CASPER COLLEGE COURSE SYLLABUS
CSEC 1500-01 Network Security Fundamentals

Semester/Year: SPRING/2015
Lecture Hours: 2  Lab Hours: 2  Credit Hours: 3
Class Time: 6-830pm  Days: Thursday  Room: Thorson 307
Instructor’s Name: Eric Salveggio
Instructor's Contact Information: Office Phone: (c) 277-3918
                                      Email: ericsalveggio@caspercollege.edu
Office Hours: 5-9 M-F

Course Description: This course examines current standards for information security through
examination of security technologies, methodologies and best practices. Topics include evaluations
of security models, risk assessment, threat analysis, attack types, encryption technologies,
organizational technology, security implementation, disaster recovery planning, and security policy
formulation and implementation.

Statement of Prerequisites: CSEC 1505

Goal: This class is going to be an eye opener for many, and yet, we’ll only be scratching the surface
of really goes on in the realm of cyber defense. It is hoped that the class will pique the interest of the
student to further pursue this field of study. Research within this field continues on into the PhD level,
is a never ending venture, and is never stagnant or dull.

Outcomes:
1. Solve problems using critical thinking and creativity
2. Demonstrate knowledge of diverse methods of attacks, and defense in depth
3. Use appropriate technology and information to conduct research
4. Describe the value of personal, civic, and social responsibilities in regards to protecting networks

Course Objectives: The overall objectives of this course is to introduce the student to world of cyber
defense and network technology. Topics covering civilian and government entities that are involved in
these topics will be touched upon, as well as the tools being used. Research of these tools, and those
that are constantly being propagated for both offense and defense will be conducted, and discussed.
With these discussions, students will be challenged to solve the problems facing all networks for their
defense, and how hackers may use some of these same tools to perform attacks.

Methodology: This course will be a combination of discussion, research, and lab simulations. Your
feedback is valuable as the instructor uses course evaluations in determining course methodology.

Evaluation Criteria: Participation is a critical part of this course! If you’re not here, you’re missing a
lot of info, and obviously not participating. As such, you will be graded on your participation. There
will be two quizzes, one research paper, a midterm, and final. The research paper will consist of a
topic, approved by the instructor, on cyber defense and security. This can either pertain to their
own corporate network, or similar topic. Each paper is to be no less than 10 pages in length,
double spaced, APA format, and is to include a cover, index, and reference area.
Casper College may collect samples of student work demonstrating achievement of the above outcomes. Any personally identifying information will be removed from student work.

**Required Text, Readings, and Materials:**
The book for this class is as follows:

**Class Policies: Last Date to Change to Audit Status or to Withdraw with a W Grade:**
The last date to withdraw from this course is **April 16, 2015**.
It is the expectation that you will attend all classes. If you are absent, it is your responsibility to obtain notes from fellow students, and keep abreast with the material. If you miss a quiz or exam, a makeup must be scheduled with the instructor no later than one week from the original testing date.

**Student Rights and Responsibilities:** Please refer to the Casper College Student Conduct and Judicial Code for information concerning your rights and responsibilities as a Casper College Student.

**Chain of Command:** If you have any problems with this class, you should first contact the instructor to attempt to solve the problem. If you are not satisfied with the solution offered by the instructor, you should then take the matter through the appropriate chain of command starting with the Department Head/Program Director, the Dean, and lastly the Vice President for Academic Affairs.

**Academic Dishonesty:** (Cheating & Plagiarism) Casper College demands intellectual honesty. Proven plagiarism or any form of dishonesty associated with the academic process can result in the offender failing the course in which the offense was committed or expulsion from school. See the Casper College Student Code of Conduct for more information on this topic.

**Official Means of Communication:** Casper College faculty and staff will employ the student's assigned Casper College email account as a primary method of communication. Students are responsible to check their account regularly. This is also, where you will find course evaluation links during course evaluation periods.

**ADA Accommodations Policy:** If you need academic accommodations because of a disability, please inform me as soon as possible. See me privately after class, or during my office hours. To request academic accommodations, students must first consult with the college’s Disability Services Counselor located in the Gateway Building, Room 344, (307) 268-2557, bheuer@caspercollege.edu. The Disability Services Counselor is responsible for reviewing documentation provided by students requesting accommodations, determining eligibility for accommodations, and helping students request and use appropriate accommodations.

**Calendar or schedule indicating course content:**
Week 1: January 19th: Chapter 1 “Introduction to Security”
Week 2: January 26th: Chapter 2 “Malware and Social Engineering Attacks”
Week 3: February 2nd: Chapter 3 “Application and Networking-Based Attacks”
Week 4: February 9th: Chapter 4 “Host, Application, and Data Security”
Week 5: February 16th: QUIZ 1! Chapter 5 “Basic Cryptography”
Week 6: February 23rd: Chapter 6 “Advanced Cryptography”
Week 7: March 2nd: Chapter 7 “Network Security Fundamentals”
Week 8: March 9th: MIDTERMS! Chapter 8 “Administering a Secure Network”
March 16 – 20: SPRING BREAK
Week 9: March 23rd: Chapter 9 “Wireless Network Security
Week 10: March 30th: Chapter 10 “Mobile Device Security”
Week 11: April 6th: QUIZ 2! Chapter 10 “Mobile Device Security” continued
Week 12: April 13th: Chapter 11 “Access Control Fundamentals”
Week 13: April 20th: Chapter 12 “Authentication and Account Management”
Week 14: April 27th: Chapter 13 “Business Continuity”
Week 15: May 4th: Chapter 14 “Vulnerability Assessment”
Week 16: May 11th: Written Final, and Submission of Final Project