Introduction

Insu Yun

Welcome to IS517: Information Security Laboratory!

- Lecture & Hands-on laboratory
  - Learn high level concepts for software attacks
  - Practice attacks with exercises

Goal: Learn how hackers attack software vulnerabilities!

One important note

- If you already took EE517, you cannot take this course
  - This will be held with the same materials with EE517
  - We hope that we can cross-listt this course with EE517

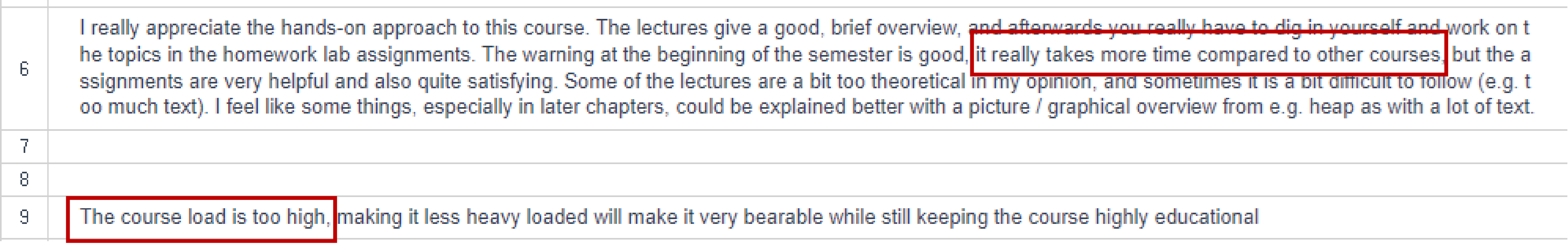
Who should take this course?

- If you are already familiar with this topic (e.g., CTF players)
  -> **Take another interesting course!** Your time is gold!

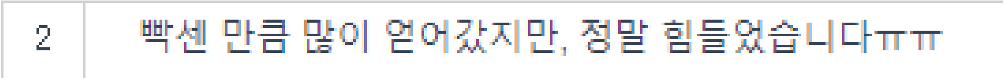
- If you want to study this topic seriously (e.g., research or job)
  -> You **SHOULD** take this!

- If you are interested in this topic + you have enough free time
  -> Good to take! It would be fun!

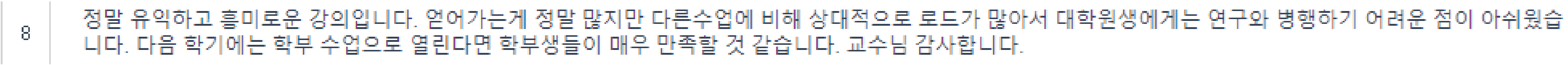
- If you are interested in this topic + your schedule is tight
  -> Think carefully!
  This would be **one of the toughest courses** in your life!



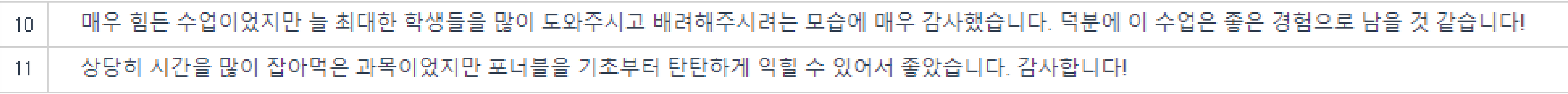
6	I really appreciate the hands-on approach to this course. The lectures give a good, brief overview, and afterwards you really have to dig in yourself and work on the topics in the homework lab assignments. The warning at the beginning of the semester is good, it really takes more time compared to other courses, but the assignments are very helpful and also quite satisfying. Some of the lectures are a bit too theoretical in my opinion, and sometimes it is a bit difficult to follow (e.g. too much text). I feel like some things, especially in later chapters, could be explained better with a picture / graphical overview from e.g. heap as with a lot of text.
7	
8	
9	The course load is too high, making it less heavy loaded will make it very bearable while still keeping the course highly educational



