CS 315 Computer Security

(计算机安全)

Instructor: Fengwei Zhang

Who Am I?

- Fengwei Zhang
  - Associate Professor of Computer Science
  - Office: Room 515, South Tower, Engineering Building
  - Email: zhangfw@sustech.edu.cn
  - Website: http://cse.sustech.edu.cn/faculty/~zhangfw/

- Course Information
  - Course website: http://cse.sustech.edu.cn/faculty/~zhangfw/22fa-cs315/index.html

Why Study Security?

Why Study Security?

It’s cool to be a hacker

It’s a hot topic and media talk about it

It’s useful for finding a job

Course Overview

- This course aims help students to learn the principles of computer security and understand how various security attacks and countermeasures work
- Providing hands-on experience in playing with security software and network systems in a live laboratory environment, including Capture-the-flag
- Taking both offensive and defense methods to help student explore security tools and attacks in practice
- Focusing on attacks, hacking fundamentals, defenses.

Course Objectives

- Understanding on real-world security vulnerabilities, exploits and defenses
- Having hands-on labs in network and system security experiments
- Learning knowledge of practical security problems and their solutions

Course Labs

- Lab 1: Packet Sniffing and Wireshark
- Lab 2: Buffer Overflows and Defense
- Lab 3: Secure Coding and Format-String Vulnerability
- Lab 4: Scanning, Reconnaissance, and Penetration Testing
- Lab 5: Reverse Engineering and Obfuscation
- Lab 6: IoT Security and Wireless Exploitation

Course Labs

- Lab 7: Nailgun Attack
- Lab 8: Nailgun Defense
- Lab 9: Dirty COW Attack
- Lab 10: RSA Public-Key Encryption and Signature
- Lab 11: Web Security
- Lab 12: Return-to-libc and Return Oriented Programming

Lab Assignments

- 12 lab assignments
  - Source code
  - Write up PDF

Two Tracks

- Term Project Track (Mentor: Fengwei Zhang)
- CTF Track (Coach: Zhao Li)

Term Project Track

Topics	Grade
Class Participation	40
Lab 1: Packet Sniffing and Wireshark	60
Lab 2: Secure Coding and Buffer Overflows	60
Lab 3: Secure Coding and Format-String Vulnerability	60
Lab 4: Scanning, Reconnaissance, and Penetration Testing	60
Lab 5: Reverse Engineering and Obfuscation	60
Lab 6: IoT Security and Wireless Exploitation	60
Lab 7: Nailgun Attack	60
Lab 8: Nailgun Defense	60
Lab 9: Dirty COW Attack	60
Lab 10: RSA Public-Key Encryption and Signature	60
Lab 11: Web Security	60
Lab 12: Return-to-libc & Return Oriented Programming	60
Term Project Proposal	60
Term Project Presentation	80
Term Project Report	100
Total	1000

CTF Track

Topics	Grade
Class Participation	40
Lab 1: Packet Sniffing and Wireshark	60+10
Lab 2: Secure Coding and Buffer Overflows	60+10
Lab 3: Secure Coding and Format-String Vulnerability	60+10
Lab 4: Scanning, Reconnaissance, and Penetration Testing	60+10
Lab 5: Reverse Engineering and Obfuscation	60+10
Lab 6: IoT Security and Wireless Exploitation	60+10
Lab 7: Nailgun Attack	60+10
Lab 8: Nailgun Defense	60+10
Lab 9: Dirty COW Attack	60+10
Lab 10: RSA Public-Key Encryption and Signature	60+10
Lab 11: Web Security	60+10
Lab 12: Return-to-libc & Return Oriented Programming	60+10
Attack-Defense CTF	120
Total	1000

Course Prerequisites

- Familiar with Linux/Unix Commands
- It would be better if you know:
  - Basic C, Java, Assembly, etc.
  - Operating systems
  - Computer networks

Policies on Late Submissions

- Lab and project deadlines will be firm.
- Late homework will be accepted with a 10% reduction in grade for each day they are late by.
- Once a homework assignment is discussed in class, submissions will no longer be accepted.

Grading Scale

The grades for the course will be based upon the percentages given by the university

A+	97 - 100%	C+	77 - 79%
A	93 - 96%	C	73 - 76%
A-	90 - 92%	C-	70 - 72%
B+	87 - 89%	D+	67 - 69%
B	83 - 86%	D	63 - 66%
B-	80 - 82%	D-	60 - 62%
F	0 - 59%		

Academic Integrity

- Students need to sign the Assignment Declaration Form in your first lecture.
- Our department can refuse students to choose the CSE Major if they do not sign the declaration form.
- Please read and fill the Undergraduate Students Assignment Delcaration Form in Chinese and English. More details on Regulations.

Academic Integrity

南方科技大学 SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY | 计算机科学与工程系 Department of Computer Science and Engineering

本科生作业承诺书

本人_____（学号_____）本学期已选修计算机科学与工程系_____课程。本人已阅读并了解《南方科技大学计算机科学与工程系本科生作业抄袭学术不端行为的认定标准及处理办法》制度中关于禁止本科生作业抄袭的相关规定，并承诺自觉遵守其规定。

承诺人：

南方科技大学 SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY | 计算机科学与工程系 Department of Computer Science and Engineering

Undergraduate Students Assignment Declaration Form

This is_____(student ID:_____, who has enrolled in _____ course, originated the Department of Computer Science and Engineering. I have read and understood the regulations on plagiarism in assignments and theses according to "Regulations on Academic Misconduct in Assignments for Undergraduate Students in the SUSTech Department of Computer Science and Engineering". I promise that I will follow these regulations during the study of this course.

Signature:

Student Disabilities Services

- If you have a documented disability that requires accommodations, you will need to register with the University for coordination of your academic accommodations, and let me know.

Other Resources

- Course Website:

  http://cse.sustech.edu.cn/faculty/~zhangfw/22fa-cs315/index.html

- Instructor homepage:
  - http://cse.sustech.edu.cn/faculty/~zhangfw

Lab Session

- Lab 1: Packet Sniffing and Wireshark
  - Be prepared!

Please read and fill the Undergraduate Students Assignment Declaration Form