CMPS 485 Computer Security

Syllabus and Course Admin

Dr. Abdelkarim Erradi

Department of Computer Science & Engineering

Qatar University


بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Outline for Today

- Course introduction
- Grading
- Policies

About the Instructor

- **Dr. Abdelkarim Erradi**
  - **Office:** Office 132 Female Engineering Building
  - **Phone:** 4403 4254

Office hours:

- Female - **Thursday 10am to 11am** at my office
- Male - **Thursday 11am to 12pm** at CSE Meeting Room BCR-E104
- Other times are available **by appointment only** on Tuesday before 2pm
- You can talk to me **after** class if you have issues/questions
- **Best way to contact me is by Email** erradi@qu.edu.qa

Three Main Course Goals

1. Learn *security fundamentals*
   – Core security concepts and techniques

2. Experiment with *security tools*
   – Tools for attacks and defense

3. Apply the *security mindset*
   – A new way to think about and analyze systems

Security mindset

- The main objective of this course is to learn how to think like an adversary
- Thinking like an adversary is essential for building secure systems
- Always ask yourself
  - Who is the adversary?
  - What are the attack possibilities?
  - What are the attack impacts?
- "security involves **thinking like an attacker, an adversary or a criminal**. If you don't see the world that way, you'll never notice most security problems." - Bruce Schneier

Not Course Goals

- Learn the entire field
  - Security is broad and covers too many areas
- Legal and economic impacts
  - We'll touch on these, but not focus
- Learn to hack/crack computers
  - This is not a hacking class

Quick Note on Ethics

- We will learn attack techniques and tools in this class
- To provide good defense, you need to understand attacks
- Do not use them against computers or networks you do not have *written* permission for
  - Legal action may be pursued, be very careful

Prerequisites

- Required
  - Basic networking
  - Basic computer organization
  - Java/Python programming
- Useful
  - Linux usage
  - Operating systems
- Most Important
  - Desire to learn and experiment!

Why this Course?

- The increased **number** and **sophistication** of attacks on computing systems motivates further emphasis on security

=> This course **equips you with the skills** and best practices needed to protect computing systems from attacks

Topics	Chapter	Weeks
Basic security concepts and principles	Online readings	1
Cryptography		4
Authentication & Authorization		2
Network Security: Port scanning, Network attacks, Network defenses		3
Web Application Security		2
Ethics and Legal Issues		1
Student Presentations		1
Total		**14**