2	빡센 만큼 많이 얻어갔지만, 정말 힘들었습니다ㅠㅠ



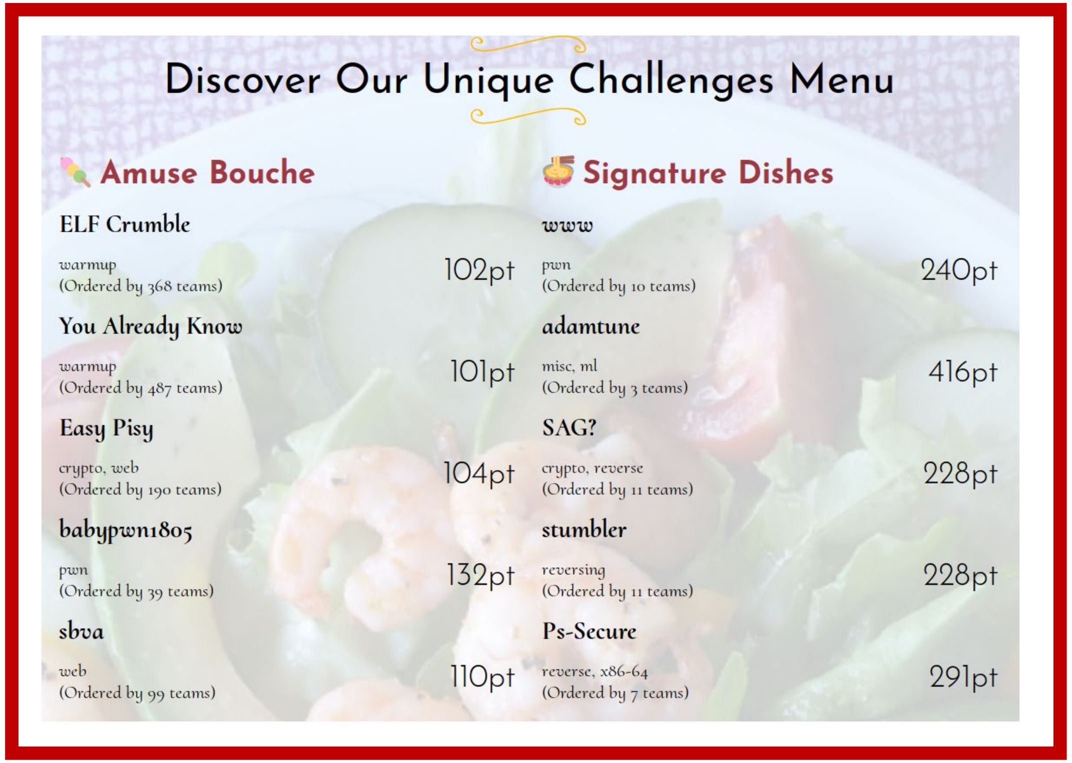
8	정말 유익하고 흥미로운 강의입니다. 얻어가는게 정말 많지만 다른수업에 비해 상대적으로 로드가 많아서 대학원생에게는 연구와 병행하기 어려운 점이 아쉬웠습니다. 다음 학기에는 학부 수업으로 열린다면 학부생들이 매우 만족할 것 같습니다. 교수님 감사합니다.



10	매우 힘든 수업이었지만 늘 최대한 학생들을 많이 도와주시고 배려해주시려는 모습에 매우 감사했습니다. 덕분에 이 수업은 좋은 경험으로 남을 것 같습니다!
11	상당히 시간을 많이 잡아먹은 과목이었지만 포너블을 기초부터 탄탄하게 익힐 수 있어서 좋았습니다. 감사합니다!

Through Capture The Flag(CTF)

