CPRE/INFAS 332X Cyber Defense Competition
Spring 2015, Department of Electrical and Computer Engineering

Catalog Listing
Participation in cyber defense competition. Scenario based computer system setup, risk assessment and design of security systems. Defense of computer and network systems against trained attackers. Team based.

Instructor
Dr. Julie Rursch, Department of Electrical and Computer Engineering
207 Nuclear Engineering (NucE)
Iowa State University
Phone: 515/294-2803
Email: jrursch@iastate.edu **** Best way to communicate with me

Course Overview
The cyber defense competition (CDC) course will encompass several major focal points of information assurance which culminate in a two day CDC. These major focal points include the planning & implementing of a defensive network based on a scenario, defending the network while under attack from a red team, and a written reflection of the effectiveness of the overall design.

Teams of students are required to plan a network to include many of the services that are provided in an average corporation, including mail, web, programming environments, and more. While on a much smaller scale, the intent is to give students experience with a “corporate” network and an understanding of security important to successful network implementations. The teams implement their network and defend their implementation during a cyber defense competition to be held on campus during the semester.

The students will submit multiple elements listed at the end of this syllabus for a grade.

After taking the course student will be able to:
- Design and document a “corporate” network, focusing on security and usability considerations
- Work in small teams to implement a planned network
- Defending their network against attacks during the cyber defense competition
- Write a summative, reflective paper which answers key questions demonstrating their their understanding of best security practices, network implementation implications, and end user usability.

Course Materials: Available on Blackboard. All projects will be turned in via Blackboard.
Course Grading (Satisfactory / Fail):
Reporting: 80%
  Team List: 5%
  Status Update on network design, security assessment, and implementation: 10%
  Planning Report including network design, security assessment, and implementation
    (white team documentation): 25%
  Assessment Report including reflections on the CDC 60%
CDC participation: 20%
  Must attend and participate in the ISU CDC.

Course Schedule:
Students will be given the scenario approximately three to four weeks prior to the competition. A status report is due one week after the CDC setup opens. The final report and other materials will be due on a Sunday night two weeks after the competition. The exact dates will be posted on Blackboard Since students work in teams to prepare for and participate in the CDC and not every person on the team is required to take this course, students in the course will each submit separate reports for grading. Members of the same team can share materials and work together on preparing the some of the reports (white team documentation and team list). The other reports (status update and assessment report) will be the student’s individual work.

Four reports will be required to be submitted via Blackboard for each student taking this course. There are two groups of students taking this course –Blue Team and White Team members. You will all turn in four things. However, when it says Blue in italics, Blue Team members follow that process. When it says White in italics, White Team members follow that process.

1) Status Report – Due one week after the competition opens
   o Blue: A one page summary of what your network design is, what your security plan is, where you are in the setup process, what your role is on the team, and what you hope to gain from participating in the CDC.
   o White: A one page summary of the purpose of the CDC, what the role of the white team is, what your role is on the white team, and what your contributions will be for this specific CDC. Think of this as your elevator speech to give to a potential employer when asked about what you contributed to the CDC.
   o Everyone: Each person in the course must submit an ORIGINAL paper for this requirement. This is NOT A TEAM effort. It is your own work.

2) A Team List – Due two weeks after the CDC
   o Blue: The CDC team number, CDC team name, and the names of the team members must be submitted. Please submit all team member names, even if they are not participating in the course.
   o White: Please submit a list of all White Team members and a one sentence description of their job. This should help you concisely come up with words to describe your work on the CDCs.
   o Everyone: You may make one list per team, but each person in the course needs to submit it.
3) **Planning Report – Due two weeks after the CDC**
   - **Blue:** Please submit your White Team documentation which includes a network diagram, as well as details about the network. Please include all the elements required for your White Team documentation as described in the CDC scenarios and rules.
   - **White:** Please submit a document about how ISEAGE is configured for a CDC including a diagram and specific details about configuration files, networking, servers, etc. The paper also needs to include what tasks have to be done to setup, manage, support, and run a CDC as a White Team member, and what kind of time commitment is needed. Again, this is to help you talk to potential employers in more depth about the skills you have because you had a leadership role on the White Team during a CDC. Please do a thorough job on this, just as the Blue Team will do on their documentation.
   - **Everyone:** Again, you only need to write one copy of the documentation, but it needs to be submitted for each person in the course.

4) **Assessment Report – Due two weeks after the CDC**
   - **Everyone:** A template is provided on Blackboard. The differences for Blue and White Team members will be addressed in the template. All in the template questions must be addressed and be in the order listed on the template. Each person in the course must submit an ORIGINAL paper for this requirement. This is NOT A TEAM effort. It is your own work and evaluation of your team network design and security, as well as a reflection of what you learned and what you would do differently.