Syllabus: INT685 Fundamentals of Network Security

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 is a course focusing on security concepts as they relate to internetworks, including: security policy design and management, security technologies and solutions, firewalls, hands-on implementation using firewalls, Authentication-Authorization-Accounting (AAA), and secure VPNs.

This course focuses on the overall security processes in a network with particular emphasis on hands-on skills in the following areas:

- Security policy design and management
- Security technologies, products, and solutions
- Firewall and secure router design, installation, configuration, and maintenance
- AAA implementation using routers and firewalls
- Securing the network at both routers and firewalls

This course is intended to introduce a variety of network security theories and technologies. Upon completion of this course students will be able to complete the following objectives:

- Explain the basic concepts of network security
- Explain the common network protection and management techniques
- Identify the security devices manager
- Explain PIX Security Appliance translations and connections
- Explain AAA
- Identify and describe network Admission control (NAC)
- Operate the configuration RADIUS and TACACS+ with Cisco Secure ACS
• Explain the Cisco IOS Firewall authentication proxy
• Configure 802.1x port-based authentication
• Configure Cisco IOS Firewall Context Based Access Control
• Configure ACLs and content filters
• Configure a Security Appliance modular policy
• Explain MAC address, ARP, and DHCP vulnerabilities

**PREREQUISITES:**

INT293 Internetworking III  
Or CCNA curriculum 1-4

**REQUIRED LEARNING RESOURCES AND TEXTS:**

Cisco Networking Academy – “Network Security I”  
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 I 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 devices 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:
70% - Chapter Quizzes  
25% - Final  
5% - Case Studies/Skills Exams/ Labs and Packet Tracer Activities

Final grades earned by each student will be based on the following scale:
A 90 - 100  
B 80 - 89  
C 70 - 79
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 mailto: 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: Vulnerabilities, Threats, and Attacks & Quiz

**Week 4** Chapter 2: Security Planning and Policy & Quiz

**Week 5** Chapter 3: Security Devices & Quiz

**Week 6** Chapter 4: Trust and Identity Technology & Quiz

**Week 7** Review chapter 1-4

**Week 8** Chapter 5: Cisco Secure Access Control Server & Quiz

**Week 9** Chapter 6: Configure Trust and Identity at Layer 3 & Quiz

**Week 10** Chapter 7: Configure Trust and Identity at Layer 2 & Quiz

**Week 11** Review Chapter 5-7

**Week 12** Chapter 8: Configure Filtering on a Router & Quiz

**Week 13** Fall Break

**Week 14** Chapter 9: Configure Filtering on a PIX Security Appliance & Quiz

**Week 15** Chapter 10: Configure Filtering on a Switch & Quiz

**Week 16** Review chapter 8-10

**Week 17** Final Exam