Course Description

Computer security is one of the susceptible topics because of the importance of this device, as it contains private information or provides access to people for spying, etc. Therefore, this topic is one of the matters closely related to the ABCs of the student's specialization as a programmer. Therefore, it has become part of the curriculum scheduled for this stage. The fourth in the Department of Computer Science is an explicit curriculum because it contains the basics of important computer security and software applications that develop students' mental abilities and give them many basic concepts that enrich their cognitive and programming requirements.

1. Educational Institution/ college	Tikrit University/College of Computer Science and Mathematics
2. Scientific Department/Center:	Computer Science Department
3. Course name/code:	Computer Security
4. Available attendance formats:	Weekly
5. Course /year:	Second Course 2023/2024
6. Number of study hours (total):	30 theoretical hours and 30 practical hours

1. Course objectives

The course aims to teach the student the different ways to defend computer security from various attacks such as viruses and worms, in addition to Learn about different software protection methods, such as:

- Firewall
- Prevent Intrusion System
- Detection Intrusion System .and others

In addition to some protocols to ensure the reliability and credibility of both the sender and the recipient.

2. Course Outcomes and Teaching, Learning and Evaluation Methods

A- Knowledge objectives

A1- Know the basics of computer security work.

A2- Knowledge and understanding of computer security functions.

A3- Knowledge of computer security programming Data protection.

A4- Knowing the vulnerabilities, some attack methods, and how to deal with them.

B - The skills objectives of the course

The students responded clearly to the subject through the course teacher’s evaluation as a result of the students’ interaction during the explanation of the topics to be taught and through their effective contribution in using computer security programs and the ability to apply them.

B 1 - Enabling the student to choose the best ways to protect the computer.

B2 - Teaching students about the dangers that exist on the Internet.

Teaching and learning methods

Theoretical Lectures

Practical Lectures

Evaluation methods

1 . Direct questions during the theoretical lecture

2 .Daily exams in each lecture on the subject of the previous lecture

3 .Homework assignments and reports

4. Monthly exams

C- Expressive and Value Objectives

C-1 Asking them in the lecture and assigning them to search for the answer by searching on the Internet.

C-2 Do not transfer solutions between all groups of students by changing tasks from one group to another.

C-3 Pushing the student to commit to attending theoretical lectures by taking daily exam.

3. Course structure

Number of teaching hours		Syllabus Vocabulary	Week
Practical	Theoretical		
2	2	What is computer security? Introduction to CIA security objectives and computer security challenges and a review of the practical aspect	.1
2	2	Concepts of threats, vulnerabilities, and attacks, and conducting practical experiments on the computer	.2
2	2	How to secure access to resources - Two-step authentication: identification of the access requester and authorization to grant or deny access. And apply it programmatically	.3
2	2	How to secure communications over a computer network - in three steps:	.4
2	2	First: Confidentiality by preventing intercepted communications from being understood. Explain this practically	.5
2	2	Second: Authentication by creating an identification of the sender's identity. Explaining physical security and authentication models. Learn about PKI and encryption protocols.	.6
2	2	Third: Clarifying the integrity of the information by proving that communications have not been tampered with.	.7
2	2	General access control techniques: something you have, something you know, something you are. Access control methods and models and how to apply them in practice.	.8
2	2	Advantages and disadvantages of passwords. Programming examples implemented in the laboratory.	.9
2	2	ACL and C-list identification declaration	.10
2	2	Explain the concepts of: spyware, advertising-supported software, malware (viruses and worms), Trojan horses, logic bombs... etc.	.11
2	2	Defensive measures: firewall and intrusion detection system. And methods of applying it	.12
2	2	Methods for checking and removing viruses	.13
2	2	Methods for checking and removing malware	.14
2	2	Security applications: e-commerce security, SSL/TLS, virtual private networks (VPN), web security	.15

4.Infrastructure

1- Required prescribed books	Nothing
2- Main references (sources)	-Network Security Essentials: Applications & Standards, William S., Pearson Education Asia. -CompTIA security+ - David L. Prowse, Pearson USA 4th Edition, 2019.
3- Recommended books and references (scientific journals, reports …..)	-Database Security Mechanisms for Computer Network-Sead Muftic, John Wiles . -Designing Security Architecture Solutions -Jay Ramachandran, Wiley dream tech -Security in Computer Operating System -G. O.Shea , NCC Blackwell Manchester Oxford