CSCI 3250 – Computer Security
Fall 2016 UNG Online

GENERAL INFORMATION
Aaron Walker
Contact Email: Aaron.Walker@ung.edu
Website: http://faculty.ung.edu/arwalker/
Office Hours: This is an online course – feel free to contact me via email or D2L as needed
D2L: http://ung.view.usg.edu

TEXT AND OTHER MATERIALS
- Several free, open-source tools and operating systems are required to be downloaded, installed, and utilized in the applied labs for this course (VirtualBox, Kali Linux, an Apache web server, OpenSSL, and similar) – a laptop or desktop with at least 8GB of RAM is recommended.

COURSE DESCRIPTION
This course covers several security topics pertaining to real-life systems currently deployed and commonly used in the Internet computing environment. Materials covered include program security issues, database security issues, and operating systems security issues. Pre-requisite: CSCI 1301

COURSE OBJECTIVES
Topics include access control, physical security, operating systems security, malware, network security, web security, cryptography, security models, and distributed application security. Students will learn about techniques for identifying and defending against vulnerabilities in computers and networks, as well as methods for detecting and repairing infected systems.

LEARNING OUTCOMES
Students shall demonstrate the ability to:
- Explain the differences between different types of malware, and how we can defend systems against them
- Assess vulnerabilities and harden a computer system
- Compare and contrast different methods of encryption, as well as types of cryptanalysis
- Identify management issues in information security, and recommend policy, process and practice improvements
- Understand TCP/IP, UDP, and other protocol vulnerabilities
- Anticipate and mitigate various web, Internet and network threats
METHODS OF INSTRUCTION
This course is designed as to use technology-enhanced lecture and applied lab. Online labs and tutorials will be used for some lessons.

EVALUATION METHODS
Labs: 40%; Discussion: 10%; Mid-Term Exam: 25%; Final Exam: 25%

All assignments are expected to be submitted by their respective due dates. Students who are unable to meet a deadline must contact their instructor prior to the due date in order to arrange an appropriate alternative in order to avoid the penalty - 10% deducted for each day the assignment is past due.

CLASS DISCUSSIONS
Discussions are an important part of online instruction and class participation. Each week a new graded topic will be posted in the D2L class forum. A total of 3 points are possible for each week for posting in the graded forum and the grading is as follows:
- 1 point for posting by the Wednesday of the topic week
- 1 point for posting after the Wednesday and by the Sunday of the topic week
- 1 point for making a meaningful comment regarding another’s post
  - Constructive criticism is allowed (do not breach the netiquette rules as outlined in D2L)
  - Posts of agreement are allowed, but you must add to the conversation (do not simply post “yeah, I feel the same way”
  - Your post must enhance the argument with corroborating information from online articles, detailed personal experience, etc.)

EXAM DELIVERY
The Midterm Exam will be proctored through ProctorU (https://proctoru.com/portal/ung).

In order to use ProctorU you will need to have a high-speed internet connection, a webcam (internal or external), a windows or apple Operating System, and a government issued photo id. ProctorU recommends that you visit http://proctoru.com/testitout/ prior to your proctoring session to test your equipment. For additional technical services needed before your exam, you can click on the button that says “connect to a live person.” There is also a test taker walk through video available at https://vimeo.com/107066503.

The Final Exam will not be proctored but made available to take online via D2L.

COURSE GRADING
Weighted total grade from above: 90-100%: A, 80-89%: B, 70-79%: C, 60-69%: D; 0-59%: F
## COURSE CALENDAR

<table>
<thead>
<tr>
<th>Week #</th>
<th>Date</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>8/22/2016</td>
<td>Intro, Ch 1: The Threat Environment</td>
</tr>
<tr>
<td>Week 2</td>
<td>8/29/2016</td>
<td>Ch 2: Planning and Policy; Lab1 assigned</td>
</tr>
<tr>
<td>Week 3</td>
<td>9/5/2016</td>
<td>Labor Day Holiday (Monday), Ch 3: Cryptography</td>
</tr>
<tr>
<td>Week 4</td>
<td>9/12/2016</td>
<td>Ch 3 continued; Lab2 assigned</td>
</tr>
<tr>
<td>Week 5</td>
<td>9/19/2016</td>
<td>Ch 4: Secure Networks</td>
</tr>
<tr>
<td>Week 6</td>
<td>9/26/2016</td>
<td>Ch 5: Access Control; Lab3 Assigned</td>
</tr>
<tr>
<td>Week 7</td>
<td>10/3/2016</td>
<td>Ch 5 continued; Mid-Term Exam</td>
</tr>
<tr>
<td>Week 8</td>
<td>10/10/2016</td>
<td>Ch 6: Firewalls; Lab4 assigned</td>
</tr>
<tr>
<td>Week 9</td>
<td>10/17/2016</td>
<td>Ch 6 continued</td>
</tr>
<tr>
<td>Week 10</td>
<td>10/24/2016</td>
<td>Ch 7: Host Hardening; Lab5 assigned</td>
</tr>
<tr>
<td>Week 11</td>
<td>10/31/2016</td>
<td>Ch 7 continued</td>
</tr>
<tr>
<td>Week 12</td>
<td>11/7/2016</td>
<td>Ch 8: Application Security</td>
</tr>
<tr>
<td>Week 13</td>
<td>11/14/2016</td>
<td>Ch 8 continued; Lab6 assigned</td>
</tr>
<tr>
<td></td>
<td>11/21/2016</td>
<td>Fall Break - no classes</td>
</tr>
<tr>
<td>Week 14</td>
<td>11/28/2016</td>
<td>Ch 9: Data Protection</td>
</tr>
<tr>
<td>Week 15</td>
<td>12/5/2016</td>
<td>Ch 10: Incident and Disaster Response</td>
</tr>
<tr>
<td>FINALS</td>
<td>12/12/2016</td>
<td>Final Exam</td>
</tr>
</tbody>
</table>

This syllabus may be adjusted if deemed necessary by the instructor.

Students are expected to refer to the Supplemental Syllabus for the following information:


1. Academic Exchange
2. Academic Integrity Policy
3. Academic Success Plan Program
4. Class Evaluations
5. Course Grades and Withdrawal Process
6. Disruptive Behavior Policy
7. Inclement Weather
8. Smoking Policy
9. Students with Disabilities