

CSSE 490

Network Security

Sunday, March 6, 2022

Today's Goals

- Introductions
- Logistics
- Grading
- Projects
- Course Overview
- Network security

About Me

□ Mohammad

- Dr. Noureddine if you want to make me feel old



Education

Education

- BE in Computer Engineering from AUB
- ME in Electrical Engineering from AUB
- PhD in Computer Science from UIUC



Research

- Network security
- Programmable networking



Interests and Hobbies

- Basketball 😞
- Music
 - Listening and playing
- Reading
 - Philosophy
 - Mythology
- Coffee



About you?

- ❑ Name and Major
- ❑ At least one hobby or interest in life
- ❑ Favorite book or movie
- ❑ One cool thing you did over break
 - Cannot say “played video games”
 - Must specify which games

Course Logistics

- ❑ Course website:
<https://rhit-csse490-netsec.github.io/netsec-public/>
- ❑ Keep a close eye on the schedule page
<https://rhit-csse490-netsec.github.io/netsec-public/schedule/>
- ❑ Submission of labs via Gradescope
<https://www.gradescope.com/courses/375534>

Prerequisites

- General familiarity with data structures (CSSE230)
- Coding in Python
- Coding in C (to some extent)
- A lot of shell and terminal management
- Reading?
- Writing?

