CSIS 641

Advanced Cybersecurity
Spring 2017

Instructor: Xenia Mountrouidou (Dr. X)
E-Mail: mountrouidoux@cofc.edu
Phone: (843)-953-2754
Office: Harbor Walk East, Room #312
Office Hours: Tues/Thurs 11:10 – 12:10 pm and 2:30 – 3:30 pm, 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 631

Outcomes

After completing CSIS 641 students will be able to:

1. Examine the architecture of a cyber system to discover vulnerabilities
2. Develop and use already existent tools for pen testing and vulnerability assessment
3. Explain main Information Security components and security lifecycle
4. Discover different types of network intrusions based on their key features
5. Describe and evaluate the effectiveness of firewalls and VPNs
6. Develop rules for Intrusion Detection/Prevention Systems and evaluate these using statistical Receiver Operating Characteristic (ROC) curves
7. Use scanning techniques for information gathering
8. Analyze Denial of Service and other common attacks
9. Evaluate and propose defense mechanisms
10. Develop a buffer overflow attack and propose defense mechanisms
11. Point out non-secure programming practices and substitute these with secure programing and input sanitizing techniques
12. Understand key concepts: HTTPS, SSL, IPSec, IEEE 802.11 wireless security and hypothesize their weaknesses.
13. Articulate laws and policies, ethical issues on cybersecurity
14. Design risk assessment, understand security team roles
15. Explain the role of management in development, maintenance, and enforcement of cybersecurity policy
16. Formulate social engineering scenarios to test the preparedness of their organization
17. Identify and propose security controls
18. Recognize human factors in security and the value of education and training

Materials

Required book:
"The Basics of Hacking and Pen Testing", Patrick Engebretson

Recommended books:
"Red Team Field Manual", Ben Clark
"Blue Team Field Manual: Incident Response Edition", Don Murdoch
"The Hacker Playbook 2", Peter Kim
"Penetration Testing: A Hands-On Introduction", Georgia Weidman
We will also read several academic publications that will be posted on the course website

Software:

1. Putty for Windows or terminal for Mac OS
2. Kali VM
3. Metasploitable VM
4. OWASP Webgoat VM

Class Meeting times: Wednesday 6:00 – 8:30 pm
Class Location: Harbor Walk East #300
My Office: Harbor Walk East, Room #312
Office Hours: Tues/Thurs 11:10 – 12:10 pm and 2:30 – 3:30 pm, or by appointment
Course Website:
http://mountrouidoux.people.cofc.edu/CSIS641/index.html

Evaluation

Project	40%
Reports	30%
Midterm	20%
Participation	10%
Total	100%

Your weighted average will result in a letter grade assigned according to the usual scale: A: 93%-100% A-: 90%-92% B+: 87%-89% B: 83%-86% B-: 80%-82% C+: 77%-79% C: 73%-76% C-: 70%-72% D+: 67%-69% D: 63%-66% D-: 60%-62% 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

- **Reports**
  - You will have one lab report assignment every week or two weeks.
  - Lab reports will be submitted by teams of maximum two students.
  - You need add your lab teams in a google sheet by January 18th.
  - **Reading Reports**: You will write an individual blog entry with minimum 300 words every week related to the reading of the week.
  - **Blog entries:** I will ask for additional blog entries where you will need to perform a security critique for a new product. You may discuss these blog entries and submit them with your lab partner.
- **Project**
  - The project will be completed by teams of two students.
  - You need add your project teams in a google sheet by January 18th.
  - The project topic will involve *research on cybersecurity*. You will need to discover a new vulnerability on a computer network, web application, software package, or hardware device.
  - You will have multiple deliverables and presentations for your project.
  - We will use Oaks for Project submissions.
- **Participation**:
  - Participation will be the average of your attendance, presentation(s), and active in class participation.
  - You need to actively answer and ask questions during class to earn active in class participation points. A good idea is to prepare a question based on the reading and be ahead of the material at least by one lecture.
  - The participation points are dependent on my discretion based on your attention and active preparation.

- You should contribute positively to the classroom learning experience, and respect your classmates right to learn (see College of Charleston Student Handbook, section on *Classroom Code of Conduct* (p. 58)).
- You will have **one or two paper presentations during class time** that will be part of your participation.
- Presentations will be performed individually.

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	Topics
1	Intro: Syllabus, Attacks and Defense Mechanisms, Pen Testing Lab Setup

2	Vulnerability Assessment, Pen Testing Primer
	Reconnaissance
3	Intrusion Detection
	Scanning
4	Firewalls & VPNs
	Finding Vulnerabilities
5	IDS & IPS
	Capturing Traffic
6	Network Attacks
	DDoS Lab
7	Network Security Protocols
	Metasploit, Exploit DB
8	Web App Exploits
	SQL Injection, XSS
9	Spring Break
	Spring Break
10	Stack Exploits & Secure programming
	Stack overflow Linux/Windows
11	Social Engineering
	SE framework
12	Wireless security, IoT
	MiTM
13	Legal, Ethical, Professional issues
	Audit & reporting
14	Security Management and Risk Assessment
	Audit & reporting
15	Security controls, plans and procedures
	Audit & reporting
16	Final Exam: Project Presentations

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 Java API.
4. If you plan to use a library that is not on the Java API in a project, you will need to discuss this with me.

Discussing solutions with other students: Make sure you apply the **"empty hand 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 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.