CS437 / SEC537 Cybersecurity Practices and Applications

Dr. Orçun Çetin

Course Information

- https://sucourse.sabanciuniv.edu
  - all class materials will be uploaded to SuCourse+
  - you are responsible to check your e-mails and sucourse for announcements
- Instructor: Dr. Orçun Çetin
  - Office: FENS L015
  - E-mails: orcun.cetin@sabanciuniv.edu
  - Assistant: Yağız Yılmaz
- Lectures: Tuesday 9:40- 10:30 and
  Thursday 15:40 - 17:30

Course Information for CS 437

Tentative Grading Policy

- 30% Homework
- 20% Labs
- 50% Final exam
  - No mid-term

Course Information for SEC 537

Tentative Grading Policy

- 50% Project
  - 2 Projects (Estimation)
  - *Maybe* also few labs
- 50% Final exam
  - No mid-term

Labs

- Composed of instructions that serve as hands-on exercises on course topics.
- Students are required to submit their lab results via SuCourse +.
- New programming languages might be also taught to prepare you for the labs or the assignment / homework!

Ethics and Cheating

- Plagiarism is not tolerated, homeworks are to be done personally
  - Unless, you are told otherwise!
- ***Cooperation is not an excuse;***
  - ***if you do not know how to cooperate, don't do it.***
- Students are assumed to agree that they will not use the knowledge they gain in this class to ***perform cybercrime!!!***.

Linux Virtual Machine

- During the class, we will need a Linux virtual machine to replicate what you learn in the classroom
  - For that reason
    - I advise you to get a Linux Virtual machine
      - Options:
        - Ubuntu
        - Kali

Tentative Syllabus

-Introduction and general terminology
-> Classification of Attacks
-> Cyber Threats
-> Vulnerabilities and misconfigurations
-> Human Issues
-> Basic security components
-Phishing and social engineering
-Introduction to Linux
-Basic Security Testing with Linux
->Introduction to Red Team Tools
->Reconnaissance attempts
->Initial Access
->Persistence
-Application and web security
->Command Injections
-> Memory Injections
->Script Injection
-Secure software development lifecycle
-> Threat Modeling

Tentative Syllabus (If we have time)

Maybe also ?

Analysing malicious PDF analysis
Honeypots
IDS
DNS Amplification Attacks
IoT Security
Yara Signatures
Common smart city security issues
And more …..