

10/21/2022 DATE



REQUIRED COURSE



ELECTIVE COURSE

Business DIVISION



NEW COURSE



REVISION

Lake Land College

Course Information Form

COURSE NUMBER:	CIS-070	TITLE: (30 Characters Max)		Network Security			
SEM CR HRS:	3	Lecture:	2	Lab:	2	ECH:	4
Course Level:	<input type="checkbox"/> Gen Ed / IAI <input type="checkbox"/> Baccalaureate /Non-IAI		<input checked="" type="checkbox"/> Career/Technical <input type="checkbox"/> Dev Ed/ Not in Degree Audit	Clinical Practicum:	0	Work-based Learning	0
COURSE PCS #	12 - 11. 1003		IAI Code			Contact Hours Per Week	
Repeatable (Y/N):	Y	Pass/Fail (Y/N):	N	Variable Credit (Y/N):	N	Min:	Max:
Prerequisites:	CIS-081, CIS-079						
Catalog Description: (40 Word Limit)	An overview course of security topics as it applies to a typical Server-based network. Course of study includes Security+ Exam content: authentication, remote access, external attacks, intrusion detection, web and email security, and disaster recovery.						

List the Major Course Segments (Units)	Contact Lecture Hours	Contact Lab Hours	Clinical Practicum	Work-based Learning
Overview	2			
Security Architecture	3			
Authentication	4			
External Attacks	5			
Email and Web Security	4			
Remote Access	3			
Intrusion Detection	4			
Physical Security	2			
Disaster Recovery	3			
Lab Exercises		30		
TOTAL	30	30	0	0

EVALUATION

QUIZZES	<input checked="" type="checkbox"/>	EXAMS	<input checked="" type="checkbox"/>	ORAL PRES	<input type="checkbox"/>	PAPERS	<input checked="" type="checkbox"/>
LAB WORK	<input checked="" type="checkbox"/>	PROJECTS	<input checked="" type="checkbox"/>	COMP FINAL	<input checked="" type="checkbox"/>	OTHER	<input type="checkbox"/>

COURSE MATERIALS

TITLE:	CompTia Security+ Get Certified Get Ahead: SYO-501 ST GD
AUTHOR:	Gibson
PUBLISHER:	Amazon.com
VOLUME/EDITION/URL:	4th Edition
COPYRIGHT DATE:	2017

TITLE:	Security Essentials
AUTHOR:	Lavender/Goodheart-Wilcox
PUBLISHER:	Goodheart-Wilcox Co. Inc.
VOLUME/EDITION/URL:	1st Edition
COPYRIGHT DATE:	2022

TITLE:	Incident Response & Computer Forensics
AUTHOR:	Luttgens
PUBLISHER:	McGraw Hill
VOLUME/EDITION/URL:	3rd Edition
COPYRIGHT DATE:	2014

MAJOR COURSE SEGMENT	HOURS	LEARNING OUTCOMES
		<i>The student will be able to:</i>
Overview	2	Identify key security issues in a network environment.
Security Architecture	3	Evaluate various physical network layouts that enhance security. A. DMZ structure B. VLANs C. NAT and ICS

Authentication	4	Identify the variety of logon methods and their security enhancements. A. Passwords B. Biometric devices C. Cryptography
External Attacks	5	Describe the methods of launching an external attack on a network. A. Denial of Service (DoS) B. Spoofing C. Replays D. Viruses and worms E. Trojan horses
Email and Web	4	Explain ways to secure electronic communication and commerce and be knowledgeable of their security weaknesses. A. SSL B. Java C. ActiveX
Remote Access	3	Identify methods of securing external access to the network. A. PPTP B. L2TP/IPSec C. VPN configuration
Intrusion Detection	4	Examine methods of detecting, logging and reacting to unwanted access to the local network. A. Active detection B. Passive detection C. Appropriate responses
Physical Security	2	Explain the importance of physically limiting access over other forms of potential security.
Disaster Recovery	3	Describe the methods and procedures for recovering from a system, drive or OS failure. A. Backups B. Recovery plans and policies
Lab Exercises	30	
	60	

COURSE OUTCOMES*	At the successful completion of this course, students will be able to:
	<ul style="list-style-type: none"> Identify the fundamental elements of security.
	<ul style="list-style-type: none"> Understand the basic security tools available.
	<ul style="list-style-type: none"> Understand the basic security tools available.

* Course Outcomes will be used in the Assessment Software for Outcomes Assessment. Limit to 3 - 5.