- Cyber game like puzzle solving
- Types: Jeopardy, Attack and defense



Discover Our Unique Challenges Menu

Amuse Bouche

ELF Crumble
warmup
(Ordered by 368 teams)
102pt

You Already Know
warmup
(Ordered by 487 teams)
101pt

Easy Pisy
crypto, web
(Ordered by 190 teams)
104pt

babypwn1805
pwn
(Ordered by 39 teams)
132pt

sbva
web
(Ordered by 99 teams)
110pt

Signature Dishes

www
pwn
(Ordered by 10 teams)
240pt

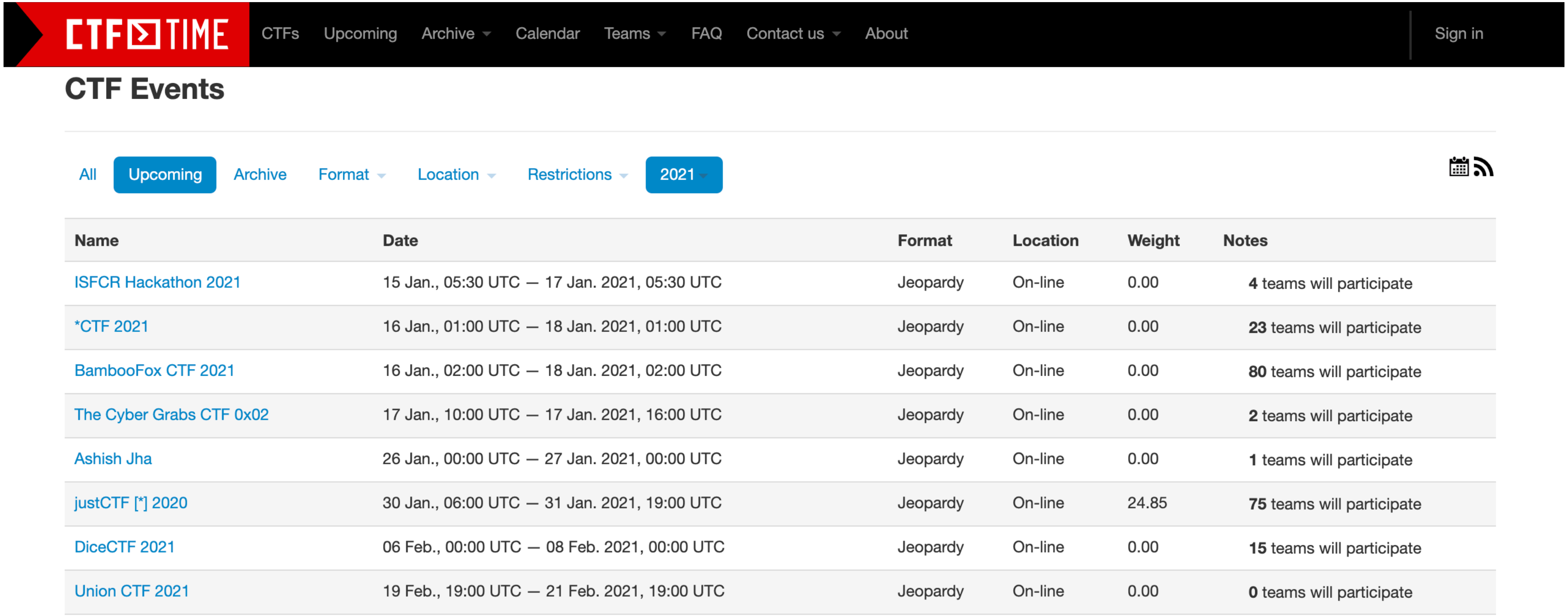
adamtune
misc, ml
(Ordered by 3 teams)
416pt

SAG?
crypto, reverse
(Ordered by 11 teams)
228pt

stumbler
reversing
(Ordered by 11 teams)
228pt

Ps-Secure
reverse, x86-64
(Ordered by 7 teams)
291pt

Many people are already enjoying CTF!



CTF Events

Name	Date	Format	Location	Weight	Notes
ISFCR Hackathon 2021	15 Jan., 05:30 UTC — 17 Jan. 2021, 05:30 UTC	Jeopardy	On-line	0.00	**4** teams will participate
*CTF 2021	16 Jan., 01:00 UTC — 18 Jan. 2021, 01:00 UTC	Jeopardy	On-line	0.00	**23** teams will participate
BambooFox CTF 2021	16 Jan., 02:00 UTC — 18 Jan. 2021, 02:00 UTC	Jeopardy	On-line	0.00	**80** teams will participate
The Cyber Grabs CTF 0x02	17 Jan., 10:00 UTC — 17 Jan. 2021, 16:00 UTC	Jeopardy	On-line	0.00	**2** teams will participate
Ashish Jha	26 Jan., 00:00 UTC — 27 Jan. 2021, 00:00 UTC	Jeopardy	On-line	0.00	**1** teams will participate
justCTF [*] 2020	30 Jan., 06:00 UTC — 31 Jan. 2021, 19:00 UTC	Jeopardy	On-line	24.85	**75** teams will participate
DiceCTF 2021	06 Feb., 00:00 UTC — 08 Feb. 2021, 00:00 UTC	Jeopardy	On-line	0.00	**15** teams will participate
Union CTF 2021	19 Feb., 19:00 UTC — 21 Feb. 2021, 19:00 UTC	Jeopardy	On-line	0.00	**0** teams will participate

ref: ctftime.org

I am also one of them (from DEFCON CTF)

ME ☺

Instructor / TA

- Instructor: Insu Yun
- TA
  - Donguk Kim (Head TA)
  - Donghyeon Kim

Prerequisite

- (Strict) EE209 or other equivalent courses (e.g., CS230)
- (Recommended) Operating system, system programming, architecture

