



# Course Specification

— (Bachelor)

**Course Title:** Network Security

**Course Code:** CIT1407

**Program:** Bachelor in information technology

**Department:** Information Technology

**College:** Faculty of Computers and Information Technology

**Institution:** University of Tabuk

**Version:** 1.0

**Last Revision Date:** 27 July 2022



## Table of Contents

<b>A. General information about the course:</b>	<b>3</b>
<b>B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods</b>	<b>4</b>
<b>C. Course Content</b>	<b>4</b>
<b>D. Students Assessment Activities</b>	<b>5</b>
<b>E. Learning Resources and Facilities</b>	<b>5</b>
<b>F. Assessment of Course Quality</b>	<b>5</b>
<b>G. Specification Approval</b>	<b>6</b>



## A. General information about the course:

### 1. Course Identification

#### 1. Credit hours:

3 CHrs. (Three Credit Hours)

#### 2. Course type

- A.  University  College  Department  Track  Others
- B.  Required  Elective

#### 3. Level/year at which this course is offered: : (Level 8, Year 4)

#### 4. Course general Description:

The course covers the fundamental concepts of Transport-Level Security, Wireless Network Security, Electronic Mail Security, and IP Security. Moreover, the course introduces Intruders and IDS, Malicious Software and DDoS, and Firewalls.

#### 5. Pre-requirements for this course (if any):

Computer and Information Security (CIT1402)

#### 6. Co-requisites for this course (if any):

#### 7. Course Main Objective(s):

In this course, students will learn how to design a simple Network Secure System and develop a simple IDS. Moreover, students will have the ability to evaluate the strength of a Network Security System.

### 2. Teaching mode (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	45	100%
2	E-learning		
3	Hybrid <ul style="list-style-type: none"> <li>● Traditional classroom</li> <li>● E-learning</li> </ul>		
4	Distance learning		



### 3. Contact Hours (based on the academic semester)

No	Activity	Contact Hours
1.	Lectures	45
2.	Laboratory/Studio	
3.	Field	
4.	Tutorial	
5.	Others (specify)	
<b>Total</b>		<b>45</b>

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

Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
<b>1.0</b>	<b>Knowledge and understanding</b>			
1.1	Recognize the basic concepts of Transport-Level Security.	K1	Lectures, textbooks, provided handouts, references.	Exams, and the project.
1.2	Recognize Network Security and Electronic Mail Security.	K1, K2	Lectures, textbooks, provided handouts, references.	Exams, and the project.
1.3	Define Electronic Mail Security, IP Security.	K1, K2	Lectures, textbooks, provided handouts, references.	Exams, and the project.
1.4	Specify and describe Intruders and IDS.	K1, k2	Lectures, textbooks, provided handouts, references	Exams, and the project.
1.5	Demonstrate and identify Malicious Software and DDoS, and Firewalls.	K4	Lectures, textbooks, provided handouts, references	Exams, and the project.
<b>2.0</b>	<b>Skills</b>			
2.1	Design a simple Network Secure System.	S1, S3	Lectures, textbooks, provided handouts, references.	Exams, and the project.





Code	Course Learning Outcomes	Code of PLOs aligned with program	Teaching Strategies	Assessment Methods
2.2	Develop a simple IDS.	S1, S3	Lectures, textbooks, provided handouts, references.	Exams, and the project.
2.3	Evaluate the strength of a Network Security System.	S2	Lectures, textbooks, provided handouts, references.	Exams, and the project.
<b>3.0</b>	<b>Values, autonomy, and responsibility</b>			
3.1	The ability to work in groups.	V1, V2	Lectures, textbooks, provided handouts, references.	project.
3.2	The ability to work professionally and effectively.	V2	Lectures, textbooks, provided handouts, references.	project.

### C. Course Content

No	List of Topics	Contact Hours
1.	<b>Introduction and overview:</b> Network OSI Layers, Network security, Symmetric Cryptography review.	3
2.	<b>Public key Encryption:</b> Asymmetric Cryptography, RSA.	3
3.	<b>Key distribution:</b> Key Management, KDC, Active directory, Certificate authority CA.	3
4.	<b>Hashing and Data integrity:</b> Message authentication, Hash function, MAC, HMAC.	3
5.	<b>Digital signature:</b> Properties, Direct digital signatures, arbitrated digital signatures, Replay attacks.	3
6.	<b>Authentication protocols:</b> Authentication Applications, Kerberos v4 and v5, Kerberos realms, Authentication Procedures.	3
7.	<b>Electronic Mail Security:</b> Email security, E-mail security Enhancements, PGP Protocol, S/MIME Protocol.	3
8.	<b>IP Security:</b> IPSec, IPSec uses, IPSec services, Authentication Header (AH), Encapsulating Security Payload (ESP), Transport and Tunnel Modes.	3
9.	<b>Transport-Level Security:</b> Web Security, HTTPS, SSL and TLS, SSH.	3
10.	<b>Intruders (Part1):</b> classes of intruders, Intrusion Techniques, Intrusion Detection.	3
11.	<b>Intruders (Part2):</b> Approaches to Intrusion Detection, Audit Records, Honeypots, Password Management.	3
12.	<b>Malicious Software and DDoS:</b> Malicious Software Classification, Virus, Worm, Backdoor, Zombie, Trojan, Logic Bomb, DDoS.	3





13.	<b>Firewall:</b> Firewall Limitations, Firewall Types, Packet Filters, Attacks on Packet Filters, Bastion Host, Access control, Firewalls properties.	3
14.	<b>Projects discussion (Part1):</b> Students projects.	3
15.	<b>Projects discussion (Part2):</b> Students projects.	3
<b>Total</b>		<b>45</b>

## D. Students Assessment Activities

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Mid-term Exam 1	6,7	20%
2.	Mid-term Exam 2	11,12	20%
3.	Project	14,15	20%
4.	Final Exam	17	40%

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

## E. Learning Resources and Facilities

### 1. References and Learning Resources

<b>Essential References</b>	<b>Cryptography and Network Security Principles and Practice 5th Edition</b>
<b>Supportive References</b>	<b>Provided Handouts</b>
<b>Electronic Materials</b>	<b>Will be specified at the course time as needed.</b>
<b>Other Learning Materials</b>	<b>Blackboard Platform</b>

### 2. Required Facilities and equipment

Items	Resources
<b>facilities</b> (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	<b>25 students/room</b>
<b>Technology equipment</b> (projector, smart board, software)	<b>Projector</b>
<b>Other equipment</b> (depending on the nature of the specialty)	<b>Students should have laptops</b>

## F. Assessment of Course Quality

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of Teaching	Faculty, Program Leaders, and Advisory Board	Both Direct and Indirect
	Students	Indirect





Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of Students Assessment	Faculty, Program Leaders, Advisory Board, and Independent Opinion	Both Direct and Indirect
Quality of Learning Resources	Faculty, Students, and Advisory Board	Indirect
The Extent to which CLOs have been Achieved	Faculty, Program Leaders, Advisory Board, and Independent Opinion	Direct (as in section B) and Indirect/Surveys
	Students	Indirect
Other	-	-

**Assessors** (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify))

**Assessment Methods** (Direct, Indirect)

### G. Specification Approval

<b>COUNCIL /COMMITTEE</b>	
<b>REFERENCE NO.</b>	
<b>DATE</b>	

