Philadelphia University
Faculty of Administrative & Financial Sciences
Department of Business Networking and Systems Management

Course Syllabus	
Course Title: Information Security & Confidentiality	**Course code: 0371327**
Course Level: Third Year	**Course prerequisite(s) and/or co-requisite(s): Advanced Programming (2) 0371212**
Lecture Time: 09:10-10:00 (Sun, Tue, Thu).	**Credit hours: (3) hours**

Academic Staff Specifics

Name	Rank	Office Number/Location, and Office Phone Number	Office Hours	E-mail Address
Dr. Hussein H. Owaied Al-Shemery	Ph.D.	32422 / Second Building Ext: 2631	10:00-12:00 (Sun,Tue,Thu) 9:45-11:00 (Mon, Wed)	hshemery@philadelphia.edu.jo

Course Description:

Knowledge and skills required for Network Administrators and Information Technology professionals to be aware of security vulnerabilities, to implement security measures, to analyze an existing network environment in consideration of known security threats or risks, to defend against attacks or viruses, and to ensure data privacy and integrity. Terminology and procedures for implementation and configuration of security, including access control, authorization, encryption, packet filters, firewalls, and Virtual Private Networks (VPNs). Students will also learn how hackers attack computers and networks, and how to protect systems from such attacks, using both Windows and Linux systems. Students will learn legal restrictions and ethical guidelines, and will be required to obey them. Students will perform many hands-on labs, both attacking and defending, using port scans, footprinting, exploiting Windows and Linux vulnerabilities, buffer overflow exploits, SQL injection, privilege escalation, Trojans, and backdoors.

Course Objectives:

- Define areas of security concern, discuss network security, and identify network risks.
- Explain what an ethical hacker can and cannot do legally, and explain the credentials and roles of penetration testers.
- Distinguish between and define internal and external threats to data and services.
- Describe the vulnerabilities of various media (susceptibility to wiretaps or eavesdropping).
- Define the types of malicious software found in modern networks.
- Secure access to resources on the network using passwords, permissions, and access control lists (ACLs).
- Explain the threats and countermeasures for physical security and social engineering.
- Evaluate various anti-virus software programs, software firewalls, and hardware firewalls.
- Define and identify types of firewalls, including Network Address Translation (NAT).
- Discuss weaknesses of various operating systems and known and recommended fixes (patches).
- Detect unauthorized attempts to access resources by monitoring (auditing).
- Install and configure intrusion detection programs; analyze reports and recommend responses.
- Provide solutions for known vulnerabilities in communications: email, remote access, file transfer, and electronic commerce.
- Provide end-to-end security for the transmission of data between hosts on the network.
- Describe vulnerabilities inherent in wireless technologies and present suggested solutions.
- Describe how to take control of Web Servers, and how to protect them.
- Explain how cryptography and hashing work, and perform attacks against them such as password cracking and man-in-the-middle attacks.

Course Components

- **Books**

  Text book:

  Security+ Guide to Network Security Fundamentals, 4th Edition, 2012.
  Authors: Mark Ciampa
  Publisher: Course Technology.
  Year of Publication: 2012

  In addition to the above, the students will be provided with handouts by the lecturer.

Teaching methods:

- Lectures.
- Discussion groups.
- Tutorials.
- Debates.
- Homework’s.
- Basic Research/Presentation.

Learning Outcomes:

- **Knowledge and understanding:**
  The data show is used to demonstrate practical exercise in the class to enable students see how it is done to save time and make lecture effective.

- **Cognitive skills (thinking and analysis).**
  - The lecturer will present the material in the text book in an interactive way that stimulates the thinking side of students.
  - Conducting the learning objectives for each module components in clear manner to insure the material is digested by the students.

- **Communication skills (personal and academic).**
  - For every lecture the last five minutes will be open for discussion. For further discussion, the students are welcome at the lecturer's office hour as appeared in first page.
  - Project Development: Groups of approximately two to three students develop projects, complete research, schedule meetings, write papers and reports, and deliver a 20-30 minute oral presentation using visual aids.
  - Group Management: Students work on group projects to practice interpersonal skills by communicating with group members, other groups, and peers outside the group.

Assessment instruments

- Short Reports and/or Presentations and/or Short Research Projects.
- Quizzes.
- Home works.
- Final examination.

Allocation of Marks		
Assessment Instruments	**Mark**	**Exam Date and Day**
First Examination	**20**	
Second Examination	**20**	
Final Examination	**40**	
Attendance, Quizzes, Home works, and Reports and/or Research	**20**	
Total	**100**	

Documentation and academic honesty

This course is given from the textbook mentioned above. It is copyright protected. Students are encouraged to purchase this textbook from the university bookshop.

Definition of Plagiarism

Plagiarism is the unacknowledged borrowing of another writer's words or ideas.

How Can Students Avoid Plagiarism?

To avoid plagiarism, you must give credit whenever you use

- another person's idea, opinion, or theory;

- any facts, statistics, graphs, drawings—any pieces of information—that are not common knowledge;
- quotations of another person’s actual spoken or written words; or
- Paraphrase of another person’s spoken or written words.

If you are in doubt about whether what you are doing is inappropriate, consult your instructor. **A claim that “you didn’t know it was wrong” will not be accepted as an excuse.**

Penalty for Plagiarism

The minimum penalty for an act of plagiarism is a 0 on the assignment, homework, and project. Serious cases of plagiarism may result in failure in the course as a whole, or expulsion from the university.

Course Academic Calendar

Week	Basic and support material to be covered	Homework/reports and their due dates
(1)	Introduction to Security	
(2)	Malware and Social Engineering Attacks	
(3)	Application and Network Attacks	
(4)		
(5)	Vulnerability Assessment and Mitigating Attacks	
(6) **First Examination**		**First Examination**
(7)	Host, Application, and Data Security	
(8)		
(9)	Network Security	
(10)		
(11) **Second Examination**	Access Control Fundamentals	**Second Examination**
(12)		
(13)	Authentication and Account Management	
(14)	Basic Cryptography	
(15)		
(16) **Final Examination**	Comprehensive review for all the topics learned in the whole semester to resolve obstacles that may appear while studying.	**Final Examination**

Expected Workload:

On average students need to spend 2 hours of study and preparation for each 50-minute lecture/tutorial.

Attendance Policy:

Absence from lectures and/or tutorials shall not exceed 15%. Students who exceed the 15% limit without a medical or emergency excuse acceptable to and approved by the Dean of the relevant college/faculty shall not be allowed to take the final examination and shall receive a mark of zero for the course. If the excuse is approved by the Dean, the student shall be considered to have withdrawn from the course.