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 14:40- 15:30 and
  Thursday 14:40 - 16:30

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 machines to replicate what you learn in the classroom
  - For that reason
    - I advise you to get a Linux Virtual (Kali & Ubuntu) machine
      - Local (Kali)
        - VirtualBox, Parallels (paid) veya VMware Fusion
          -
      - Remote(Ubuntu)
        - Free options
          - Digital Ocean, Google Cloud or Alibaba
        - Paid options
          - Vultr and others

Tentative Syllabus

-Introduction and general terminology
-> Classification of Attacks
-> Cyber Threats
-> Vulnerabilities and misconfigurations
-> Human Issues / End user awareness
-> 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
-Honeypots design and development

Last year :
-Introduction to Cybersecurity
-Introduction to Linux
-OWASP TOP 10 and Programming Best Practices
-Some Command Injections
-Code Review and Static Analysis
-Identifying Design Flaws of Honeypots
-Secure Software Development
-Proven Best Practices for Resilient Applications
-Typical Memory Injection
-Penetration Testing (Kali & Web vulnerabilities)
-Penetration Testing (Active Directory)
-Penetration Testing (Databases)
-Penetration Testing (Information gathering)

Tentative Syllabus (If we have time)

Maybe also ?

->API Security
->Linux and Windows forensics
->Licensed Penetration Tester (LPT) material

And even more if we have time…..

Analysing malicious PDF analysis
IDS
DDoS attacks
IoT Security
Yara Signatures
Common smart city security issues
And more …..