ISM 324: Information Systems Security
Spring 2014

Instructor: Jeffrey Wall
Co-Instructor: Hamid Nemati
Office: 392 Bryan Building
E-Mail: jdwall2@uncg.edu (email is the preferred method of contact)
Phone: (336) 334-4159 (I don’t have a voicemail box)
Office Hours: Tue & Thu from 1:00 pm – 2:30 pm
And by Appointment

Catalog Description:
Study of technical and business issues in information systems security, systems security models, analysis of process and technology in systems security, and security policies leading to information assurance.

Course Objectives:
This course is designed to provide students with a knowledge overview of information security topics. Students who successfully complete the course should be prepared to take the CompTIA Security+ certification exam.

Upon completion of the class, students will be able to:

1. Understand the basics of information security
2. Recognize the different types of controls and methods used to secure information
3. Understand basic network security, host security, and data security
4. Implement wired and wireless networks in a secure manner
5. Identify threats to information assets
6. Differentiate among different types of malware
7. Understand the different types of information security attacks
8. Identify, assess, and mitigate the risks and vulnerabilities in information systems
9. Know how to make information security plans for an organization
10. Appreciate the role of cryptography in information security
11. Learn how to operationalize/implement information security for an organization
12. Acquire the knowledge required to pass the CompTIA Security+ certification exam

Required Textbook:

Instructional Methods:
This course will be delivered by mixing lectures with hands-on security exercises and a team project. Lectures will give students a basic understanding of security topics to prepare for the CompTIA Security+ exam and a foundation for engaging in the hands-on exercises. Students will have the opportunity to practice the techniques discussed in lecture by completing hands-on activities. Students are expected to learn how to find information to solve the problems they encounter in the hands-on exercises. Knowing how to find answers is extremely important, as new security threats and tools arise regularly. Thus, hands-on activities will not follow a formal and structured lab style. Students will be provided with an objective and asked to complete the objective using any legal and ethical means. This structure is to ensure that students learn how to find information and solve problems on their own or in teams. A great deal of learning in the class is self-directed, particularly for students who plan to take the CompTIA Security+ exam. Students are encouraged to use materials and resources outside of the required textbook to assist in their learning. Finally, class projects challenge students to understand different perspectives about security and apply the knowledge learned in class while engaging with the business community.
General Preparedness:
Students are expected to participate in class. Students are expected to be prepared for class by reading assigned materials. Each student is responsible for all of the information and announcements that are made in class and on Blackboard. Announcements are frequently posted to Blackboard. Poor performance in this course is directly related to poor attendance. Students are expected to conduct themselves in a professional manner. Professionals show up for scheduled meetings prepared and on time and participate regularly. Any student missing the first two classes without notifying the instructor will be administratively dropped from the course.

Late Assignments:
Quizzes cannot be turned in late. Quizzes must be completed at their assigned date and time.

Points for hands-on activities cannot be made up. Students must attend and participate in activities to receive points.

Exams may only be made-up with a written, verifiable, legitimate excuse or prior written consent from the instructor.

Late projects will be docked 10% for every day late up to 40% off unless previous written arrangements are made with the instructor. No assignment will be accepted after the last official day of class; this does NOT include finals week.

Quizzes:
Quizzes account for approximately 14% of the total grade. There will be 5 quizzes throughout the semester. Quiz dates are posted on the course schedule, but adjustments may be made to the quiz schedule with at least 2 days notice by email. Any changes to the schedule will also be posted to the Blackboard announcements section. Quizzes are each worth 25 points toward your final grade. The lowest quiz score will be dropped. Quiz questions will come from reading materials and class discussions and activities. Not all material is covered in class. Students are expected to do the assigned readings to further develop their knowledge. Students who miss class on the date of a quiz will not be allowed to take a quiz at a later time. Students who are late to class on the day of a quiz will not be granted extra time.

Participation:
Participation accounts for approximately 14% of the total grade. Participation is based on attendance and participation during class activities. There are 5 class activities, including: the Social Engineering Audit, Crack a System: White Box Penetration Testing, Crack a System: Black Box Penetration Testing, Crack a Website, and the Mock Security Incident. Activity dates are posted on the course schedule, but adjustments may be made to the activity schedule with at least 2 days notice by email. Any changes to the schedule will also be posted to the Blackboard announcements section. Activity participation is worth 25 points per activity. I will drop the lowest activity score. Participation points cannot be made up and students must attend class and participate on the day of an activity to receive points. Students who come late to activities will only receive half points for the activity. To participate in class activities students must agree to the terms in this syllabus.

