SEC 537 /CS 437 - Cybersecurity Practices and Applications

Fall 2021-2022

Description and objectives: This course provides an introduction to the exciting field of cybersecurity, cybercrime and secure software development. Topics include phishing and social engineering, introduction to Linux operating system, security testing with Linux, code and memory injection techniques and secure software development lifecycle. Basic Linux operating system knowledge and bash programming will be provided. Moreover, various scripts and testing tools will be used to assess systems for vulnerabilities and misconfigurations.

Keywords: Vulnerabilities, phishing, malware, cyberattacks, basics of Linux, security testing, buffer overflows, SQL injection, cross-site-scripting, secure software development life cycle, threat modelling, phishing, social engineering

Instructor: Orçun Çetin – orcun.cetin@sabanciuniv.edu

Tentative Outline:

-Introduction and general terminology (1 week)

-> Classification of Attacks

-> Cyber Threats

-> Vulnerabilities and misconfigurations

-> Human Issues

-> Basic security components

-Phishing and social engineering (2 weeks)

-Introduction to Linux (1 week)

-Basic Security Testing with Linux (3 weeks)

->Introduction to Red Team Tools

->Reconnaissance attempts

->Initial Access

->Persistence

-Application security (5 weeks)

_>Command Injections

-> Memory Injections

->Script Injection

-Secure software development lifecycle (2 weeks)

_> Threat Modeling

Student Responsibilities

Students are required to work on *homework assignments*.

Tentative Grading Policy:

Final exam	50%
Homework	30%
Labs	20%