

# CIST 2602 - Network Security ( version 201003L )

Course Title	Course Development	Learning Support
Network Security	Standard	No

## Course Description

This course provides knowledge and the practical experience necessary to evaluate, implement and manage secure information transferred over computer networks. Topics include network security, intrusion detection, types of attacks, methods of attacks, security devices, basics of cryptography and organizational security elements.

## Pre-requisites

(CIST 1401 or CIST 2451 or CIST 2441)

Pre-requisites (CIST 1401 or CIST 2451 or CIST 2441)

CIST 1601 - Information Security Fundamentals ( 201003L )

## Regstr. Co-requisites

Regstr. Co-requisites: None

## True Co-requisites

True Co-requisites: None

## Course Length

	Lecture Contact Time	Regular Lab Type	Reg. Lab Contact Time	Other Lab Type	Oth. Lab Contact Time	Total Contact Hrs
Contact Hours Per Week	2 hrs	Lab	4 hrs	N/A	0 hrs	6 hrs
Contact Min/Hrs Per Semester	1500 min		3000 min		0 min	90 hrs
	Lecture Credit Hours	Lab Credit Hours	Total Credit hours	WLU		
Semester Credit Hours	2	2	4	142.5		

## Competencies & Outcomes

### Order Description

#### 1 Network Security Goals

Order	Description	Learning Domain	Level of Learning
1	Define network security.	Cognitive	Knowledge
2	Identify , define and describe the relevance of security goals (integrity, confidentiality, availability).	Cognitive	Knowledge
3	Demonstrate an understanding of and be able to identify both internal and external threats.	Psychomotor	Guided Response

#### 2 Network Attacks Prevention

Order	Description	Learning Domain	Level of Learning
1	List the major types of malicious code and identify appropriate countermeasures.	Cognitive	Knowledge

2	Detail types of social engineering attacks.	Cognitive	Knowledge
3	Demonstrate an understanding of the concept and significance of auditing, logging and system scanning.	Psychomotor	Guided Response

**3 Communication Security**

Order	Description	Learning Domain	Level of Learning
1	Recognize and understand the administration of securing the following technologies: remote access, email, web, directory, file transfer and wireless.	Affective	Valuing

**4 Infrastructure Security Devices**

Order	Description	Learning Domain	Level of Learning
1	Demonstrate an understanding of the purpose of a firewall and different kinds of firewall technology.	Psychomotor	Guided Response
2	Demonstrate an understanding of the role of routers, switches, modems and other network devices.	Psychomotor	Guided Response
3	Identify key elements of VPN (Virtual Private Network) and RAS (Row Access Strobe) technology for secure connectivity.	Cognitive	Knowledge

**5 Intrusion Detection**

Order	Description	Learning Domain	Level of Learning
1	Explain intrusion detection.	Cognitive	Knowledge
2	Define the difference between host and network based detection.	Cognitive	Comprehension
3	Demonstrate an understanding of the difference between passive and active detection.	Psychomotor	Guided Response
4	Identify some characteristics of an intrusion detection system.	Cognitive	Knowledge

**6 Cryptography in Information Security**

Order	Description	Learning Domain	Level of Learning
1	Demonstrate an understanding of how encryption algorithms are used in modern cryptography.	Psychomotor	Guided Response
2	Identify and be able to differentiate different cryptographic standards and protocols.	Cognitive	Knowledge
3	Discuss PKI.	Cognitive	Comprehension