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+ Guide to Network Security Fundamentals, Sixth Edition. Mark Ciampa, Ph.D. ISBN 978-1-337-28878

Other Required Materials:
None

Course Outcomes

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

- Explain challenges of securing information. Define information security and explain why it's important, identify threat actors and defenses, layers of security and the security life-Cycle
- Define malware; types and payload. Discuss technology and personal safety including stalking, bullying, sexual exploitation. Understand how locality impacts how laws are applied. Describe social engineering attacks and defenses.
- Define and describe cryptography and basic algorithms (hash, symmetric, asymmetric), explain different attacks and how cryptography is used.
- Implement cryptography, define and describe digital certificates, PKI, transport encryption algorithms. Understand the challenges and failures of common systems.
- Describe various network-based attacks and defenses. Explain how servers are attacked and defended.
- Discuss how network technologies can enhance security. List different network security devices and uses. Describe secure network architectures and how to implement them.

- Show familiarity with network protocols. Apply understanding to the function and implementation of secure network protocols. Explain network security devices and where they should be deployed. Show an understanding of how to analyze data. Explain how to manage and secure network platforms.
- Describe wireless security devices, protocols and use. Discuss various wireless network attacks, vulnerabilities. Explain solutions for securing wireless networks.
- List the steps for securing client devices and locations. Define and describe application security. Give examples of physical security and how to implement them.
- List and compare different types of mobile device. Discuss deployment, risks and mitigation. Discuss how IoT and connected devices of all types increase convenience as well as risk to health and safety.
- Describe different types of authentication and credentialing. Explain single Sign-On, list account management procedures for securing passwords. Discuss risks and mitigations associated with passwords and other credential/authentication systems
- Define access management and list access control modes. Describe how to manage access through account management. List best practices for access control and implementation. Explain different types of identity and access services. Discuss ways we deal with failures in access management and control.
- Discuss how we assess enterprise security posture. Define vulnerability assessment and explain its importance. Contrast vulnerability scanning, and pen testing. Discuss personal and business data privacy and security. Identify risks and mitigations. Explore the internet, examining privacy as it applies to their own information. Students will write and discuss the impact of technology on privacy and the prevailing policies and laws on privacy.
- Describe fault tolerance through redundancy. Define business continuity. Explain different environmental controls. Describe forensics and incident response procedures.
- Describe the concept of risk. Explain how to manage risk. Describe practices for reducing and mitigating risk. Describe common security issues that cause risk.

Topical Description

1	**Introduction to Security** Challenges of securing information Avoiding Legal Consequences Basic Defense Threat Actors Information Security Life Cycle
2	**Malware and Social Engineering Attacks** Common attacks and countermeasures

	Payloads Detection Social engineering, tricking users
3	**Basic Cryptography** Hash, symmetric, asymmetric Different attacks and uses Confidentiality, non-repudiation
4	**Advanced Cryptography** Implementation Digital Certificates Public Key Infrastructure Securing data at rest, data in transit Transport encryption protocols
5	**Networking and Server Attacks** Types of network-based attacks Detection of network-based attacks How servers are attacked Sessions and attacks Client-side vs. server-side attack and defense
6	**Network Security Devices, Design and Technology** Network Security Devices IDS,DPS,firewalls, etc. Secure network architectures Using network tech to enhance security

7	**Administering a Secure Network** Detection Secure network protocols Analyzing security data Managing and securing network platforms
8	**Wireless Network Security and Exam Review** IEEE 802.11 networks & standards Wireless network attack types and defense Securing wireless networks
	Midterm Exam
9, 10	**Host, Application and Data Security and Mobile and Embedded Device Security** Security client devices Application security Physical Security Mobile device types and deployment Mobile device risk Securing mobile devices Embedded systems IOT and risk
11	**Authentication and Account Management** Authentication & credentials SSO Password security

	Audit and exceptions
12	**Access Management** Account Management Access control models and best practices Implementation of access control Security Models Identity and access services
13	**Vulnerability Assessment and Data Security** **Assessing enterprise security posture** Vulnerability assessments Vulnerability scans vs. pen. Testing Secure methodology **Data privacy and data security techniques** FIPPS framework, PII HIPAA,Sarvox, GLBA, PCI DSS Tracking, survelance
14	**Business Continuity** What it is Fault Tolerence through redundancy Environmental Controls Forensics and incedent response procedures
15	**Risk Mitigation and Exam Review** Risk management, mitigation and recovery Common security issues

	Final Exam

Notes to Instructors

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