CSP 544

System and Network Security

Course philosophy

- You will “learn by doing”
- You will study security fundamentals **and implement** real attacks
- You will apply what you’ve learned

Logistics

- ***Heavily*** lab-oriented
- We will lecture for a short period at the beginning of most classes
- Then lab time! We (and TA) will be around to help

Logistics (cont)

- Labs + reports in class (and outside)
- No homeworks
- Readings
- One (final exam)

Grading Breakdown

- Again, emphasis placed on labs and learning by doing!

- 70% Labs + reports, 20% participation, 10% Final Exam

- Internet/India: 80% Labs+reports, 20% Final exam

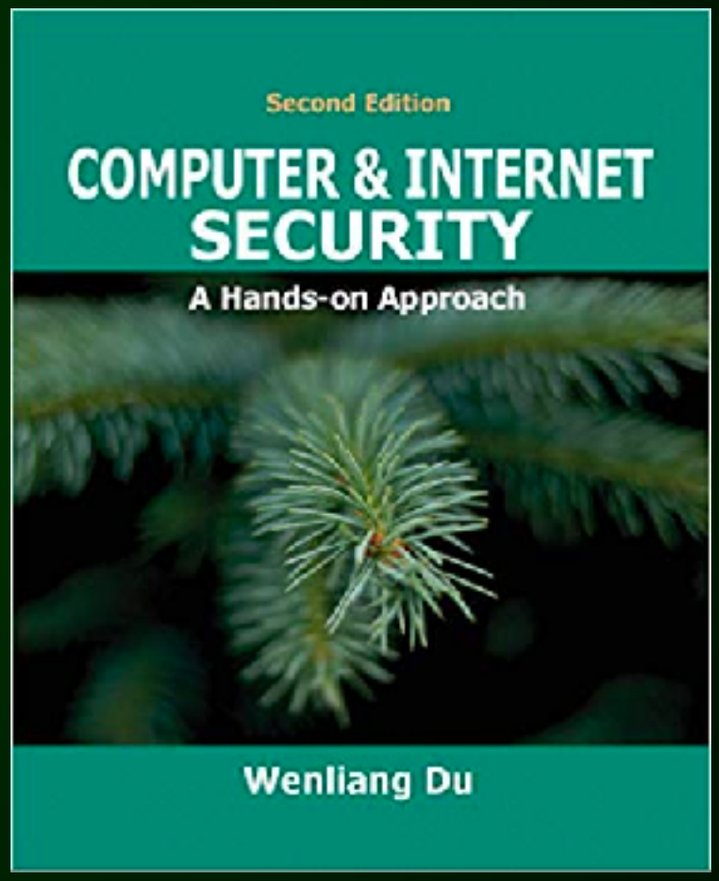
CTFs

- We will (hopefully) be participating in a team CTF (Capture the Flag) competition near the end of the course

- We encourage you to practice on your own (we'll talk more about this)

Book

- Books is required
- Other recommended books listed on course webpage



Labs

- *Most* labs are from SEED
- Some (5) are developed by Hale
- A few will be optional

Your instructors

- Kyle: First half (software & system security)
- Lan: Second half (web & network security)
- Lan’s office hours decided later

At a glance

- Software Security
- System Security (especially OS, system software)
- Web Security
- Network Security
- Crypto (very little)
- Tools of the Trade

We Want to Shift Your *Mindset*

- You after your prior classes: “software is something I build to serve a certain purpose”
- Hopefully you after this class: “software is something that can be *manipulated* to achieve certain purposes”

Why is this useful?

- Security is important (duh)
- Put you in a mindset to build more secure software
- Common preemptive defense is offense “red teaming” - very lucrative
- Apply knowledge from other courses
- Skills are in demand broadly, including research

Why are the labs useful?

- Many of the vulnerabilities are dated, have been patched. What's the point?

- We give you a *flavor* of the kind of knowledge & work that goes into developing/deploying exploits

- Broadly applicable *techniques*

Warnings

- Do not abuse what you learn
- Hacking into unauthorized systems and into unauthorized accounts is almost always illegal and unethical!

Your Day 1 TODOs

- **Lab**: SEED Lab Setup
- **Reading**: daily phrack
- Make an account on HackTheBox
- Join the course discord channel (see course website)