CASPER COLLEGE COURSE SYLLABUS

CSEC 1510-N1 Network Defense Principles

Semester/Year: FALL/2104

Lecture Hours: 2	**Lab Hours**: 2	**Credit Hours**: 3
Class Time: Online	**Days:** S-S	**Room:** Your Own!

Instructor's Name: Eric Salveggio

Instructor's Contact Information: (c) 277-3918	**Office Phone:** (c) 277-3918	**Email:** ericsalveggio@caspercollege.edu

Office Hours: 5-9 M-F

Course Description: This course introduces students to the various methodologies used for attacking a network. Students are introduced to the concepts, principles and techniques, supplemented by hands-on exercises for attacking and disabling a network. These methodologies are presented within the context of properly securing the network. Students are provided with updated security resources that describe new vulnerabilities and innovative ways to protect networks by using the skills and tools of an ethical hacker.

Statement of Prerequisites: CSEC 1500

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 online discussion, online 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 one research paper, a midterm, one written, and one hands-on final in the simulator. **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:
Computer Security and Penetration Testing, 2nd edition. Basta and Basta, 2013. ISBN 9780840020932
All other material used within the class is found online at www.testout.com. Research material is found in any source the student chooses, with the exception of all Wiki-type sites.

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 **November 13, 2014.**
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:
As the online portion, in LabSim, is a pretty much a self-paced course, there are still mile-stones required, as follows;
Weeks 1 - 7: By the week of October 6: You should have progressed through Section 7 "Network Defenses"

Week 8: October 13 – Written Midterm
Week 15: By the week of December 1: Completion of the remainder of the LabSim course, and all three exam simulations

For the actual classroom, there are weekly discussions, and small projects:

Week 1: Chapter 1 – Ethics of Hacking and Cracking
Week 2: Chapter 2 – Reconnaissance
Week 3 – Chapters 3 & 4 – Scanning Tools and Sniffers
Week 4 – Chapter 5 - TCP/IP Vulnerabilities
Week 5 – Chapter 6 – Encryption and Password Settings
Week 6 – Chapters 7 & 8 – Spoofing and Session Hijacking
Week 7 – Chapter 9 – Hacking Network Devices
Week 8 – MIDTERMS – Chapter 10 – Trojan Horses
Week 9 – Chapters 11 and 12 – DoS Attacks, Buffer Overflows
Week 10 – Chapter 13 - Programming Exploits
Week 11 – Chapter 14 - Mail Vulnerabilities
Week 12 – Chapter 15 – Web Application Vulnerabilities
Week 13 – Chapter 16 – Windows Vulnerabilities
Week 14 – Chapter 17 – UNIX and Linux Vulnerabilities
Week 15 – Chapter 18 – Incident Handling
Week 16 – Finals and Final Projects