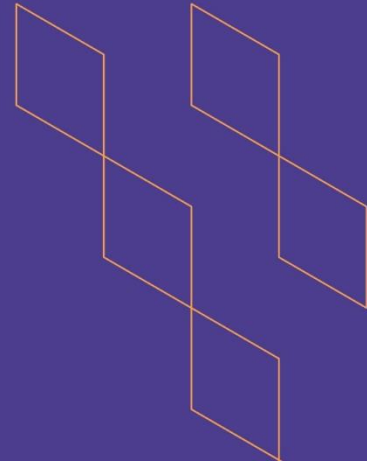T-104
2022

Course Specification

Course Title: **Fundamental of Computers Security**

Course Code: **177 CIS-3**

Program: **Information System**

Department: **Computer**

College: **Applied College**

Institution: **Najran University**

Version : **T-104 2022**

Last Revision Date: **20/8/2023**

Table of Contents:

A. General information about the course:

Course Identification				
1. Credit hours:	3(2+2)			
2. Course type				
a.	University ☐ College ☐	Department☒	Track☒	Others☐
b.	Required ☒ Elective☐			
3. Level/year at which this course is offered:	**Level: 3rd / Year: 1st**			
4. Course general Description: This course provides an in-depth understanding into the fundamental concepts of computer security. It covers basic cryptography, including symmetric and public key cryptosystems as well as key management and distribution and user authentication. It provides an introduction to digital signatures, hash functions, message authentication codes and their application to message and user authentication. The course further focuses on software vulnerabilities and the malware exploiting them.				
5. Pre-requirements for this course (if any):				
6. Co- requirements for this course (if any): **Not Exist**				
7. Course Main Objective(s) - 1. Define the basic concepts and terminologies of computer security. 2. Describe types of attacks related to computer/network systems and security services. 3. Distinguish symmetric and asymmetric cryptographic algorithms and their applications. 4. Classify user and message authentication algorithms and their applications. 5. Evaluate different types of malicious software, intrusion detection and prevention methods.				

1. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1.	Traditional classroom	56	95%
2.	E-learning		5%
3.	Hybrid • Traditional classroom • E-learning		
4.	Distance learning		

2. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	28
2.	Laboratory/Studio	28
3.	Field	
4.	Tutorial	
5.	Others (specify)	
	Total	56

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
1.0	Knowledge and understanding			
1.1	Define the concepts of computer security	K1=I	• Lectures, • Brainstorming, • Class • Discussion • Lab Reports	• Class work • home works assignments • Quizzes • Midterm Exams • Final Exam
1.2	explain the vulnerabilities of information system as well mitigations to information system attacks.	K2=I		
1.3	Describe types of attacks related to computer/network systems and security services	K3=I		
2.0	Skills			
2.1	Distinguish symmetric and asymmetric cryptographic algorithms and their applications.	S1=M	•Lecture •Brainstorming •Small Group Work •Lab Demonstration •Project •Exam •Group Reports •Lab Reports	•homework assignments •Quizzes •Midterm Exams •Final Exam
2.2	Evaluate different types of malicious software	S2=M		
2.3	Classify user and message authentication algorithms and their applications.	S3= M	Lecture •Brainstorming •Small Group Work •Lab	•homework assignments

Code	Course Learning Outcomes	Code of CLOs aligned with program	Teaching Strategies	Assessment Methods
3.0	Values, autonomy, and responsibility			
3.1	Demonstrate projects and assignments in team work for computer security	C1=P	• Small group work and presentations • projects	•Group reports and presentations
3.2				
...				

C. Course Content

No	List of Topics	Contact Hours
1.	fundamental concepts of computer security Firewall	2 4
2.	Cryptographic Introduction to Wireshark	4 4
٣	Authentication and Authorization Install Wireshark	4 3
٤	Symmetric & Asymmetric Capture dump file	4 3
5	Public key cryptography Wireshark commands	2 3
6	Hash Algorithms MD5	2 3
7	software vulnerabilities and the malware lab	4 2
8	Malicious software lab	2 2
9	Intrusion detection and prevention system lab	2 2
	Review	2
	practical exam	2
	Total	56

D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignment	During semester	10%
2.	Mid Monthly Exam	8	20%
3.	Practical exam	14	20%
4	Final exam	End of semester	50%
5	Total		100%

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities

1. References and Learning Resources

Essential References	Introduction to Computer Security by Matt Bishop
Supportive References	William Stallings. Cryptography and Network Security, 5th Edition (Prentice Hall)
Electronic Materials	Charles P. Pfleeger and Shari L. Pfleeger, Security in Computing, Prentice-Hall
Other Learning Materials	http://www.uoitc.edu.iq/images/documents/informatics-institute/exam_materials/Introduction%20to%20Computer%20Security%20pdf%20DONE.pdf

2. Required Facilities and equipment

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Computer Lab with 25 seats + A Lecture room with 30 seats per section
Technology equipment (projector, smart board, software)	25 PCs, Data show
Other equipment (depending on the nature of the specialty)	Oracle/SQL Server Lab

F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Student	Direct: Questioners
Effectiveness of students assessment	Teacher Audit and review committees	Direct: CW & HW Exercises and short quizzes Projects Mid and final paper exams.
Quality of learning resources	Teachers and course description committees	Indirect: Benchmarking Self-evaluation External evaluation
The extent to which CLOs have been achieved	Teacher	Direct: Measuring the learning outcomes
Other		

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data

COUNCIL /COMMITTEE	
REFERENCE NO.	
DATE	