**CIS 480 – Introduction to Network Security**

**Professor**

|  |  |
| --- | --- |
| Name | Ghiyoung Im, PhD |
| Office | COB Building 303 |
| Office Hours | Tue & Thur, 3:00-5:00, and by appointment |
| Phone | (502) 852-4794 |
| Email | ghiyoung.im@louisville.edu |

**Class Meetings**: Monday 5:30 p.m. - 8:15 p.m.

**Prerequisites**: CIS 350.

**Required Materials**: Panko, R. R. (2010). *Corporate Computer and Network Security* (2nd). Boston: Prentice Hall. ISBN-13: 978-0131854758

**Optional Materials**: Cole, E., Krutz, R. L., & Conley, J. (2009). *Network Security Bible*. Indianapolis, IN: Wiley. ISBN-13: 978-0470502495

**Course Description**

The purpose of this course is to introduce the business student to the rapidly evolving and critical international arenas of network security. This course is designed to develop knowledge and skills for network security within and across organizations. It focuses on concepts and methods associated with TCP/IP, cryptography, access control, web security, wireless security, e-mail security, firewalls, and intrusion detection systems.

**Course Objectives**

Upon successful completion of this course, students will develop a broad appreciation for and a basic understanding of

* The overall framework of networking and network security
* The mounting threats and vulnerabilities of interconnected systems
* The crucial concepts such as cryptography, firewalls, intrusion detection systems, etc
* The basic tools that are designed to manage network security
* The importance of defense-in-depth

**Class Policies**

* Students are expected to attend all classes and group meetings (whether online or in person), except when precluded by emergencies, religious holidays or bona fide extenuating circumstances.
* Students who, for non-academic reasons beyond their control, are unable to meet the full requirements of the course should notify the instructor. Incompletes may be given if a student meets the criteria.
* Spirited class participation is encouraged and informed discussion in class is expected.  This requires completing readings and assignments before class.
* Unless specifically stated by the instructor, all exams and lab assignments are to be completed by the student alone.
* Within group collaboration is allowed on project work.  Collaboration between project groups will be considered cheating unless specifically allowed by an instructor.
* Copy work from the Internet without a proper reference will be considered plagiarism and subject to disciplinary action as delineated in the Student Handbook.

**Academic Honesty**

Students should abide by the Academic Honesty Code of University of Louisville. Follow the link for the details (https://louisville.edu/undergraduatecatalog/previous-years-catalogs/2006\_08/unitinfo/college-of-business/academic-dishonesty.html). The following is copied from the webpage.

“Every student is expected to be thoroughly familiar with the University's Code of Student Rights and Responsibilities and Student Conduct, which can be found in the "General Information" section of this catalog.

Every student is responsible for reading the academic policies in the Undergraduate Catalog and official announcements of the College of Business and for abiding by such regulations. Specifically, every student is responsible for knowing the grade point averages and program requirements needed for graduation. Students are encouraged to see a COB academic advisor to clarify any questions or concerns.

Along with preparing for and attending class, each student has the responsibility to promote high academic standards. Students are expected to cooperate in all classes with faculty members to achieve an optimal learning environment. Inappropriate classroom behavior may result in the student being withdrawn from the course, and potentially assigned academic penalties. Inappropriate classroom behavior will be dealt with in the same manner as academic dishonesty.

The COB will not tolerate academic dishonesty. The COB has a strong policy of academic discipline for action against students who commit academic dishonesty or conduct themselves inappropriately in the classroom. A proven case of academic dishonesty will normally result in the student being denied admission to or dismissed from the COB.

Academic dishonesty is defined by the Code of Student Conduct in the Undergraduate Catalog. Its definition pertains to but is not limited to cheating, fabrication, falsification, multiple submission, plagiarism, and complicity. It is the student's responsibility to maintain high standards of ethical conduct, and intellectual integrity and to be familiar with the definition of academic dishonesty.

As evidence of the seriousness with which the COB regards these matters, academic dishonesty allegations are handled in accordance with COB Procedures for Dealing with Academic Dishonesty.”

**Grade Policy**

|  |  |  |
| --- | --- | --- |
| **Grade Components** | **Points** | **Scale** |
| 5 Quizzes (each 10 points) | 50 | A = 90%-100%  B = 80%-89%  C = 70%-79%  D = 60%-69%  F = below 60% |
| Project1 (individual) | 50 |
| 4 Lab exercises (each 25 points) | 100 |
| Research paper (group) | 125 |
| Mid-term | 200 |
| Final | 200 |
| Class participation | 100 |
| *Total* | *825* |  |

**Projects/Reports**

All assignments/projects will be handed out and discussed in class. Due dates will be typically one week from their assigned dates. The following requirements for assignments exist:

* All assignments will be due on designated class days.
* Hard copy assignments must be submitted to the instructor on their due dates at the beginning of class time.
* Electronic file assignments must be uploaded to the instructor using Blackboard’s Assignment tool on their due dates before the beginning of class time.
* No assignments will be accepted after their due dates/times without advanced approval by the instructor.
* Students are expected to keep a backup copy of their assignments at least until their assignments have been graded.

