Zarqa University
Faculty: Information Technology
Department: CIS
Course title: Information and Network Security (1502361)

Instructor:
Lecture's time:
Semester:
Office Hours:

Course description:

Overview principles and technologies behind computer security. Topics include: principles of computer security; encryption and decryption; security mechanisms in computer programs, operating systems, databases, and networks; administration of computer security , and legal and ethical issues.

Aims of the course:

1. Recognize the concepts and principles of Information Security.
2. Explain how to encrypt and decrypt data
3. Describe the effect of malicious code in it field
4. Describe the main networks threats.
5. Explain how to increase the protection level for networks

Intended Learning Outcomes: (ILOs)

A. Knowledge and Understanding

A1. Concepts and Theories:

- Recognize the concepts and principles of Information Security.
- Define the computer security.
- Define the computer Criminals.
- List the basic approaches to defense of computing systems.
- Provide understanding of how cryptography is used in secure communication
- An overview of Stream/Block Ciphers
- Develop knowledge of security mechanisms in computer programs, operating systems, databases, and networks, administration of computer security, and legal/ethical issues in computer security
- An overview of wireless security.

A2. Contemporary Trends, Problems and Research:

- Develop knowledge of vulnerabilities, threats and attacks in computing systems
- Describe the main networks threats.
- Understand the importance of senior system manager's role in information assurance

A3. Professional Responsibility:

- List the main security Principles.
- Describe the effect of malicious code in it field
- Explain how to increase the protection level for networks

B. Subject-specific skills

B1. Problem solving skills:

- Learn how to use cryptography algorithms to encrypt and decrypt data.

B2. Modeling and Design:

- Learn how to uses of encryption.
- Learn how to uses of network security controls

B3. Application of Methods and Tools:

- Learn how to collect and define the vulnerabilities.
- Learn how to apply cryptography algorithms to encrypt and decrypt data.
- Develop proficiency in use of various software tools for computer security.

C. Critical-Thinking Skills

C1. Analytic skills: Assess:

- Distinguish between viruses and other malicious code.
- Analyze, design, build and manage secure systems

C2. Strategic Thinking:

- Analyze the typical attack scenario.
- How controls against program threats work.

C3. Creative thinking and innovation:

- Investigate the virus's signature.

D. General and Transferable Skills (other skills relevant to employability and personal development)

D1. Communication:

- Discuss how the IDS and firewalls work.

D2. Teamwork and Leadership:

- Discuss and work in a group in order to study several cases related to the computer threats, vulnerability and controls.

Course structures:

Week	Credit Hours	ILOs	Topics	Teaching Procedure	Assessment methods
1, 2	6	A1, A2, A3, B3 D2	Principles of computer security	- Lecturing with active participations. - Problem solving. - Cooperative learning. - Discussion. - Learning by activities. - Connecting students with different sources of information.	Diagnostic tests to identify the students level and areas of weakness Formal (stage) evaluation a) Class Participation b) Ist Exam c) 2nd Exam d) Activity file
3, 4, 5	9	A1, B1, B2, B3, C1	Elementary cryptography Part1	- Lecturing with active participations. - Problem solving. - Cooperative learning. - Discussion. - Learning by activities. - Connecting students with different sources of information.	Diagnostic tests to identify the students level and areas of weakness Formal (stage) evaluation a) Class Participation b) Ist Exam c) 2nd Exam d) Activity file
6, 7	5	A1, B1, B2, B3, C1	Elementary cryptography Part2		Diagnostic tests to identify the students level and areas of weakness Formal (stage) evaluation

					a) Class Participation b) Ist Exam c) 2nd Exam d) Activity file
7,8	4	A1, A2, A3, B3, C1, C2, C3, D2	Program Security	- Lecturing with active participations. - Problem solving. - Cooperative learning. - Discussion. - Learning by activities. - Connecting students with different sources of information.	Diagnostic tests to identify the students level and areas of weakness Formal (stage) evaluation a) Class Participation b) Ist Exam c) 2nd Exam d) Activity file
			First exam		
9, 10, 11	9	A1,A2, A3, B2, C1, C2	Network Security Part1	- Lecturing with active participations. - Problem solving. - Cooperative learning. - Discussion. - Learning by activities. - Connecting students with different sources of information.	Diagnostic tests to identify the students level and areas of weakness Formal (stage) evaluation a) Class Participation b) Ist Exam c) 2nd Exam d) Activity file
			Second exam		
12, 13, 14		A1,A2, A3, B2, C1, C2, D1	Network Security Part2	- Lecturing with active participations. - Problem solving. - Cooperative learning. - Discussion. - Learning by activities. - Connecting students with different sources of information.	Diagnostic tests to identify the students level and areas of weakness Formal (stage) evaluation a) Class Participation b) Ist Exam c) 2nd Exam d) Activity file
15	1	A1	Wireless Security	- Lecturing with active participations. - Problem solving. - Cooperative learning.	Diagnostic tests to identify the students level and areas of weakness Formal (stage) evaluation a) Class Participation

				- Discussion. - Learning by activities. - Connecting students with different sources of information.	b) Ist Exam c) 2nd Exam d) Activity file
15	1	D1, D2	Admin	- Lecturing with active participations. - Problem solving. - Cooperative learning. - Discussion. - Learning by activities. - Connecting students with different sources of information.	Diagnostic tests to identify the students level and areas of weakness Formal (stage) evaluation a) Class Participation b) Ist Exam c) 2nd Exam d) Activity file

References:

A. Main Textbook:

- Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger, Prentice Hall, Fourth Edition, 2007.

B. Supplementary Textbook(s):

- Network Security Essentials: Applications and Standards, Wm. Stallings, Prentice Hall, Fifth Edition, 2013.
- Network Security - Private Communication in a Public World, Charlie Kaufman, Radia Perlman and Mike Speciner, Prentice Hall, Englewood Cliffs, New Jersey, 1995.
- Handbook of Applied Cryptography

Assessment Methods:

Methods	Grade	Date
First Exam	20%	
Second Exam	20%	
Assignments (Reports /Quizzes/ Seminar / Tutorials ….)	10%	
Final Examination	50%	