Midterm and Final Exams:
The midterm and final exams are written, in class, and closed-book. They are meant to simulate the CompTIA Security+ Exam as much as possible. Again, students are responsible for material in the assigned readings even if not covered in class. No make-up examinations are offered unless a written, verifiable, legitimate excuse for the absence is presented to the instructor or written arrangements are made beforehand. The final may include some content covered on the midterm. Attendance on the date of exams is MANDATORY.

Team Project:
Students will engage with a business in the community or with working professionals in order to develop a paper related to information security. Teams will consist of 5-6 students. An assignment sheet will be posted to Blackboard describing the details of the project. The project is worth 200 points of your final grade.

CompTIA Security+ Exam:
This course is designed to help you pass the CompTIA Security+ certification exam. Taking the CompTIA Security+ certification exam is entirely optional. However, if you take the exam and pass it, you will earn an additional 200 points toward your overall points for the course. Additionally, if you pass the exam, you are not required to take the final exam for the course. You must provide proof that you passed the CompTIA Security+ certification exam before the final exam for the course in order to receive the additional 200 points.
Grading:

Your final grade is determined using the following scale and assignment weights:

<table>
<thead>
<tr>
<th>Points</th>
<th>Grade</th>
<th>Points</th>
<th>Grade</th>
<th>Points</th>
<th>Grade</th>
<th>Points</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>97-100%</td>
<td>A+</td>
<td>87-89%</td>
<td>B+</td>
<td>77-79%</td>
<td>C+</td>
<td>67-69%</td>
<td>D+</td>
</tr>
<tr>
<td>93-96%</td>
<td>A</td>
<td>83-86%</td>
<td>B</td>
<td>73-76%</td>
<td>C</td>
<td>63-66%</td>
<td>D</td>
</tr>
<tr>
<td>90-92%</td>
<td>A–</td>
<td>80-82%</td>
<td>B–</td>
<td>70-72%</td>
<td>C–</td>
<td>60-62%</td>
<td>D–</td>
</tr>
<tr>
<td>Below 60%</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Deliverables                  Points
Quizzes (25 points each)       100 points
Participation (25 points each) 100 points
Midterm Exam                   100 points
Final Exam                     100 points
Team Project                   200 points
Total                           700 points

Ethical Issues and the Honor Code Policies:

University students are expected to conduct themselves in accordance with the highest standards of academic honesty. Academic misconduct for which a student is subject to penalty includes all forms of cheating, such as illicit possession of examinations or examination materials, forgery, plagiarism, etc. Although students are allowed to work with others during activities and on team projects, students may NOT borrow, or "share". Students will receive a 0 for the deliverable if misconduct is proven. Students should read and must follow the UNCG Honor Code.

Plagiarism is defined as "presenting as one’s own work that work which is, in whole or in part, the work of another person or persons without giving proper credit to the appropriate source." This includes submitting work done by another as one’s own work. It is understood that what you turn in to me for a grade represents your own effort. Plagiarism will be immediately punished with a 0 for the assignment in question. Further disciplinary action will be pursued as the instructor deems appropriate. **No credit will be received for shared work, and other penalties may be imposed.**

This course also has some additional issues owing to the unique nature of security. You may NEVER attempt to penetrate the UNCG network as part of this class. Although a simple system will be provided for penetration testing activities, students may not attack the system without permission from the instructor. **Students caught misusing the UNCG network or the network used for class activities will receive an F in the course and will be reported to the dean of students for misconduct. Depending on the offense, students who attack a system without authorization may be criminally prosecuted as well.**

UNCG’s academic integrity policy can be viewed at: [http://academicintegrity.uncg.edu/complete/](http://academicintegrity.uncg.edu/complete/)

Bryan Faculty/Student Guidelines:

Faculty and students at UNCG have certain obligations. Please view these obligations and guidelines at: [http://www.uncg.edu/bae/faculty_student_guidelines_sp07.pdf](http://www.uncg.edu/bae/faculty_student_guidelines_sp07.pdf)

Disabilities:

If you have a documented disability and wish to discuss academic accommodations, please contact me as soon as possible.

Inclement Weather:

Rarely, UNCG closes for inclement weather. The radio and TV stations will have the closing notification by 6:30 am. You may also call 334-5000 for a message related to weather closings. These messages are updated hourly.

