CSCI 345

Computer & Network Security
Spring 2020

Instructor: Xenia Mountrouidou (Dr. X)
E-Mail: mountrouidoux@cofc.edu
Phone: (843)-953-2754
Office: Harbor Walk East, Room #312
Office Hours: Tues/Thurs 10:30 – 12:30 or by appointment

Overview

This course will cover the techniques used to secure cyber systems. Topics covered will include security policies, computer security management and risk assessment, secured network protocols, software security issues, ethical and legal aspects of cybersecurity, and disaster recovery. Special emphasis will be given to designing, deploying, and managing complete secured cyber systems.

Prerequisites: CSCI 230 with C- or better grade.

Outcomes

After completing CSCI 345 students will be able to:

1. Examine the architecture of a cyber system, i.e., software, operating system, computer network, to discover vulnerabilities, evaluate and propose defense mechanisms
2. Use or develop tools for pen testing and vulnerability assessment
3. Discover different types of network intrusions based on their key features
4. Describe and evaluate the effectiveness of firewalls and VPNs
5. Develop rules for Intrusion Detection/Prevention Systems and evaluate these using statistical Receiver Operating Characteristic (ROC) curves
6. Develop a buffer overflow attack and propose defense mechanisms
7. Point out non-secure programming practices and substitute these with secure programing and input sanitizing techniques
8. Understand key concepts: HTTPS, SSL, IPSec, IEEE 802.11 wireless security and hypothesize their weaknesses.
9. Articulate laws and policies, ethical issues on cybersecurity
10. Formulate social engineering scenarios to test the preparedness of their organization
11. Compare security controls, human factors, education and training for cybersecurity

Materials

Required book:
"Security in Computing", 5th edition, Pfleeger & Pfleeger

Recommended books:
"Red Team Field Manual (RTFM)", Ben Clark
"Blue Team Field Manual: Incident Response Edition", Don Murdoch
"Blue Team Field Manual (BTFM)", Alan J. White
"Penetration Testing: A Hands-On Introduction", Georgia Weidman

Software:

1. Putty for Windows (SuperPutty recommended) or terminal for Mac OS (iTerm recommended)
2. Kali VM
3. Metasploitable VM
4. Docker / Virtual Box

Class Meeting times: Tues/Thurs
Section 01 14:10 – 15:25,
Section 02 15:35 – 16:50
Class Location: Harbor Walk East #334
My Office: Harbor Walk East, Room #312
Office hours: Tues/Thurs 10:30 – 12:30

Course Website:
http://mountrouidoux.people.cofc.edu/CSCI345/index.html

Evaluation

NCL-CTF	20%
Homework	30%
Midterm	20%
Final	30%
Total	100%

Your weighted average will result in a letter grade assigned per the usual scale: A: 93%-100% A-: 90%-93% B+: 87%-90% B: 83%-87% B-: 80%-83% C+: 77%-80% C: 73%-77% C-: 70%-73% D+: 67%-70% D: 63%-67% D-: 60%-63% F: below 60%

Note: I do not round up grades unless there is a 0.1 % difference with the next grade letter AND I have NOT offered extra credit opportunities during class

- **Exams:**
  - Exams are closed book.
  - You may bring *one cheat sheet*: a single page written front and back with your hand written or typed notes, slides, etc.
  - *The final exam is cumulative*.
- **Homework**
  - You will have 4 homework assignments (20%) and 6 lab assignments (10%) that will include coding, problem solving on systems security, administrative skills, and reports.
  - The homework will be completed in **teams of 2 students (both labs and assignments).**
- **NCL**
  - You will need to participate in a Capture The Flag (CTF) competition named the National Cyber League Spring 2020 Season.
  - **The CTF participation is *individual.***
  - You will need to participate in the pre-season (3/23 – 3/30) and regular season (4/3 – 4/5) of the competition.

Late Submissions

- Deadlines are firm.
- You may submit up to two days late with 20% penalty for each day that you are late.
- *A score of zero will be assigned to any project/homework that has not been submitted within two days after the deadline.*

Re-grading

If you have a request for re-grading, you need to ask me to re-grade your exam or homework up to one week (five business days) after this has been returned to you. *There will be no re-grading if the test/project that is older than one week.* I reserve the right to re-grade the full test/project. This means that I will not re-grade only the part you have requested, but the whole exam/homework and add or reduce points accordingly.

Missed Exams/Presentation

If you miss an exam/presentation date, the only way to reschedule is to have an official document (ex. from doctor, coach) verifying the reason you had to miss the test AND to let me know with an email BEFORE the date of the exam/presentation. Please refer to the student handbook "Class attendance policies" for a more detailed description of excused absences. A reason to miss the test may be a health issue, a sports tournament you had to participate, or an important personal issue. I will consider rescheduling on a case-by-case basis.

Attendance

Regular attendance is expected of all students. I take attendance at the beginning of each class session. Participants are expected to attend all sessions, ***be punctual***, and remain for the duration of each class. In the rare case where some absence is required, make up work will be assigned where it is practical to do so. Attendance is also part of the grading scale. Students may be withdrawn by the instructor if absences violate these guidelines.

