QFO-AP-FI-MO02	اسم النموذج: Course Syllabus	جامعة فيلادلفيا Philadelphia University
رقم الاصدار : 1 (Revision)	الجهة المصدرة: كلية تكنولوجيا المعلومات	
التاريخ :2017/11/05	الجهة المدققة: عمادة التطوير والجودة	
عدد صفحات النموذج:		

Course Title: Information Security **Course level:** 4 **Lecture time:**	**Course code:** 0750446 **Course prerequisite:** 0731340 **Credit hours:** 3

Academic Staff Specifics

Name	Rank	Office Number and Location	Office Hours	e-mail Address
		IT building		

Course description: This course is based on the textbook SECURITY+ GUIDE TO NETWOK SECURITY FUNDAMENTALS, Fourth Edition. It is not a course in cryptography. In addition to fundamentals, it takes an in-depth and comprehensive view of security by examining the attacks that are launched against networks and computer systems, the necessary defense mechanisms, and offers end-user practical tools and techniques to counter attacks. For a summary of the topics covered in each chapter, consult the textbook.

Textbooks and Supporting Material:
1-Network security essentials : applications and standards, William Stallings, Harlow: Pearson Education Limited, 2014.

2- Information security and cyber laws, Sanjeev Puri, New Delhi: Technical Publications, 2014

Teaching methods: lectures, tutorials, lab work, discussion groups.

Learning Outcomes:

A. Knowledge and Understanding

A1. Define authentication services, List the account management procedures for securing passwords, Describe relevant cryptography algorithms and list the various ways in which cryptography is used, Define digital certificates, Describe the components of Public Key Infrastructure and describe the different transport encryption algorithms.

A2. List the steps for securing a host computer, Define application security and explain how to secure data using data loss prevention, List the different types of network security devices

and explain how they can be used.

A3. Explain how to enhance security through network design, Explain how network administration principles can be applied, Define the new types of network applications and how they can be secured, Explain the solutions for securing a wireless network. Define access control and various control models.

A5. Describe the challenges of securing information attacks, Identify the types of attackers, List various techniques for mitigating and deterring attacks.

B. Intellectual skills

B1. Analyse relevant features of Web application and compare them with those relevant to client-side attacks.
B2. Compare techniques and tools used in vulnerability assessment.
B3. Carry out appropriate procedures to establish host security.
B4. Model and analyse various types of attacks.

C. Practical skills

C1. Apply relevant security principles to hosts, applications, and networks.
C2. Implement secure network administration principles.

D. Transferable Skills and Personal Qualities

D1. Prepare structured technical reports for assigned lab works.
D2. Deliver verbal communication on the performed Hands-On projects.

Learning Outcomes Achievement

- Development: A1, A2, A3, A5, B3 are developed through lectures
  B1, B2, B4, D2 are developed through tutorials and practical works

  C1, C2, D1 are developed through homework

- Assessment: A1, A2, A3, A5, B1, and B2 are assessed by examinations and quizzes;
  B3, B4, C1, C2, D1, D2 are assessed by assignments and lab work.

Assessment instruments:
Quizzes: 4
Lab works: 2
Exams: 3

Allocation of Marks	
Assessment Instruments	**Marks**
First exam	20
Second exam	20
Final exam	40
Quizzes + Lab work	10 + 10
Total	**100**

- *Make-up exams will be offered for valid reasons only with consent of the Dean. Make-up exams may be different from regular exams in content and format.*

Documentation and academic honesty

- Practical works reports must be presented according to the style specified in the homework and practical work guide.
- Protection by copyright.
- Avoiding plagiarism: any stated plagiarism leads to an academic penalty.

Course/module 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 (1)	
(3)	Malware and Social Engineering Attacks (2)	Lab work – 1st group
(4)	Application and Network Attacks (1) **Quiz 1**	
(5)	Application and Network Attacks (2)	Lab work – 2nd group *Lab work assessment 1st group*
(6)	Vulnerability Assessment and Mitigating Attack *Tutorial 1*	
(7)	Host, Application , and Data Security (1) **First exam**	
(8)	Host, Application , and Data Security (2)	Lab work – 3rd group *Lab work assessment 2nd group*
(9)	Network Security (1)	Quiz 2
(10)	Network Security (2)	Lab work – 4th group *Lab work assessment 3rd group*
(11)	Administering a Secure Network *Tutorial 2*	
(12)	Wireless Network Security **Second Exam**	
(13)	Access Control Fundamentals	Lab work – 5th group *Lab work assessment 4th group*
(14)	Authentication and Account Management **Quiz 2**	
(15)	Basic Cryptography *Tutorial 3*	Tutorial 3 *Lab work assessment 5th group*
(16)	Advanced Cryptography **Final Exam**	

Expected workload: On average you need to spend 3 hours of study and preparation for each 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 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.

Supporting Material:

1. Mark Ciampa, Security+ Guide to Network Security Fundamentals, 4th Edition, Course Technology, 2012
2. William Stallings, Wireless Communications & Networks, 2nd edition, Prentice-Hall Pearson, 2005
3. Computer Networking: A top down approach 6th edition, J.F. Kurose and K.W. Ross,

Web Links: http:www.philadelphia.edu.jo/academics/mbaniyounes