ST: ST: MIS-4140-12155.201810-Information Security Lab

Winter 2018

General Course Information

Instructor: Mazyar Sahabi
Office: TBA
Office Hours: TBA
E-mail: sahabi@oakland.edu
Web site:
Classroom: Main Campus Elliot Hall 200
Class Times: Wed 6:30-9:30
Prerequisites: Undergraduate level MIS 300 Minimum Grade of 2.0 and Undergraduate level MIS 305 Minimum Grade of 2.0

Textbook: Mark Ciampa, *Security+ Guide to Network Security Fundamentals, Fifth Edition*. Course Technology, Cengage Learning, 2015, ISBN 13: 9781305093911

Lab Manual (ISBN-10: 1111640130 | ISBN-13: 9781111640132)

Course Objectives
This course offers a comprehensive guide for anyone wishing to take the CompTIA Security+ SY0-401 Certification Exam. It provides an introduction to the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The course covers new topics in network security as well, including psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security. Students will also engage in activities that link to the Information Security Community Site.

Specific topic coverage includes:

- Introduction to Security
- Malware and Social Engineering Attacks
- Application and Network Attacks
- Vulnerability Assessment and Mitigating Attacks
- Host, Application, and Data Security
- Network Security
- Administering a Secure Network
- Wireless Network Security
- Access Control Fundamentals
- Authentication and Account Management
- Basic Cryptography
- Advanced Cryptography
- Business Continuity
- Risk Mitigation

Web Site

SANS.org

http://www.nationalccdc.org/

E-Mail

All students are requested to obtain an e-mail account. If you have any questions about the course or need assistance. Also, you may submit the end-of-chapter case project assignments in class on the due date or by e-mail with a date stamp at or before 5:00 P.M. on the due date. E-mail submissions should be submitted as an attachment in Microsoft Word format.

Grading and Evaluation Criteria

40% of the grade is based on a midterm and a final examination. Both examinations are cumulative and given in a varied format. An in-class review will be held prior to each examination.

40% of the grade is based on labs which will be assigned by the instructor. This course is designed to be very hands on.

5% of the grade is based on a project, which will be assigned by the instructor.

5% of the grade is based on assignments. These are selected cases at the end of each chapter.

10% of the grade is based on quizzes.

- Course Grade Determination

Labs	40%
Midterm	20%
Final	20%
Project	5%
Assignments	5%
Quizzes	10%

All the lab works must be submitted by due date, no exception.

14-Week Course Outline

Week	Topics	Chapter Readings	Exams
1	Introduction to Security	Chapter 1	
2	Malware and Social Engineering Attacks .	Chapter 2	
3	Application and Networking-Based Attacks	Chapter 3	Quiz 1
4	Host, Application, and Data Security	Chapter 4	
5	Basic Cryptography	Chapter 5	
6	Advanced Cryptography	Chapter 6	
7	Network Security Fundamentals	Chapter 7	Midterm Exam
8	Administering a Secure Network	Chapter 8	
9	Wireless Network Security.	Chapter 9	
10	Mobile Device Security.	Chapter 10	
11	Access Control Fundamentals.	Chapter 11	Quiz 2
12	Authentication and Account Management	Chapter 12	
13	Business Continuity	Chapter 13	
14	Risk Mitigation Vulnerability Assessment	Chapter 14 Chapter 15	Final Exam