SEC 530
Malware Analysis and Detection
2022

Dr. Orçun Çetin
Course Information

- [https://sucourse.sabanciuniv.edu/plus/](https://sucourse.sabanciuniv.edu/plus/)
  - 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](mailto:orcun.cetin@sabanciuniv.edu)
  - Office hour: Tuesday 13.40 - 14:40
- Lectures: Tuesday 14:40 - 17:30
- Useful Books:
  - Michael Sikorski and Andrew Honig, Practical Malware Analysis Handbook
Course Information

Tentative Grading

● 40% homework
  ○ 1-2 assignments (Optional)
    ■ Typically, no group assignments
  ○ 1 project
    ■ Typically, group projects

● 20% labs

● 40% final
Labs

● Composed of instructions that serve as hands-on exercises on course topics.
  ○ most of the samples are from books and training courses.
  ○ only few samples will be real malware samples.
  ○ done under the supervision of the instructor.

● Students are required to submit their lab results via sucourse.
Exam

- No mid-term
- There will be a only one Final exam
Ethics and Cheating

- Plagiarism is not tolerated, homeworks are to be done personally
  - 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.
Tentative Syllabus

● Introduction to Malware Analysis
  ○ Classification of Malware
  ○ Environment Setup for Safe Analysis
  ○ Malware Analysis in Virtual Machines

● Basic Analysis
  ○ Basic Static analysis
  ○ Basic Dynamic analysis

● Advanced Static Analysis
  ○ Review of x86
  ○ Disassembly with IDA Pro & other tools
  ○ Recognizing C Code Constructs in Assembly
  ○ Analyzing Malicious Windows Programs

● Advanced Dynamic Analysis
  ○ Debugging with OllyDbg

● Malware Functionality
  ○ Malware Behavior
  ○ Covert Malware Launching
  ○ Data Encoding

● More hands on malware analysis practice
  ○ Analyzing Java Binaries and Malware
  ○ Analyzing .NET Malware
  ○ Malware Analysis with Ghidra