Course Format

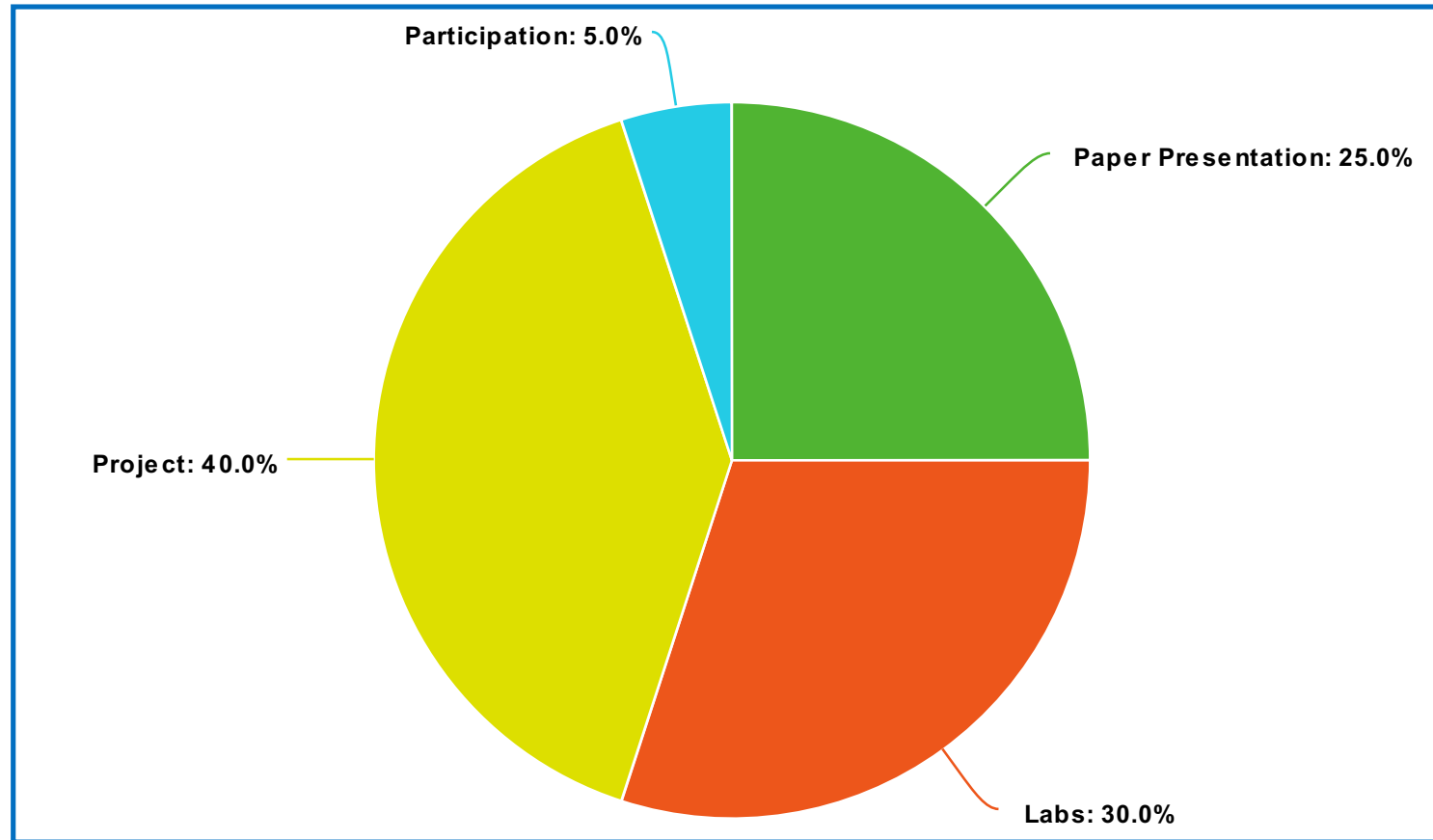
□ First five weeks

- 1-3 lectures per week
- 1-2 lab sessions per week

□ Second five weeks

- 1-2 paper presentations
- 0-1 lab sessions
- 1-2 lectures

Grading policy



■ Paper Presentation ■ Labs ■ Project ■ Participation

Participation

- Not a spectator sport
- Participate in class
- Ask questions
- Come to office hours
- Must know who you are by the end of the quarter

Presentation

- ❑ Pick a paper from a recent top conference
 - Will post a list of top conferences
- ❑ Prepare a presentation about the paper
- ❑ 25 minutes for presentation
- ❑ 5 minutes for questions
- ❑ Peer feedback for presentations

