LAGUARDIA COMMUNITY COLLEGE
CITY UNIVERSITY OF NEW YORK
DEPARTMENT OF MATHEMATICS, ENGINEERING, AND COMPUTER SCIENCE

MAC 246 – ADVANCED NETWORK SECURITY

4 hours (2h lecture, 2h lab), 3 credits
Prerequisite: MAC245 – DATA COMMUNICATION AND NETWORK SECURITY

Instructor:
Contact:
Office:
Office hours:

Description

This course covers a wide variety of security topics such as threats, vulnerabilities, data and host security, access control, identity management, cryptography, attacks and defense mechanisms. Security policies and procedures will also be covered. Additional topics include firewalls, VPNs, NAC, switch and router security, intrusion detection and prevention, malware, file security and data defenses. The course will prepare students for the CompTIA Security + Exam.

Instructional Objectives:

1. Introduce students to security challenges, access control models, authentication and authorization.
2. Introduce students to malware and social engineering attacks, network authentication and identity management.
3. Familiarize students with physical security and hardware security.
4. Introduce common network protocols and different network applications.
5. Provide students with the principles of denial of service, DNS attacks, firewalls, and VPNs.
6. Familiarize students with malware, password attacks and file server security.
7. Familiarize students with web application attacks and Internet browsers, wireless network security attacks, vulnerabilities and solutions.
8. Introduce students to data defenses, redundancy, back-up and restore, and file encryption.
9. Familiarize students with assessment and audit techniques. penetration testing, protocol analysis, audits and log management.
10. Provide students with real-world or simulated examples of network setup, management and security provisions.

Performance Objectives:

1. Identify types of security challenges and access control models; illustrate authentication and authorization techniques.
2. Define malware, network authentication and identity management; illustrate social engineering attacks.
3. Compare and contrast physical security and hardware security.
4. Identify the security principles and techniques required to secure a network infrastructure.
5. Describe and illustrate denial of service and DNS attacks; define firewalls and VPNs.
6. Explain malware, password attacks, and file server security.
7. Describe web application attacks, Internet browsers and wireless security attacks; illustrate vulnerabilities and solutions.
8. Illustrate data defenses, redundancy, back-up and restore and file encryption.
9. Illustrate different assessment and audit techniques; explain penetration testing, protocol analysis and log management.
10. Apply skills learned in previous courses and in this course to configure a network and implement security measures and policies; communicate the results digitally. a

Required Textbook :

Ciampa, Mark, *CompTIA Security+ Guide to Network Security Fundamentals*, Cengage Learning, 5th Ed. August 2014
ISBN: 978-1305093911

Grading Standards:

Project		10%
Assignments	(5 @3% each)	15%
Laboratory	(10 @2% each)	20%
Midterm Exam		25%
Final Exam		30%
Total		100%

Comments:

The grading standards listed above and the suggested homework problems listed in the course outline are both subject to modification by the instructor.

Course Outline

Week 1
Introduction to security: challenges, terminology and access control models.
Lab 1: Set-up and introduction to course software

Week 2
Threats: malware, social engineering attacks, application attacks, networking authentication and identity management.
Lab 2: Identifying threats; and mitigating threats
HW1
Digital project discussion

Week 3
Threats: malware, social engineering attacks, application attacks, networking authentication and identity management (continued).
Lab 3: Identifying threats; and mitigating threats (continued)

Week 4
Different policies and procedures, manageable network plans, risk management and incident response.
Lab 4: Devising a plan for assessing risk
HW2

Week 5
Physical security, tailgating and piggybacking, breaking into a system.
Lab 5: Physical security

Week 6
Cryptography: definition, algorithms, usage, and encryption.
Lab 6: Securing data; implementing different encryption techniques
HW3

Week 7
Denial of service, DNS attacks, firewalls.
Lab 7: Midterm exam

Week 8
Virtual Private Networks (VPNs).
Lab 8: Denial of service, setting up a firewall
HW4

Week 9
Securing network devices, switches, routers and switch administration principles, malware and file server security.
Lab 9: Securing the network; identifying threats in the network

Week 10
Web application attacks and Internet browsers, wireless network security, attacks, vulnerabilities, solutions.
Lab 10: Attacks in wireless networks, assigning roles to prevent unauthorized users
HW5

Week 11
Data defenses, redundancy, back-up and restore and file encryption.
Lab 11: Back-ups
Digital project due

Week 12
Assessment and audit techniques, penetration testing, protocol analysis, audits, and log management.
Lab 12: Penetration testing; assessing threats
Review final

Week 13
Final examination

Note: Your labs will be graded according the following rubric:

1	2	3	4	5
The student cannot set up the experiment correctly.	The student can set up the physical environment for the experiment but cannot execute it.	The student sets up the experiment correctly but configures it incorrectly.	The student sets up the experiment well, runs it well, but does not comprehend the results and cannot relate the meaning of what he or she has accomplished. Essentially, they followed the recipe but show a lack of	The student successfully sets up and runs the experiment, documents his or her results and shows a clear understanding of the process.

			understanding.	

Letter Grade Assignment

Final grades assigned for this course will be based on the percentage of total points earned and are assigned as follows:

Letter Grade	Percentage	Performance
A	91-100%	Excellent Work
A-	87-90%	Nearly Excellent Work
B+	84-86%	Very Good Work
B	81-83%	Good Work
B-	78-82%	Mostly Good Work
C+	75-77%	Above Average Work
C	72-74%	Average Work
C-	69-71%	Mostly Average Work
D+	66-68%	Below Average Work
D	60-65%	Poor Work
F	0-59%	Failing Work

Course Policies

Attendance

Students are expected to attend all class sessions as listed on the course calendar. The maximum number of unexcused absences allowed is 15% of the total class meetings (about 7 hours). Unexcused absences beyond this maximum will result in a grade of WU or F.

Late Work Policy

Be sure to pay close attention to deadlines—there will be no makeup assignments or quizzes, or

late work accepted without a serious and compelling reason and instructor approval.

Most online activities will have an automated deadline. Past the due date the activities will not be visible on Blackboard.

For handed on assignments, there will be 20% reduction of the grade for every three days late. The assignment won't be accepted after one week late.

Understand When You May Drop This Course

It is the student's responsibility to understand when they need to consider drop from a course. Refer to the official calendar at LaGuardia's website.

Incomplete Policy

The INC (incomplete) grade will be given to **ONLY** students who pass both midterm and final exams and did not complete lab work, or special emergency cases with a prior agreement of the instructor. All incomplete course assignments must be completed within one semester otherwise the grade will turn into F.

Inform Your Instructor of Any Accommodations Needed

If you have a documented disability, and wish to discuss academic accommodations, please contact your instructor as soon as possible. It is the student's responsibility to provide documentation of disability to the office for Students with Disabilities (OSD) at LaGuardia Community College. For more information visit: www.lagcc.cuny.edu/osd

Commit to Integrity

As a student in this course (and at this college) you are expected to maintain high degrees of professionalism, commitment to active learning and participation in this class and also integrity in your behavior in and out of the classroom.

LaGuardia Community College Academic Honesty Policy & Procedures

Cheating and plagiarism are extremely serious offenses in all academic areas (consult the College's Catalog for the **definition** of Academic Dishonesty). **Any form of academic dishonesty, including cheating and plagiarism, may be reported to the office of student affairs**