Syllabus: INT686 Network Security Firewalls

Instructor Information

Name   Keyu Jiang, Ph.D.
Department   Information Networking and Telecommunications
Contact information:   email:   kjiang@fhsu.edu
                        Phone:  785.628.4684
                        Fax:  785.628.4098
                        Web Site:  blackboard.fhsu.edu

Online Resources:
Please refer to https://sites.google.com/site/professorjiang/ia-links.

Virtual Labs:
Please refer to https://sites.google.com/site/professorjiang/ia-labs

Course Description:
This course focuses on network security concepts as they relate to the edge protection of an internetwork. Material covered will include: protocol-based security technologies, hardware-based firewall security appliances and their use with Authentication- Authorization-Accounting (AAA), and intrusion detection. Additionally, hardware-based security appliance Virtual Private Network configuration and implementation as well as firewall redundancy, maintenance and management will be covered.

PREREQUISITES:
INT685 or permit by instructor

REQUIRED LEARNING RESOURCES AND TEXTS:
Cisco Networking Academy – “Network Security II”
Access to the curriculum is provided online to students enrolled in the course.
No textbooks required.

COURSE ACTIVITIES:
Students in this course will study the Cisco Network Security II curriculum. Each chapter will have an associated formative assessment. Additional knowledge will be gained through hands-on laboratory exercises along with network simulation activities integrated into the on-line curriculum. Students will access NetLab with a network security pod consisting of routers, firewalls, and other devises to conduct laboratory exercises. Access to the FHSU Virtual Laboratory and NetLab is provided through directions you will find in Blackboard. For summative assessment, there will be one written Final Exam and one hands-on skills exam completed at the conclusion of the course.
Additional readings may be provided throughout the semester as supplemental information to the text. Any supplemental material provided has a potential of becoming lab exercise(s) and/or a quiz subject.

GRADING:

Assignments will be weighted in the following manner:
72 points - Chapter Quizzes
25 points - Final
3 points - Case Studies/Skills Exams/ Labs and Packet Tracer Activities
25 points – Research paper of Network Security (required for graduate students as described below)

For Graduate Students: You will be required to perform at a level significantly higher than that required of undergraduate students. Your work will be required to show mastery of the subject matter; your assignments will be require thorough research and demonstrate a comprehensive, synthetic viewpoint of the subject matter and original, important thought. Your assignments will be graded using higher standards than the standards used in grading upper division undergraduates taking this course.

Graduate students are required to write a research paper in network security. Papers should be at least 15 pages long, single spaced, 12 font of Time New Roman, in APA format with at least 15 references. The instructor reserves the right to require revisions to the paper. This is a required assignment for all students enrolled in graduate sections of this course. Failure to complete a satisfactory research paper will prevent the student from passing the course.

Final grades earned by each student will be based on the following scale:
A 90 - 100
B 80 - 89
C 70 - 79
D 60 - 69
F 0 - 59

ADDITIONAL INFORMATION / INSTRUCTIONS
Some additional readings included in the course schedule may require you to use the library's website as well. I also reserve the right to add or change readings during the course of this class. FHSU’s Blackboard system will serve as the backbone of this class. Since you have enrolled for this virtual course, I assume you are proficient enough with Blackboard to use it. If you are not, it is your responsibility to learn the login and navigation procedures of the Blackboard system. Please call 1-800-628-FHSU for technical support or e-mail support@fhsu.edu. As the instructor of this class, I have no technical expertise in Blackboard. Any technical questions should be directed to the Support staff, and not me.

ACCESSIBILITY
Fort Hays State University will ensure that no qualified person with a disability is denied the benefits of, excluded from participation in, or otherwise subjected to discrimination because of inaccessibility of education programs and activities operated by Fort Hays State University. To obtain information as to the existence and location of services, activities, and facilities that are accessible to persons with disabilities, contact the Director of Affirmative Action.

ACADEMIC HONESTY
Membership in the FHSU learning community imposes upon the student a variety of commitments, obligations and responsibilities. It is the policy of FHSU to impose sanctions on students who misrepresent their academic work. Classroom instructors will select appropriate sanctions or other designated persons consistent with the seriousness of the violation and related considerations.

Examples of academic dishonesty include but are not limited to: (1) Plagiarism, taking someone else’s intellectual work and presenting it as one’s own (which covers published and unpublished sources). Using another’s term paper as one’s own; handing in a paper purchased from an individual or agency; submitting papers from living group, club or organization files; or using another’s computer program or document are all examples of plagiarism. Standards of attribution and acknowledgment of literary indebtedness are set by each discipline. In political science, students must cite all work from which they take any recognizable length of work, including but not limited to phrases, sentences, and data. Students should consult with their department or with recognized handbooks in their field if in doubt. (2) Cheating is unacceptable in any form. Examples include consultation of books, library materials or notes during tests without the instructor’s permission; use of crib sheets or hidden notes; intentional observation of another student’s test; receipt of a copy of an exam or questions or answers from an exam to be given or in progress; substitution of another person for the student on an exam or another graded activity; deliberate falsification of lab results; submission of falsified data; alteration of exams or other academic exercises; and collaboration on projects where collaboration is forbidden. (3) Falsification, forgery or alteration of any documents pertaining to assignments and examinations. (4) Students who (cooperate or in other ways promote) participate in promoting cheating or plagiarism by others (or who take credit for the work of others) will also be in violation of this policy.

Students participating in any violation of this policy must accept the consequences of their actions. Classroom instructors and/or university review/appeals committees and administrators will assess the sanctions for violation of this policy. The seriousness of the violation will dictate the severity of the sanction imposed.

Academic sanctions may include but not be limited to any of the following: (a) verbal or written warning; (b) lowering of grade for assignment/activity; (c) lowering of term grade; (d) failure of class assignment. Administrative sanctions may include but not be limited to either of the following: (a) suspension from the University; (b) dismissal from the University. I take academic honesty as the bedrock of collegiate work, and I will not accept cheating in any way, shape, or form. My personal policy is to give students grades

of “U” (unsatisfactory, or fail) for both the assignment AND the course. Any incident of plagiarism is subject to the perpetrator’s immediately removal from class and failure.
Tentative Course Schedule:

Week 1 Account set up

Week 2 Familiar with Cisco Academy website and study tools

Week 3 Chapter 1: Intrusion Detection and Prevention Technology & Quiz

Week 4 Chapter 2: Configure Network Intrusion Detection and Prevention & Quiz

Week 5 Chapter 3: Encryption and VPN Technology & Quiz

Week 6 Chapter 4: Configure Site-to-Site VPN Using Pre-Shared Keys & Quiz

Week 7 Chapter 5: Configure Site-to-Site VPN Using Digital Certificates & Quiz

Week 8 Chapter 6: Configure Remote Access VPN & Quiz

Week 9 Chapter 7: Secure Network Architecture and Management & Quiz

Week 10 Chapter 8: PIX Security Appliance Contexts, Failover, and Management & Quiz

Week 11 Review chapter 1-8 & Final Exam

Week 12 Topic and Abstract of research paper Due

Week 13 Working on research and paper

Week 14 Draft paper due if requested by the instructor

Week 15 Final research paper due