**Lab Exercises**

This course includes four hands-on lab exercise sessions. These are designed to provide practical implications of the obtained knowledge in lectures via the available security tools. Students will download, install, and run security tools, and perform exercises as directed.

* These are individual/group exercises.
* Students are expected to bring their own laptops.
* Students are expected to complete the lab exercises during the class time and submit the outputs before the end of the day.
* The failure to submit the output of the lab exercise leads to zero points.

**Exams**

Exams will be given on the dates specified in the course schedule. Any changes to these dates will be announced as far in advance as possible with a minimum of a one-week notice. The following requirements for exams exist:

* Unless otherwise specified by the instructor, exams will be closed-book and closed-note paper-based assessments.
* Cell phones, pagers, and other electronic devices must be turned off during the exams.
* Missed exams count as zero points.
* Make-up exams will not be given without advanced approval by the instructor or without convincing extenuating evidence for reasons of absence, such as a doctor’s note or similar documentation.

**Research Reports**

Students are required to produce a term project, building upon and complementing the material covered in class. You will be working with other class members as part of a team. Teams will be formed during the third class, in plenty of time for you to meet, plan, and work with other members of your team. Some class time may be set aside for team meetings. Projects must culminate with either a presentation for the class or the submission of a final report.

**Readings**

Ayoub, R. (2011). The 2011 (ISC)² *Global Information Security Workforce Study*. Frost & Sullivan.

Im, G., & Baskerville, R. (2005). A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error. *The Database for Advances in Information Systems*, 36(4), 68-79.

Richardson, R. (2011). *2010/2011 CSI Computer Crime and Security Survey*. Computer Security Institute.

Trend Micro. 2009. *The Future of Threats and Threat Technologies: How the Landscape is Changing*.

**Resources**

Java Cryptography Extension (JCE):

<http://download.oracle.com/javase/6/docs/technotes/guides/security/index.html>

<http://download.oracle.com/javase/1.4.2/docs/guide/security/jce/JCERefGuide.html>

Brain Krebs on Security:

<http://krebsonsecurity.com/>

Bloomberg Businessweek:

[Riley, M. & Vance A. 2011. Cyber Weapons: The New Arms Race, Bloomberg Businessweek, July 25 – July 2011.](http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html)

CyberProtect (security simulation):

<http://iase.disa.mil/eta/cyber-protect/launchpage.htm>

VMWare (for CIS students):

<http://e5.onthehub.com/WebStore/Welcome.aspx?vsro=8&ws=92418b8d-a432-de11-9d57-0030485a8df0>

**Class Schedule (Subject to Change)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Week | Date | Topics | Chapters | Major Event | Reading Discussions |
| 1 | 8/22 | Introduction and review of the syllabus  The threat environment | Ch1 |  | 🞄Security Workforce Study (Ayoub, 2011)  🞄Play CyberProtect (simulation game) |
| 2 | 8/29 | The threat environment  IP security | Ch1  Module A | Submit the result of the sim game | 🞄2010/2011 Computer Crime and Security Survey  🞄The Future of Threats and Threat Technologies (Trend Micro)  🞄IT Threats Framework: (Im & Baskerville, 2005) |
| - | 9/5 | Labor day holiday – no class |  |  |  |
| 3 | 9/12 | IP security  Transport-level security | Module A | Team formation  Quiz1 |  |
| 4 | 9/19 | Transport-level security  Protocol analysis (Lab1) | Module A | Lab1: Packet analysis |  |
| 5 | 9/26 | The elements of cryptography | Ch3 | Project1: due 9/26  Quiz2 |  |
| 6 | 10/3 | Crypto analysis (Lab2)  Mid-term |  | Lab2: Encryption  Mid-term |  |
| 7 | 10/10 | Mid-term break | - |  |  |
| 8 | 10/17 | Cryptographic system standards | Ch4 |  |  |
| 9 | 10/24 | Access control | Ch5 | Quiz3 |  |
| 10 | 10/31 | Password management (Lab3)  Web security | Ch5  Ch8 | Lab3: Password cracking |  |
| 11 | 11/7 | Wireless security  Guest speaker | Ch4 | Quiz4 |  |
| 12 | 11/14 | Firewalls | Ch6 |  |  |
| 13 | 11/21 | Defense-in-depth  Attack strategies and mitigation |  | Quiz5 |  |
| 14 | 11/28 | E-mail security  E-mail security applications | Ch8 | Lab4: PGP |  |
| 15 | 12/5 | Research paper presentations |  | Research paper: due 12/5 |  |
|  |  | Reading day (12/6); Final exams (12/7-13) |  | Final exam |  |