042 in the following way:
  - The challenge prepared by your group will be judged by the instructors on the following:
    - General idea and provided documentation
    - Novelty
    - Technical aspects
    - Fairness to other students
    - Fun
  - The scores on these categories will yield up to 8 points (i.e. equal to two labs)
  - The score will be awarded by groups
  - Your group's success in solving the other group's challenges will count towards another 4 points (equal to one exercise). For each solved challenge, you will receive 0.5 points (max 4)

5 Requirements for your CTF challenge

- You are required to design and implement a challenge for our CTF. In particular, that includes:
  - Please choose a short challenge name
  - Please provide a short (2-3 sentence) text introducing the challenge. Ideally, that will be all that is required to know to start working on the challenge. If really needed, provide a PDF with additional info.
  - The code required to pose the challenge, if needed.
  - A very brief summary of how the challenge is supposed to be solved, together with a solution program if required (for instructors only, not for your fellow students).
- Please design your challenge to be solved in about 2 hours by a group of four students
  - Judged by instructors as part of the "fairness" category

- Please prepare your challenge draft until Week 11 Thursday 11:59pm, and submit them on eDimension so that we can provide feedback asap
- You will have until Week 12 Thursday 11:59pm to polish everything, and react to our comments
- Your challenge should provide a *flag* when successfully solved. The flag should follow the format `CTF{abc}`, with `abc` a reasonably long string resistant against brute forcing (e.g., not "password").
- If you require a server/virtual machine, you can sign up with your student account to get an AWS EC2 instance. For specific cases, you can also consider use of LEET lab premises (please check and discuss with us).

6 Hand-In

- Submit the following documents:
  - Challenge draft by 11:59pm Thursday Week 11: a document/zip file with your challenge draft including the challenge description and any other necessary information/references, another document/zip file including your solution.
  - Finalized challenge by 11:59pm Thursday Week 12: a document/zip file with your finalized challenge including challenge description and any other necessary information/references, another document/zip file including your solution.
  - For each of the challenges your team has solved, please provide your solution including the flag captured and a write-up how your team has solved it. Submit by 11:59pm Thursday Week 13.
- You need to submit only once per group
- Make sure to put your group name, group member details (full name, student ID) in the submitted files.