* This syllabus is subject to change as needed *
Student Conduct Agreement for ISM 324 (Spring 2014)

By remaining in this course, I agree to the following:

1) I agree that I have read, understand, and will abide by the policies and restrictions set forth in the course syllabus for ISM 324.
2) I agree that I will not misuse the UNCG networks or computer resources as a part of ISM 324.
3) I understand that I am not allowed to attack or scan the UNCG networks as part of ISM 324.
4) I agree that I will follow the instructions given by the instructor during ISM 324 course activities.
5) I agree that I will only attack the network dedicated for the purpose of activities in ISM 324 (NOT the UNCG networks) after receiving permission from the instructor.
6) I understand that I may not use my own computer or IT resources to engage in ISM 324 class activities.
7) I understand that I will receive an F in the course and that I will be reported to the dean of students for misconduct if I misuse any UNCG resources or do not follow the instructor’s instructions regarding class activities.
8) I understand that any attack methods taught in ISM 324 are for educational purposes only and are meant to teach students about ethical and legal penetration testing that would be performed by a security professional.
9) I agree that I will not use, scan, or attack the computer systems or IT resources of the businesses or working professionals who I will engage with for the team project in ISM 324.
**Tentative Course Outline**  
*This outline is subject to change as needed*

<table>
<thead>
<tr>
<th>Week Of</th>
<th>Lecture (Tuesday)</th>
<th>Quiz/Activity (Thursday)</th>
<th>Readings</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 01 (01/13)</td>
<td>Mastering the Basics of Security</td>
<td>Social Engineering Audit</td>
<td>Chapter 1</td>
<td>Read Syllabus</td>
</tr>
<tr>
<td>Week 02 (01/20)</td>
<td>Exploring Control Types and Methods</td>
<td>Quiz for Chapters 1 &amp; 2</td>
<td>Chapter 2</td>
<td>Team Charter Due 01/23 at midnight (11:59 pm)</td>
</tr>
<tr>
<td>Week 03 (01/27)</td>
<td>Understanding Basic Network Security</td>
<td>Crack a System: White Box Penetration Testing</td>
<td>Chapter 3</td>
<td>Project Proposal Due 01/30 at midnight (11:59 pm)</td>
</tr>
<tr>
<td>Week 04 (02/03)</td>
<td>Securing Your Network</td>
<td>Quiz for Chapters 3 &amp; 4</td>
<td>Chapter 4</td>
<td>Begin Contacting Organizations for Project</td>
</tr>
<tr>
<td>Week 05 (02/10)</td>
<td>Securing Hosts and Data</td>
<td>Crack a System: Black Box Penetration Testing</td>
<td>Chapter 5</td>
<td></td>
</tr>
<tr>
<td>Week 06 (02/17)</td>
<td>Malware and Social Engineering</td>
<td>Quiz for Chapters 5 &amp; 6</td>
<td>Chapter 6</td>
<td>Interview Dates Due 02/20 at midnight (11:59 pm)</td>
</tr>
<tr>
<td>Week 07 (02/24)</td>
<td>Identifying Advanced Attacks</td>
<td>Crack a Website</td>
<td>Chapter 7</td>
<td></td>
</tr>
<tr>
<td>Week 08 (03/03)</td>
<td>Exam Review (Optional)</td>
<td>Midterm Exam in class on 03/06 (Chapters 1-7)</td>
<td>No Reading!!</td>
<td></td>
</tr>
<tr>
<td>Week 09 (03/10)</td>
<td>Spring Break. No class. Enjoy!!</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Week 10 (03/17)</td>
<td>Managing Risk</td>
<td>Open Lab. No class. Last day to conduct interviews.</td>
<td>Chapter 8</td>
<td>Interview Notes Due 03/20 at midnight (11:59 pm)</td>
</tr>
<tr>
<td>Week 11 (03/24)</td>
<td>Preparing for Business Continuity</td>
<td>Quiz for Chapters 8 &amp; 9</td>
<td>Chapter 9</td>
<td></td>
</tr>
<tr>
<td>Week 12 (03/31)</td>
<td>Exploring Operational Security</td>
<td>Mock Security Incident</td>
<td>Chapter 11</td>
<td></td>
</tr>
<tr>
<td>Week 13 (04/07)</td>
<td>Understanding Cryptography</td>
<td>Quiz for Chapters 10 &amp; 11</td>
<td>Chapter 10</td>
<td></td>
</tr>
<tr>
<td>Week 14 (04/14)</td>
<td>Open Lab. No class. Work on finalizing projects.</td>
<td>Group Project Presentations</td>
<td>No Reading!!</td>
<td>All Group Projects Due 04/17 before class (3:30 pm)</td>
</tr>
<tr>
<td>Week 15 (04/21)</td>
<td>Group Project Presentations</td>
<td>Exam Review (Optional)</td>
<td>No Reading!!</td>
<td></td>
</tr>
</tbody>
</table>

**Finals Week**  
Final Exam in class on 05/06 from 3:30-6:30 (Chapters 1-11, but primarily chapters 8-11)