JOHN A. LOGAN COLLEGE
COURSE SYLLABUS

General Information

Course: CIS 231-Firewalls & VPN's
IAI No: None
Section:
Time:
Room:
Credit Hours: 3
Lecture Hours: 2
Lab Hours: 2

Instructor Information

Name:
Office:
Office Hours:

Monday	
Tuesday	
Wednesday	
Thursday	
Friday	

Phone:
Email:

Course Textbook & Materials

Michael E. Whitman, Herbert J. Mattord, and Andrew Green, *Guide to Firewalls and VPNs, Third Edition*. Course Technology, Cengage Learning, 2012, ISBN-13 978-1-111-13539-3.

Course Prerequisites

CIS 230 or taking CIS 230 concurrently.

Course Description

This course examines the major network security tools in use today, with the idea that firewalls are most effective when backed by thoughtful security planning, well-designed security policies, and integrated support from anti-virus software, intrusion detection

systems, and related tools. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The course will provide numerous realistic projects and cases incorporating cutting-edge technology and current trends, giving students the opportunity to hone and apply the knowledge and skills they will need as working professionals. Students will also learn about relevant National Institute of Standards and Technology guidelines that are used by businesses and information technology professionals.

Course Objectives

- Explain the component parts of information security in general and network security in particular.
- Define the key terms and critical concepts of information and network security
- Define information security policy and describe its central role in implementing a successful information security program
- Explain the three types of information security policy and list the critical components of each
- Design the network topology when given a specific scenario.
- Define management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
- Explain why authentication is a critical aspect of perimeter defense
- Explain why firewalls authenticate and how they identify users
- Identify common misconceptions about firewalls
- Explain why a firewall is dependent on an effective security policy
- Understand what a firewall does
- Describe packets and packet filtering
- Explain the approaches to packet filtering
- Configure specific filtering rules based on business needs
- Describe why good human machine interfaces are important to system use.
- Demonstrate the interaction between security and system usability.
- Understand the importance of minimizing the effects of security mechanisms.
- Describe the role encryption plays in firewall and VPN architectures
- Explain how digital certificates work and why they are important security tools
- Define the principles of cybersecurity.
- Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies.
- Analyze common security failures and identify specific design principles that have been violated.
- Given a specific scenario, identify the design principles involved or needed.
- Understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms.

College-Wide Student Learning Outcomes

The faculty and staff of John A. Logan College are committed to providing students with opportunities to develop learning abilities that will last a lifetime. Graduates will be prepared to succeed in their personal and professional lives because of achieved competence in the following student learning outcomes. In this course, students will be assessed in the following learning outcome:

	Communication: Students express thoughts, ideas, and feelings in both written and oral modes.
	Critical Thinking: Students apply a rational and methodical approach to problem solving based on use of appropriate evidence.
	Cultural and Global Awareness: Students demonstrate an understanding of the influence of culture and society.
	Information Literacy: Students locate, evaluate, retrieve, organize, create, and disseminate information.
	Quantitative Reasoning: Students use and understand numbers to interpret, evaluate, and express information in quantitative terms.

Topic Outline

- Introduction to Information Security
- Security Policies and Standards
- Authenticating Users
- Introduction to Firewalls
- Packet Filtering
- Firewall Configuration and Administration
- Working with Proxy Servers and Application-Level Firewalls
- Implementing the Bastion Host
- Encryption – The Foundation for the Virtual Private Network
- Setting Up a Virtual Private Network

Tentative Course Schedule

Week Starting:	Chapter	Assignment
Week 1	Lab Setup	Lab Set up
Week 2	Chapter 1	Chapter Quiz Labs: Set up software firewalls on Windows PC
Week 3	Chapter 2	Chapter Quiz Labs: Use software firewalls to block/open ports after reviewing ports

		(KU Cybersecurity Principles Outcome 5)
Week 4	Chapter 3	Chapter Quiz Labs: Software firewalls for logging/troubleshooting and analyzing user logs Homework: Principles of cybersecurity (KU cybersecurity Outcome 1)
Week 5	Chapter 4	Chapter Quiz Labs: Cisco Packet Tracer (ASA_acl_nat) and (asa_clientless_vpn)
Week 6	Chapter 5	Chapter Quiz Labs: Cisco Packet Tracer (asa_service_policy) and (enable outside to inside)
Week 7		Project 1: Cisco Packet Tracer analyze network and report failures, identify principles used to create network and design (KU Cybersecurity Principles Outcome 3)
Week 8	Midterm	Exam 1
Week 9	Chapter 6	Chapter Quiz Labs: Install pfsense and user PC network together Interfaces, VLANS, Zones, DHCP/Static
Week 10	Chapter 7	Chapter Quiz Labs: Pfsense rules, policies, user accounts/role based, content filtering
Week 11	Chapter 8	Chapter Quiz Labs: Pfsense adding Plugins (Suricata), IDS/IPS, traffic shaping, logging
Week 12	Chapter 9	Chapter Quiz Labs: PfSense VPN (openvpn)
Week 13	Chapter 10	Chapter Quiz