Schedule

The schedule is tentative and *subject to change* during the semester.

Week	Date	Topics	Reading
Week 1	Jan. 9	Intro: Syllabus, Vulnerabilities, Threats, Attacks	Ch. 1
Week 2	Jan. 14	Risk analysis, ethics	Ch. 8.1, 8.2
	Jan. 16	Access Control	*Ch. 2*
Week 3	Jan. 21	Authentication	Ch. 2
	Jan. 23	Cryptography - intro	*Ch. 2*
Week 4	Jan. 28	Cryptography - DES, AES	*Ch. 12*
	Jan. 30	Cryptography - asymmetric	*Ch. 12*
Week 5	Feb. 4	Cryptography - Key Exchange Diffie Hellman	*Ch. 12*
	Feb. 6	Cryptography - RSA	*Ch. 12*
Week 6	Feb. 11	Computer networks nuts and volts	
	Feb. 13	Computer networks nuts and volts	
Week 7	Feb. 18	Computer networks nuts and volts, Midterm Review	

	Feb. 20	Midterm Exam	
Week 8	Feb. 25	Web App Exploits	*ch. 4*
	Feb. 27	Web App Exploits	*ch. 4*
Week 9	3-Mar	Network Security	ch. 6
	5-Mar	Network Security	ch. 6
Week 10	10-Mar	Network Security	ch. 6
	12-Mar	Network Security	ch. 6
Week 11	17-Mar	Spring Break	ch. 6
	19-Mar	Spring Break	
Week 12	24-Mar	Network Security	
	26-Mar	Software security	ch. 3
Week 13	31-Mar	Software security	ch. 3
	2-Apr	Software security	ch. 3
Week 14	7-Apr	Software security	ch. 3
	9-Apr	OS security	ch. 5
Week 15	14-Apr	OS security	ch. 5
	16-Apr	OS security	ch. 5
Week 16	21-Apr	Final review	
		Final Exam: Section 01 April 28 16:00 - 19:00, Section 02 April 26 16:00 - 19:00	

Honor Code

I expect you to abide by the Honor Code and the Student Handbook: A Guide to Civil and Honorable Conduct. If you have a question about how to interpret the Honor Code, ask before acting! I encourage collaboration, but you must document it. Thus, each student will submit their own homework and, when collaborating, provide a reference to those people and documents consulted.

What is plagiarism?
The unauthorized use or close imitation of the language and thoughts of another author and the representation of them as one's own original work, as by not crediting the author. *(Source: dictionary.com)*
As you noticed above, I am citing the Internet source from which I used my information. Plagiarism includes using material from the Internet without citing the website from which you got your material. Books, articles and any hard copy sources should be cited as well. Plagiarism is considered cheating.

Plagiarism and coding (what you can and cannot do!):

1. You may look up examples on the Internet.
2. You may NOT copy paste code from the Internet and present it as your own. Avoid copy pasting code from the internet and use this as a last resort ALWAYS with citation to the website that you used.
3. You may use libraries that are included in the language of your choice.

Discussing solutions with other students: Make sure you apply the **"empty hands policy",** i.e., do not copy or use material from the discussion, just interact, brainstorm. You *cannot look at someone's code and then type it*. *You cannot share the programs*, write code on a paper and share it with someone, or in any form whatsoever share your programs.

Collaboration in teams is allowed only if I have explicitly described in the project/homework assignment. You may collaborate based on the principles of pair programming (see below) and only if I have authorized teams. The Honor Code applies to the team members.

My actions after I suspect a cheating:

1. Contact the student and discuss the issue.
2. Consult with the honors committee and proceed to submit the issue with sufficient evidence that the student has cheated.

Pair Programming

Programming projects can be performed in teams of two members. The goal is to learn pair programming principles and extreme programming techniques that are used in industry. This allows the students to learn from each other and learn to collaborate. The main responsibilities for such collaboration are:

1. All the members of the team need to have project ownership, i.e., participate equally in the design, development and documentation. The instructor will ask in depth questions to all members of the team.
2. **All programming must be done in the pair.** Do not continue programming outside the pair. If you can't finish in one session, meet again. If that's impossible, save a copy of the code you pair-programmed for separate submission. Then work alone to finish the code. Review the part you coded alone with the other team members.
3. You need to follow the rules of pair programming, switching roles from observer to driver every 15 minutes or so.
4. All members receive the same grade.
5. A team leader will make the assignment submission. This is just to maintain one submission per team and in no way the team leader should do less or more work than the rest of the team members.
6. Students need to bring up collaboration issues early (first week of assignment) in order to switch teams.

Accommodations for Adults with Disabilities

The College will make reasonable accommodations for persons with documented disabilities. Students

should apply for services at the Center for Disability Services/SNAP located on the first floor of the Lightsey Center, Suite 104. **Students approved for accommodations are responsible for notifying me as soon as possible and for contacting me at least one week before accommodation is needed.**

Final Notes

- I have a Greek accent that may be hard to understand sometimes. Please do not hesitate to ask me to repeat something.
- If you need to record the class, you may do this with your phone if you do not disturb the class.
- Please respect your classmates. Put your phone on silent mode before the lecture starts.