Virginia Western Community College
ITN 260
Network Security Basics

Prerequisites
TEL 150

Course Description
Provides instruction in the basics of network security in depth. Includes security objectives, security architecture, security models and security layers; risk management, network security policy, and security training. Includes the five security keys, confidentiality integrity, availability, accountability and auditability.

Semester Credits: 3 Lecture Hours: 3 Lab/Clinical/Internship Hours: 0

Required Materials

Textbook:
Security and Guide to Network Security Fundamentals; Mary Ciampa; 6th edition; ISBN: 978-1337288781

Other Required Materials:
none

Course Outcomes

At the completion of this course, the student should be able to:

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attacks that are common today
- List techniques for mitigating and deterring attacks, and perform steps in typical mitigation
- List the steps for securing physical systems including typical fixed and mobile hardware
- Define and understand the basic use of cryptography
- Describe the different types of wireless network attacks
- Describe how to implement BYOD security
- Explain how to control risk
- List the ways in which security policies can reduce risk
- Describe how awareness and training can provide increased security

- Explain the differences between vulnerability scanning and penetration testing

Topical Description

Topics	Chapter Readings	Exams
Introduction to Security	Chapter 1	
Malware and Social Engineering Attacks	Chapter 2	
Basic Cryptography	Chapter 3	
Advanced Cryptography	Chapter 4	
Networking and Server Attacks	Chapter 5	
Network Security Devices, Design, and Technology	Chapter 6	
Administering a Secure Network	Chapter 7	Midterm Exam
Wireless Network Security	Chapter 8	
Host, Application, and Data Security	Chapter 9	
Mobile and Embedded Device Security	Chapter 10	
Authentication and Account Management	Chapter 11	
Access Management	Chapter 12	
Vulnerability Assessment and Data Security	Chapter 13	
Business Continuity	Chapter 14	
Risk Mitigation	Chapter 15	Final Exam

Notes to Instructors

- A mid-term and final exam should be required
- At least eight hands-on labs should be required