LAGUARDIA COMMUNITY COLLEGE
CITY UNIVERSITY OF NEW YORK
MAC247: Advanced Systems Security
3 Credits, 4 hours (Lecture – 2 hours, Lab – 2hours)

Course Description

Advanced Systems Security course presents advanced topics of systems security. Topics covered in this course include, access controls, asset management, security controls, change management, patch management, risk management, security assessment activities, monitoring systems, network monitoring and control, secure device management, network-based security devices, endpoint device security, big data access control and application vulnerabilities, software-defined networks, and clustering.

Prerequisite – MAC237

Textbooks

"Systems security Certified Practitioner Official Study Guide" by George B. Murphy. Publisher: Sybex, A Wiley Brand, ISBN: 9781119059653

Instructional Objectives

1. Reinforce students' knowledge of access controls, authentication mechanisms, identity-management life cycle.
2. Introduce students to basic security concepts, CIA triad, assess compliance with controls, asset management.
3. Familiarize students with different document and operate security controls, change management, security impact assessment, security awareness.
4. Introduce students to risk management, risk visibility, risk assessment, risk treatment, risk calculation, threat vectors and threat likelihood.
5. Provide the student with an understanding of security assessment activities, security testing and evaluation, security policy training and procedures.
6. Familiarize students with monitoring systems, analyze monitoring results, security analytics, metrics and trends.
7. Reinforce students' knowledge of cryptography, public key cryptography, key management, network and communications security, network monitoring and control, network-based security devices, and secure device management.

8. Introduce students to endpoint device security, trusted platform module, mobile device management.
9. Familiarize students with cloud security, cloud privacy concerns, big data, big data access control and application vulnerabilities, software-defined networks, hypervisor, security benefits and challenges of virtualization.

Performance Objectives

Upon completion of this course students should:

1. Illustrate in depth understanding of access controls, authentication mechanisms, identity-management life cycle.
2. Explain basic security concepts, CIA triad, assess compliance with controls, asset management.
3. Identify different document and operate security controls, change management, security impact assessment, security awareness.
4. Define risk management, risk visibility, risk assessment, risk treatment, risk calculation, threat vectors and threat likelihood.
5. Illustrate security assessment activities, security testing and evaluation, security policy training and procedures.
6. Explain monitoring systems, analyze monitoring results, security analytics, metrics and trends.
7. Explain cryptography, public key cryptography, key management, network and communications security, network monitoring and control, network-based security devices, and secure device management.
8. Identify endpoint device security, trusted platform module, mobile device management.
9. Explain cloud security, cloud privacy concerns, big data, big data access control and application vulnerabilities, software-defined networks, hypervisor, security benefits and challenges of virtualization.

Grading Guidelines

A-, A	90-100
B-, B, B+	80-89
C-, C, C+	70 – 79
D-, D, D+	60 – 69
F	Below 60
WU	Unofficial Withdrawal (Students who have stopped attending at any time before the final exam week, and did not officially withdraw will receive this grade)

Grading Standards

CATEGORY	PERCENTAGE
HomeWorks (4 @ 5% each)	20%
Labs (5@4% each)	20%
Midterm Exam (2 @ 10% each)	20%
Project	15%
Final Exam	25%
Total	**100%**

ACADEMIC INTEGRITY

This class will be conducted in compliance with LaGuardia Community College's academic integrity policy.

ATTENDANCE

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.

COMMENTS

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

For more details about the academic requirements and grading policy, see the following link: https://www.laguardia.edu/uploadedFiles/Main_Site/Content/Academics/Catalog/PDFs/AcademicRequirementsAndPolicies.pdf

Weekly Topics

Week	Lecture Topics	Labs
1	Access Controls basics: authentication mechanisms, internetwork trust architectures, subject based and object-based access controls. Identity-Management Life cycle – Proofing, Provisioning, Maintenance, Entitlement.	Homework 1 - Authentication mechanisms, access controls.
2	Basics of Security Concepts: CIA triad, Least privilege, Separation of duties. Implement and Assess Compliance with Controls – technical, operational and managerial controls. Asset Management.	Project Discussion
3	Document and Operate Security Controls: Deterrent, Preventive, Detective, Corrective, Compensating controls. Change Management: Configuration Management Plan, Security impact assessment, interoperability of systems, testing and implementing patches, fixes and updates of operating system, applications, SDLC. Security awareness and Physical security operations.	Lab 1 - Security controls, Patch Management.
4	Risk Management basics: Risk visibility and reporting, risk assessment and management. Risk treatment – accept, transfer, mitigate, avoid. Audit findings, Risk Calculation, Threat Vectors, Threat Likelihood.	Homework 2 - Risk analysis, Risk management.
5	Security assessment activities – security testing and evaluation, interpretation and reporting of scanning and testing results. Security Policy training and procedures.	Lab 2 - security testing and evaluation. Midterm Exam
6	Monitoring Systems – passive, active and real-time monitoring. Analyze Monitoring Results – security analytics, metrics and trends, visualization, event data analysis, communicate findings.	Lab 3 - Monitoring and Analyze monitoring results.
7	Cryptography basics. Requirements of Cryptography – Data sensitivity, Regulatory requirements, End-User training. Key management concepts- key composition, key creation, exchange, revocation and escrow.	Lab 4 - Public key cryptography, Key management.

8	Basics of Network and communications Security – Models, Ports and Protocols. Converged Network Communications, Network Monitoring and Control. Access Control Protocols and Standards, Remote and Local user authentication services. Secure Device Management, Network-Based Security Devices.	Lab 5 - Network Monitoring, Security devices.
9	Endpoint Device Security – HIDS, Trusted platform module, Mobile device management.	Project Status Update
10	Cloud Model basics, Cloud Security, Cloud Legal and Privacy Concerns, Cloud Virtualization Security.	Homework 3 - Cloud Security. Midterm Exam 2
11	Data Warehouse and Big Data. Securing data warehouse. Big Data deployment and operations, Big Data access control and application vulnerabilities.	Homework 4 - Big data operations and vulnerabilities. Project Due.
12	Software-defined networks, Clustering, Security benefits and Challenges of Virtualization, Hypervisor, Attacks and countermeasures.	Review
13	Final Exam	