- Required skills: C, Python, C++

Lecture: In hybrid

- Offline: N1 #112
- Online: https://kaist.zoom.us/j/87076283602?pwd=mM8UTxM73EmbfwDzuipE6Pzb4dguN5.1
  - For someone who cannot participate offline

General information

- Homepage: https://teemo.kaist.ac.kr/is517/2024/
- Piazza: https://piazza.com/kaist.ac.kr/fall2024/is517
  - Register now. For announcements. No KLMS.
- Youtube: https://www.youtube.com/playlist?list=PLpYYZoHf-Y99YxB4tTFUrmkmMbbt2GHXO
- Email: kaist-is512@googlegroups.com
  - Don’t use my or TA’s personal mail for this course

Office hour

- Me: Friday 10:00 AM (N1 819)
- TA: Thursday 3:00 PM (N1 812)

- I strongly recommend you to join office hour!
  - Concept != Reality
  - We will help you to tackle obstacles in reality (e.g., debugging)

Topics

- Lab01: Reverse engineering
- Lab02: Linux basic + shellcode
- Lab03: Stack overflow
- Lab04: Bypassing stack protection
- Lab05: Bypassing DEP/ASLR
- Lab06: Return-oriented programming
- Lab07: Remote exploits
- Lab08: Miscellaneous attacks
- Lab09: Heap exploits

> 10 challenges per lab

→ In total, you will solve 100 challenges in a semester

Three types of lectures

1. General lecture
   - Explain concepts of each topic
   - Slides (+ video) will be uploaded in the website
2. Tutorial
   - Go through the tutorial (~ 30minutes)
   - Bring your labtop, do yourself, and ask questions
   - Materials and videos will be available
3. Lab review
   - At the day of deadline, I will briefly show you how to approach the challenge
   - **Slides and videos will not be uploaded (Only live!)**

Grading rule: Overview

- We have two grading rules: Regular + Catch up
- Your grade = MAX(Grade $_{\text{Regular}}$, Grade $_{\text{Catch up}}$)

- It will be a little bit complicated. But this is for you!

Grading rule: Regular

- Goal: Grade that you are doing well in general

- Attendance (10%)
- Lab assignments (40%)
- In-class CTF (50%)
  - Problem writing (10%)
  - Solving challenges (40%)

Lab assignments

- For each challenge
  - Submit a flag with corresponding writeup
  - Total: 220 points = 200 points (10 challenges) + 20 point (one tutorial)

- Late policy: 50% of original score (one extra week)

- If you solve 6 challenges in each lab (except tutorial), you will get the full score for that lab.
  - i.e., Solving more than 6 challenges would not have any impact in general grading!

In-class CTF

- For 7 hours (9am – 4pm), instead of final exam!
  - 6 hours: Solving challenges
  - 1 hour: Presentation for challenges

- **12/21 (Sat) 9am – 4pm!**
- Solo play for solving, Team play for writing

- Your tasks
  - Make a challenge for other students (if not, F)
  - Solve challenges from other students + from us

- We will share details later

Grading rule: Catch up

- Goal: Grade that you are catching up

- If your # of solved problems (except for tutorials) >= Limit
  → you'll get grade
  - B+ >= 60
  - B0 >= 55
  - B- >= 50
  - …

- Note that Grade $_{\text{Catch up}}$ can be "B+" at maximum
- Unlike general grading, it considers # regardless of lab
  - i.e., We only consider total # of solved challenges!

Tips

- Study in group (e.g., discussion)
- Get help from me and TAs (Office hour, Piazza)
    - Strongly recommend to use office hour!

- Manage your time
- Learn basic tools (e.g., gdb, pwntools, python)
- Try to tackle in order (not strict)

- Start your assignment as soon as possible
    - Don’t assume that TAs will respond immediately

Misconduct policy

- DO NOT SHARE YOUR CODE WITH OTHER STUDENTS
  - We encourage you to discuss, but discussion != sharing code
  - Do not copy other students’ code
  - Do not copy any public code

About course material

- You should ***never*** share challenges/exploits/writeups online
- Once found → F

- Reason: It makes this course less useful for other students

Ethical hacking

- DO NOT ATTACK OTHER’s SYSTEM

- Attack your own and isolated environment
  - Use your home directory
  - DO NOT DoS our server (e.g., fork bomb)

IMPORTANT: Your task

- Join piazza (No KLMS!)

- Check your final exam schedule: 12/21 (Sat) 9am – 4pm

- ~~Try to login website + lab server~~
    - ~~If you have any trouble, let us know!~~