COURSE SYLLABUS

Tunxis Community College

Education That Works For a Lifetime

Course Title:	**Special Topics: Network Security Fundamentals**	**Date of last update:** (If this syllabus is being changed as part of a course change or new course proposal, enter the date of the proposal)	
Department:	**Arts, CIS**		
Curriculum:	**Computer Systems Technology**		

Course Descriptors: (Make certain that the course descriptors are consistant with college and Board of Trustees policies, and the current course numbering system.)

Course Code: (eg. ACC 101)	**CST298**
Course Type:	**L**

L: Lecture B: Lab X: Combined Lecture/Lab
U: Studio N: Internship P: Practicum
D: Distance Learning I: Individual / Independent

Credit Hours:	**3**
Developmental: (yes/no)	**N**
Contact Hours: Lecture:	**3**
Lab:	
Clinical:	
TOTAL:	**3**
Class Maximum:	**24**
Semesters Offered:	**Fall, Spring**

Prerequisites:

CST130 Network Essentials I

Corequisites:

None.

Other Requirements:

None.

Catalog Course Description: (Check with the Public Information Office to assure consistant taxonomy, terminology and style.)

Introduces students to the subject of network security. Topics include security models, authentication, attacks, infrastructure devices, intrusion detection, and the basics of cryptography along with physical security and disaster recovery. This course emphasizes preparing the student for the CompTIA Security+ certification.

Course Objectives & Their Evaluation: (A broad, content-based statement about what the instructor will attempt to achieve in the course.)

The student will:

1. Deomonstrate an understanding of network security and the goals of network security.
2. Create a disaster recovery plan for a given scenario.
3. Design a security plan to protect a network agains malicious software and vulnerabilities.
4. Create and implement password policies.
5. Demonstrate an understanding of cryptography and how it is used to secure date over a network.

Students will be evaluated through examinations, homework assignments and case projects.

Specific Outcomes: (Measurable skills students will be expected to demonstrate or specific tasks the student should be able to perform, as evidence that the course content has been mastered.)

Upon successful completion of this course, students will be able to:

1. Demonstrate an understanding of network security and the goals of network security.
2. Create srong passwords and store them securely.
3. Explain the major types of malicious software and identify a counter measure for each one.
4. Demonstrate how to safeguard against email vulnerabilities.
5. Identify vulnerabilities associated with certain web applications such as instant messaging.
6. Conduct a wireless site survey.
7. Explain the role of routers, switches, firewalls and other networking hardware in security.
8. Identify the place and role of the demilitarized zone in the network.

Special Topics: Network Security Fundamentals

	9. Detail the differences between host-based and network-based intrusion detection. 10. Explain the concept of cryptography and how it relates to network security. 11. Implement the disaster recovery process for a given scenario.
Topical Outline:	1. Introduction to security concepts 2. Authentication 3. Denial of Service attackes, Spoofing, Worms, Backdoors, Logic Bombs 4. Remote Access Security (L2TP, IPSec) 5. Email Security, Spam 6. Web Security 7. Wireless 802.11 Standards and Instant Messaging 8. Security devices (firewalls, routers, switches) 9. Intrusion Detection 10. Network Security Topologies 11. Cryptography 12. Physical Security 13. Disaster Recovery
Suggested Instructional Materials	Security+ Guide to Network Security Fundamentals, current edition
Resources, Equipment, & Special Facilities Required:	Network Lab