UNI CS 4410, Section 1 (Spring 2018)
System Security

Course Syllabus (Version 2.0)

Lecture: MWF 3:00pm-3:50pm WRT 112

Contact Information

Instructor
Sarah Diesburg (diesburg@cs.uni.edu)
Office: 311 ITTC
Office hours: See personal homepage: http://www.cs.uni.edu/~diesburg
Class website: http://www.cs.uni.edu/~diesburg/courses/cs4410_sp18/

Course Description

Topics include the need for security services, data integrity, network intrusion and monitoring, configuration of secure services, root kits, and buffer overflow techniques and remedies. Additional topics include enterprise-wide monitoring, honeypots, and recognizing trends in a networked environment. Prerequisite(s): CS 3470; junior standing.

Goals and Objectives

After taking this class, students should understand general terms and tools to perform offensive and defensive security. Students will have hands-on experience with small and large projects with use of current tools. Students will work in a small group to secure (harden) a small network of servers with realistic/real services.

Prerequisites

- Computer Science and NASA Majors
  - CS 3470 Networking

Course Material

- Instead of a traditional book, we will use provided notes from the NSA C5 "Module 2a - Cybersecurity Threats and Countermeasures"
- Traditional website – notes, assignments, deadlines
- GitLab Wiki – group documentation, individual weekly journals
- Blackboard – gradebook, place to take quizzes and surveys

Project Course Requirements

Use of a versioning system
Documentation for each project will be placed on a shared group wiki. You may copy and paste directly from your journal entries to create the final document, but the final product must be professional-looking. Also, **do not** forget to cite your sources. If you have a question about how this should be done, ask me.

Peer reviews
Group members will assign team points to each member of the team based on effort for projects. After the final project, students will also assess the completeness of projects from other groups and their own group members' efforts.

Group projects(s)
The first five projects are small, instructive projects for each group to learn key system security concepts and tools. The last project will be at a level above the ability for a single person to accomplish and will consist of putting together both offensive and defensive security skills learned from the previous projects to create a secured (hardened) network. Documentation is important, and each documentation deliverable will count significantly to each group project grade (even if a presentation is not necessary).

Tentative Course Schedule

The following schedule is subject to change and is for general planning purposes only.

Module	Components
Setup (1 week)	• Experience survey • Assign teams • Get familiar with GitLab for journals and documentation (group) • Get familiar with course materials (individual)
Offensive Security – Terms and Background (2 weeks)	• Mini presentation (all groups) • Documentation deliverable for assigned tool (all groups) • Quiz over C5 material (individual)
Offensive Security – OWASP (2 weeks)	• Documentation deliverable (all groups) • Quiz over C5 material (individual)
Offensive Security – LAMPSec Capture the Flag – Training Wheels (2 weeks)	• Documentation deliverable (all groups) • Quiz over C5 material (individual)
Offensive Security – LAMPSec Capture the Flag – No Training Wheels (2 weeks)	• Documentation deliverable (all groups) • Quiz over C5 material (individual) • Mini presentation (all groups)
Defensive Security – Terms and Background (2 weeks)	• Documentation deliverable for assigned tool (all groups) • Mini presentation (all groups) • Quiz over C5 material and tools (individual)
Defensive Security Final Project (4 weeks)	• Firewall, IDS, and hardened LAMPSec machine or other servers (all groups) • Use Nessus, Nikto, and other tools to determine vulnerabilities of another group's network (all groups) • Surprise servers to secure (all groups) • Final documentation deliverable (all groups) • Final large presentation (all groups)
Hacking News and Whitepapers (if time)	• TBD

Class Grading

The following coursework components contribute to your final grade, and to the degree shown:

Activity	Percentage
Quizzes over C5 materials (individual)	**20%**
Class Participations/Attendance (individual)	**5%**
Small Projects (group)	**40%**
Final Documentation and Presentation (group)	**35%**

** While most groups will receive a single grade for each assignment, and all members of the group will receive this same score, I reserve the right to assign an individual student ***fewer*** "group points" than the other members of his/her group if I feel that student has failed to participate in his/her group's work to a sufficient level. I will determine this through each student's journal entries, commits (saves) on the documentation wiki in GitLab, and peer reviews.

Typical grading scale

100 – 92	A	81.9 – 80	B-	69.9 – 68	D+
91.9 – 90	A-	79.9 – 78	C+	67.9 – 62	D
89.9 – 88	B+	77.9 – 72	C	61.9 – 60	D-
87.9 – 82	B	71.9 – 70	C-	59.9 – 0	F

You must earn at least a C- to count this class towards your CS major. Scores will be posted to the course Blackboard gradebook as each item is graded. I reserve the right to apply a curve to shift all grades up if I believe it is necessary, but I will never apply a curve to lower a grade.

Expectations: This course will challenge you. Doing well requires you to dedicate a significant amount of time completing projects, reviewing materials, and thinking critically about new information. A commonly-accepted guideline in higher education is that you should spend 2-3 hours outside of class for every hour inside of class. If you are unsure how to spend your time, please talk with me and I can suggest activities. If you are putting in the suggested amount of time and you are still not getting the outcomes you desire, please talk with me and we can tailor your studying approach to maximize your learning. If you require additional help, don't hesitate to ask! The responsibility for learning the material is yours and yours alone – I am only an additional resource available to help you with your learning!

It is important that we are all respectful of each other's viewpoints, knowledge levels, and abilities. We will have fun in this class, and we will always foster a safe and positive learning environment. You should feel free to ask any question or share any view that you wish. Your behavior should demonstrate to others that they are free to share any viewpoint they wish, as well.

As part of being respectful to other students, keep in mind that disruptive behavior is distracting and disrespectful to others. Please make sure your actions do not impede the learning of other students.

Incompletes: Incompletes are awarded only in very rare instances when an unforeseeable event causes a student who has completed all the other coursework to date to be unable to complete a small portion of the work in the ***last week or two*** of the semester (typically the final project). Incompletes will not be awarded for foreseeable events including a heavy course load or a poorer-than-expected performance. Verifiable documentation must be provided for the incomplete to be granted, and arrangements for the incomplete should be made as soon as such an unforeseeable event is apparent.

Attendance: I try to accommodate student needs whenever possible, but I can do so only if I know about them. If you ever need to make alternate arrangements that will affect your participation in this course, contact me -- and your teammates! -- in advance. The safest way to make such arrangements with me is by sending e-mail regarding your circumstances and of how you can be reached.

Scholastic Conduct: You are responsible for being familiar with UNI's Academic Ethics Policies (http://www.uni.edu/pres/policies/301.shtml). Remember, discussing assignments is good. Copying code or answers is not. Remember to cite any and all resources you use, including books, websites, and class materials. I want you to look things up, so I am expecting a lot of citations.

Accessibility: In compliance with the University of Northern Iowa policy and equal access laws, I am available to discuss appropriate academic accommodations that may be required for students with disabilities. Requests for academic accommodations are to be made during the first three weeks of the semester, except for unusual circumstances, so arrangements can be made. Students should register with Student Disability Services, 103 Student Health Center, to verify their eligibility for appropriate accommodations.