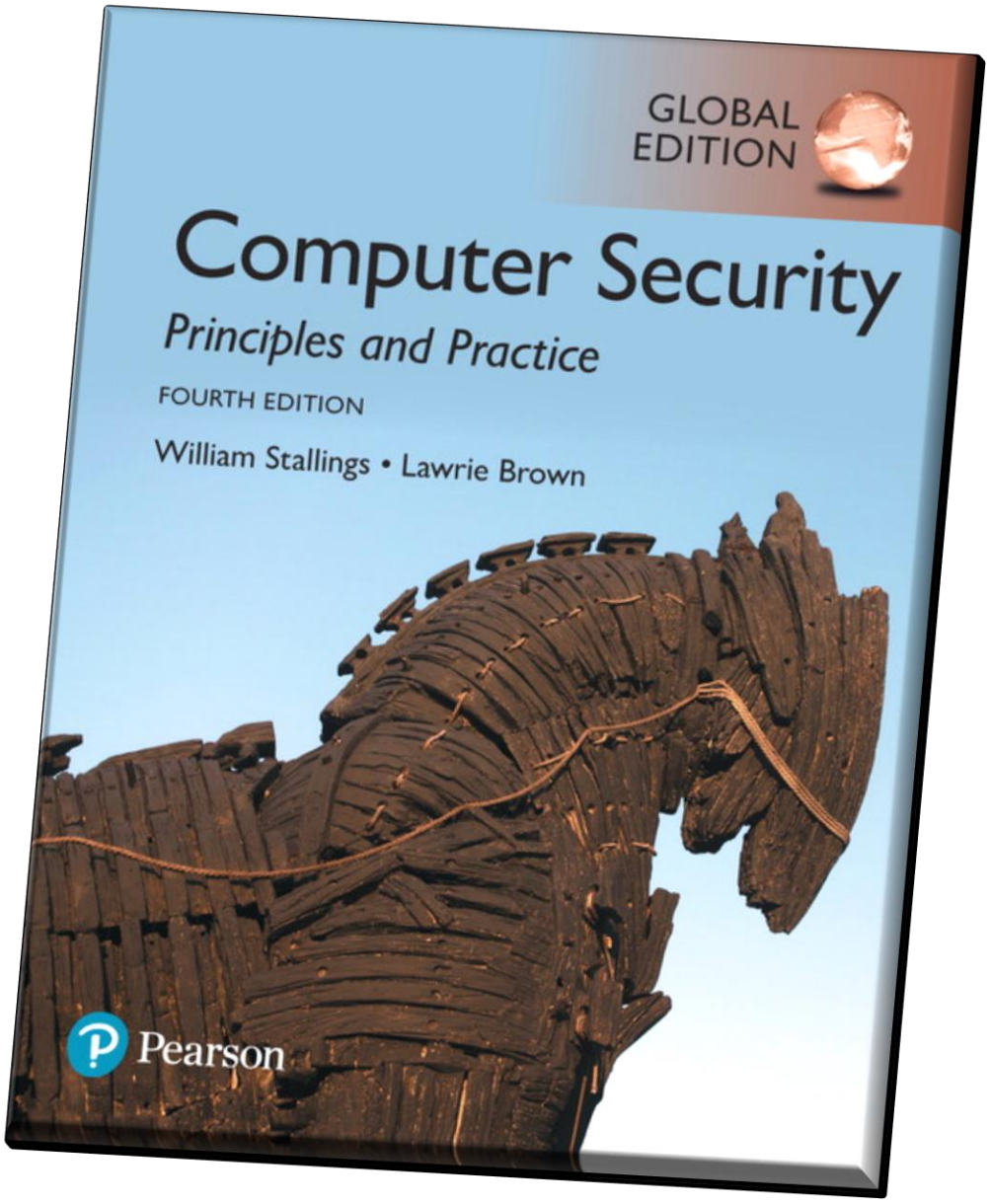
Textbook

- Recommended

William Stallings & Lawrie Brown, ***Computer Security: Principles and Practice***, 4th Edition, 2018

- Online resources

will be provided



Your Grade is Based on:

Quizzes	15%	5 Quizzes
Homework	20%	4 homework assignments
Review paper & Presentation	20%	
Midterm exam	20%	Week 7
Final exam	25%	QU Exam schedule

GitHub will be used to deliver content and assignments

Check regularly!

https://github.com/cmps485f18/cmps485-content

Lecture slides, Demos and Assignments are there!

Communications will be by email

Software we will use

- Kali Linux (Penetration Testing toolkit)
- Nmap port scanner
- aircrack-ng suite
- Wireshark
- Java or Python programming language (student choice)

How to succeed in this course….

- Do your weekly assigned readings
- **Read the slides before you come to the class**
- **Experiments with security tools that will be introduced**
- **Attend and participate in class**
  - **Many of the exam questions are from the class explanation**
- Do all the assignments **yourself.** Actively contribute to your group work.
- Do not wait till last minute to work on assignments
- Seek help when needed and ask questions (and do it EARLY): During Lectures & Come to office hours
- Have fun!

Important Notes

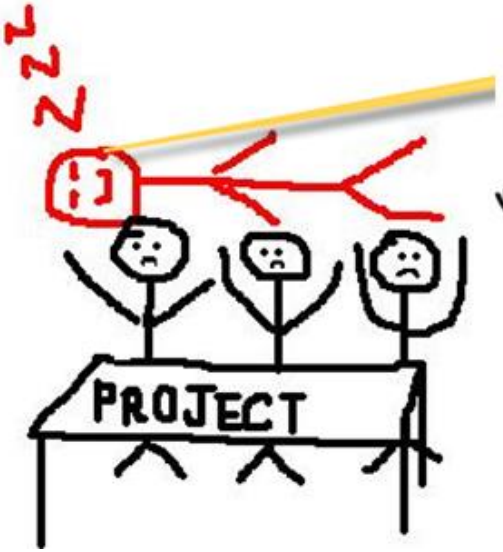
- Attendance… QU attendance policies will be enforced
  - Do not miss classes
- **Start your assignments early!!!**
- This is a senior-level course and students are expected to learn independently as much as needed in order to complete the course requirements
  - Do not expect me to find/fix your code bugs
  - Do not expect me to find and fix your technical issues
  - I can only give you high level suggestions and guidance

Plagiarism / Cheating

- “Getting an unfair academic advantage"
  - Using other people's work as your own
  - Not doing your assignments yourself
- **All submitted work should be yours!**
  - Do NOT copy from each other or from the Internet - **I will know it!**
  - Cite sources properly
  - You can be picked-up randomly to explain your implementation
- Cheating will be treated very seriously
  - Penalties START with a zero on the assignment, failing the course! and other disciplinary actions as per QU policy

No ‘Free Riding’ allowed

- ‘free riders’ (who do not contribute much to group work) => not acceptable and not fair for hardworking students
  - You must actively contribute to group work and do your ultimate best to deliver the best possible results
  - Otherwise you will be asked to do the work alone



Email Rules

- When emailing me you must add – **CMPS 485** to the beginning of the email title

e.g., CMPS 485 – Request for a meeting

- I reply to **CMPS 485** emails on Sundays, Tuesdays and Thursdays

- For **guidance** on technical issues come to office hours NOT by email

To do before next class

- Let me know your team members (StudentID and Student Name)
- Install the required software (see the email I have sent you)
- Register for GitHub and Piazza
- Read the posted content and prepare any questions you might have

I wish you a fruitful and enjoyable journey!