		Labs: Palo Alto Lab user accounts, networking, rules web vs cli
Week 14		Labs: Palo Alto content filtering, logs, IDS/IPS, Wildfire
Week 15		Project 2: Pfsense project combining networks and previous labs knowledge and write a paper explain the security principles required and how they were implemented (KU Cybersecurity Principles outcome 2 and 4)
Week 16	Exam 2	Exam 2
Finals	Final	Final

Method of Presentation

In Class Lectures, Labs and Hands on

Method of Evaluation

Quizzes: There will be a quiz after each chapter there will be a total of 10 quizzes. Each Quiz will be worth 20 points.

Exam: There will be two exams in this class, the first one will cover chapters 1-5, the second one will cover chapters 6-10 and the final will cover all 7 parts. Each exam will be worth 100 points. **You will be required to take the final exam if you miss Exam 1 or Exam 2.**

Labs/Class Work: These may not be made up and are completed in class during the semester. They will add up to 400 points.

Final exam: If a student misses' exam 1 or 2 they will be required to take the final. The final is worth 100 points and will cover chapters 1-10.

Project: There is 2 major projects in this class worth 100 points.

Quizzes: 10 Quizzes @ 20 points each	200 Points
Exams: 2 @ 100 points	200 Points
Labs/Class Work	400 Points
Project: 2 @ 100 points	200 Points

Total Points	**1000 Points**

Grading Scale:
A – 90% - 100%
B – 80% – 89%
C – 70% - 79%
D – 60% – 69%
F – 0% – 59%

Specific Course Requirements

The student is required to read and study the textbook material. Students are responsible for all discussion, assignments, and announcements posted on the course Web site.

No work may be turned in late

Class Conduct:

Student Responsibilities: The student is required to read and study the textbook materials. Students are responsible for all discussions, assignments, and announcements made in class and posted on the course Web site. Note: All inquiries/questions should be directed to the instructor via email. There is a response time of 24 hours 8am Monday – 4pm Friday. A 48-hour response time 4pm Friday – 8am Monday. Both the instructor and students will observe this. **THE ONLY EMAIL ADDRESS THAT I WILL RESPOND TO IS THE VOLMAIL ACCOUNT THAT THE COLLEGE SET UP FOR YOU. I WILL NOT RESPOND TO HOTMAIL, YAHOO, GMAIL, OR ANY OTHER EMAIL ACCOUNTS.**

Students are to behave in a respectful manner while in the classroom. Respect should be given to the classroom instructor, classmates, and classroom activities. Students should not engage in activities that will distract from the learning environment. Therefore, the following conduct must be followed:

- Students are to give the instructor/presenter their full attention during presentations.
- Students should not be working on anything other than class material during class time.
- Students should not be surfing the Internet, checking e-mail, instant messaging, playing games, etc., during class time.
- Personal electronic device activity such as: cell phones, lap tops, PDA's, Ipods, etc., are not permitted in the classroom without prior permission.
- Software should not be disabled on classroom computers.

Cell Phones: No talking, texting, or Internet use on cell phones will be permitted in the classroom without instructor permission or you may be asked to leave if it happens twice you will lose 1/2 points on Exam (50 points). If you are expecting a phone call

place your phone on vibrate, if it vibrates you will not lose the points, please go outside the classroom before you begin talking.

If, during lab time, all assigned class work has been completed and submitted for grading, the students may engage in other school related activities while in the computer lab. However, under NO circumstances should a student be doing anything other than what the instructor is presenting during lectures.

If students engage in activities contrary to the above, the following procedures will be adhered to:

1. First offense – students will be warned and counted absent for the day.
2. Second offense – students will be asked to leave the classroom with no questions asked and will be counted absent for the day.
3. Third offense – students will be asked to leave the classroom, will be counted absent for the day, and will not be allowed back until they have met with the department chair. Students could, at this time, be subject to expulsion from the class.

Additional College Information and Resources

Please see the JALC Syllabus Attachment