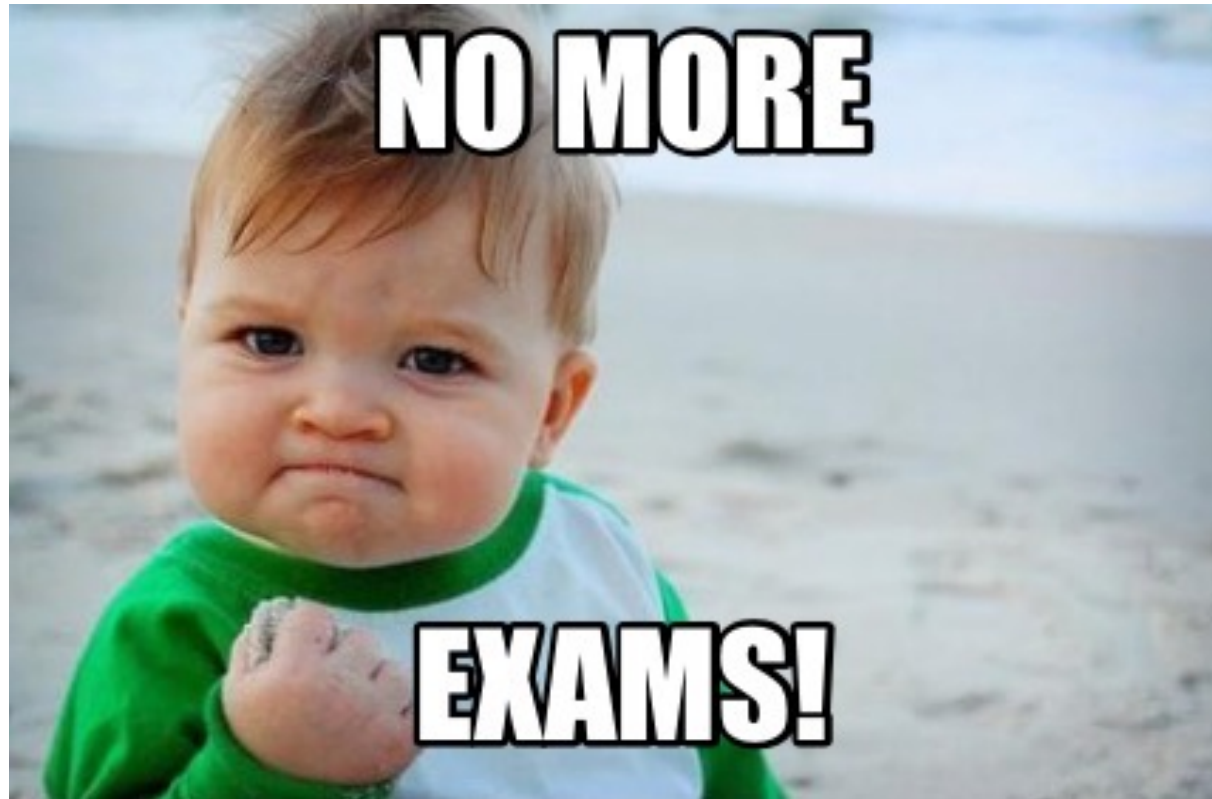
Labs

- ❑ ~1 lab per week
- ❑ Calibrated based on your feedback
- ❑ Implementing network attacks/defenses
- ❑ Using the **DETER testbed**

Project

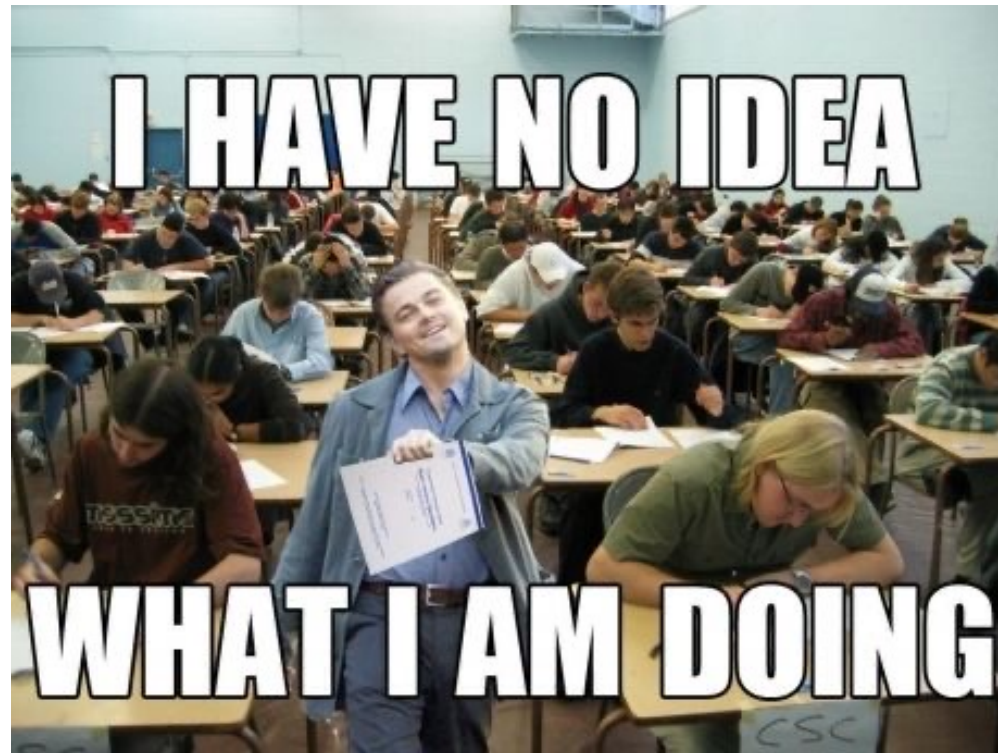
- ❑ Open-ended project
- ❑ Pick your own network security topics
 - Yes you can do machine learning stuff
- ❑ Perform a literature review
- ❑ Develop a hypothesis
- ❑ Test the hypothesis

No Exams



Help Wanted

- ❑ Building it from scratch
- ❑ Will solicit **A LOT** of feedback



What is a Network?

What is Security?

The CIA Triad

❑ Confidentiality

❑ Integrity

❑ Availability



Why Study Network Security?

What Network Security is NOT?

- Buffer overflow attacks
- XSS scripting
- SQL injection
- Spectre and Meltdown
- Password cracking
- CSSE 340