Lab 7-9: Kopi-CTF Challenge

50.020 Security

Hand-out: March 23
Hand-in Draft: March 30, 9pm
Hand-in Final: April 6, 11am
Challenges online: April 6, 6pm- April 9, 9pm

1 Objective

- This year, we will have the second Kopi-CTF as part of the 50.020 Security class!
- This is your chance to design a security-related challenge for your classmates
- Your objective for the next week:
  - Get familiar with CTF challenges
  - Select a topic to work on for you challenge
  - Prepare a first draft of your challenge and writeup

2 Familiarize yourself with CTFs

- Capture the Flag (CTF) is a special kind of information security competitions. Kopi-CTF will be a Jeopardy-style event for students of the 50.020 Security class.

  Jeopardy-style CTFs has a couple of questions (tasks) in range of categories. For example, Web, Forensic, Crypto, Binary 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`

3 General setup Kopi-CTF

- 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.
- There will be a 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 available for 75 hours (from April 6 6:00 pm to April 10 9:00pm)
- Teams can then attempt to solve the challenges, and gain some points for every solved task
- Your fellow students will have one week to solve your group's challenge
- For KopiCTF, all student submitted challenges will have the same amount of points
  - We might add some additional challenges if we feel that is necessary
- We will also have a vote on the most popular challenge. Your group will receive bonus points based on their challenge's ranking in that vote.
- The vote will be an individual vote by every student, based on his/her top 3 challenges
- The group with overall most points wins!
- The top three team will be awarded a book price donated by Citibank
- The Kopi-CTF will also count towards your exercise grade in 50.020 in the following way:
  - The challenge prepared by your group will be judged by us 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 exercises)
  - 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 one point (max 4)

4 Requirements for your Kopi-CTF challenge

- You are required to design and implement a challenge for our Kopi-CTF. In particular, that includes:
  - Please select an appropriate category for you challenge, e.g. "reverse engineering", "crypto", "exploit", "forensic" or similar
  - 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, e.g. source code for a buffer overflow binary, or similar

  - A very brief summary of how the challenge is supposed to be solved, together with a solution program if required (for us).

- Please design you challenge to be solved in about 1-2 hours by a group of good students
  - Judged by us as part of the "fairness" category
- Please prepare early drafts of all three until March 30, and submit them on eDimension so that we can provide feedback asap
- You will have until April 6 11am afterwards to polish everything, and react to our comments
- Your challenge should provide a *flag* when successfully solved. The flag should follow the format `kopiCTF{abc}`, with `abc` a reasonably long string resistant against brute forcing (e.g., not "password").
- For the third week, we will provide an infrastructure that allows groups to get the description of all challenges, submit their flags for points, and see the current leaderboard
- If you require a server/virtual machine, we can provide you one (or more) in the LEETlab or as EC2 instance

5 Hand-In

- Submit a document/zip file with draft of the challenge, the challenge description, and the solution
- You need to submit only once per group
- Make sure to put your usernames/group name prominently in the submitted files.