CS 437 / SEC 537 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-mail: orcun.cetin@sabanciuniv.edu

Course Information

- Assistant: Batuhan Kertmen
  - E-mail: batuhankertmen@sabanciuniv.edu
  - Please direct all course-related inquiries to this contact.
- Lectures:
  - Tuesday 14:40 - 15:30
  - 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

- 45% Project
  - 2 Projects (Estimation)
- 45% Final exam
  - No mid-term
- 10% Labs

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!
- Reports consist of only screenshots are not allowed
  - Each screenshot must be explained

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) machine
      - Local (Kali)
        - VirtualBox, Parallels (paid) veya VMware Fusion
          -
      - Remote(Ubuntu)
        - Free options
          - Digital Ocean, Google Cloud or Alibaba
        - Paid options
          - Vultr and others

Previous Syllabus

2022:

-Introduction to Cybersecurity
-Introduction to Linux
-Identifying Design Flaws of Honeypots
-OWASP TOP 10 and Programming Best Practices
-Some Command Injections
-Secure Software Development
-Proven Best Practices for Resilient Applications
-API Security
-Pentesting: Web-Based API Security
-Pentesting: API testing
-Pentesting: Burp Suite
-Typical Memory Injection
-C vulnerabilities
-YARA & Basic Static Malicious Documents Analysis

2021:

-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

2023:

Introduction to Cybersecurity
Introduction to Linux
Identifying Design Flaws of Honeypots
OWASP TOP 10 and Programming Best Practices
Some Command Injections
Secure Software Development (Waterfall)
Proven Best Practices for Resilient Applications
API Security
Pentesting: Web-Based API Security
Pentesting: API testing
Pentesting: Burp Suite
Typical Memory Injection
C vulnerabilities
YARA & Basic Static Malicious Documents Analysis

This year will be similar to 2024:

->Introduction to Cybersecurity
->Introduction to Linux
->Identifying Design Flaws of Honeypots
->OWASP TOP 10 and Programming Best Practices
->Some Injections Vulnerabilities
->Secure Software Development (Waterfall-DevSecOps)
->Proven Best Practices for Resilient Applications
->API Security
->Pentesting: Introduction to Penetration Testing
->Pentesting: Web-Based Security
->Pentesting: Post-exploitation
->Typical Memory Injection
->C vulnerabilities
->Introduction Operational Technology (OT) Security
->YARA & Basic Static Malicious Documents Analysis (Optional)

Tentative Syllabus (If we have time)

Maybe also ?

->Linux and Windows forensics
->More cybersecurity forensics