INFO-2600 CyberSecurity Essentials Course Syllabus Fall 2025

"Responsibility for learning belongs to the student, regardless of age" Robert Martin

Contents

Your Instructor

William A Loring

Mailing Address: 1601 E 27th St, Scottsbluff, NE 69361

Scottsbluff Office: Room B7F Office Phone: 308.635.6163

E-mail: loringw@wncc.edu (Preferred contact method)

Scottsbluff Office Hours: MW 1-2 pm, M 5-6 pm, TTh 10-11 am or by appointment

Online Office Hours: By appointment. www.calendly.com/loringw

"There are no stupid questions. Ask questions whenever something isn't completely clear. You can't remember what you don't understand."

Tolerate chaos, uncertainty, and vagueness. "Figuring it out" is part of learning.

Class Information

Class Location: Scottsbluff Campus, Room D1

Time: Mon & Wed, 1:00-01:50 pm

Catalog Description

This course introduces the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. This course covers new topics in network security as well, including psychological approaches to social engineering attacks, web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security. The student is encouraged to take the CompTIA Security+ certification exam. The instructor for this course is certified by CompTIA. The CompTIA Security+ certification can be accepted as equivalent for this class. Contact the instructor for details.

3.0 semester hours

(3/45/0/0/0/0) See Figure 1

Course Objectives

Using this course as an instructional medium, the instructor will:

1. Define and explain common computer and network security terms and concepts.
2. Explain the role of security and risk mitigation in a network environment.
3. Explain and give examples of how to prepare and document security procedures and policies.
4. Show and demonstrate how to administer a secure wired and wireless network.
5. Explain and demonstrate how to prepare a vulnerability assessment.
6. Model self-directed and lifelong learning.

Student Learning Outcomes

Upon completion of this course, the student will be able to:

1. Recognize and define common computer and network security terms and concepts. [GE 1, 2]
2. Explain the role of security and risk mitigation in a network environment. [GE: 1]
3. Prepare and document security procedures and policies. [GE 1]
4. Administer a secure wired and wireless network. [GE 3]
5. Prepare a vulnerability assessment. [GE 1, 2]
6. Self-direct their learning while gaining an ongoing interest in learning more about programming. [GE 5]

Instructional Materials

The materials required for this course are included in Cengage Unlimited eTextbooks + Online Homework Platforms. This is a subscription service providing access to ALL Cengage eTextbooks and digital learning products. One Cengage Unlimited subscription can be used across all courses where Cengage products are assigned, at no additional cost.

The access code for the eBook and labs can be purchased at the Cougar Bookstore, Scottsbluff Campus, (308) 635-6066, or online at http://bookstore.wncc.edu

MindTap contains the eBook used in this class. Access to both is within Blackboard. Buying the physical book is optional. The MindTap eBook can be accessed by any computer or mobile device.

Other Materials

- Computer with ability to run virtualization software

Security+ Certification Test

There is a PearsonVue testing center at the Harms Center in Scottsbluff. WNCC is a CompTIA Authorized Academy and receives a 50% discount on test vouchers.

- CompTIA Security+ Exam # SY0-701

If you pass the Security+ test, you will receive an A+ for the class.

Course Schedule

Course content and schedule may change.

Week	Activities	Assignments
Week 1 08/18 - 08/24	Introduction Discussion Introduction to Course Introduction to Blackboard Module 1 Introduction to Information Security	Getting Started Activities in Blackboard Professional Communication Security+ Pre-Course Assessment Live Virtual Machine Lab Pre-Requisite Lab 1.2: Configure Microsoft Windows Sandbox Windows 11 Virtualization Chapter 1 Quiz

Week 2 08/25 - 08/31	Module 2 Pervasive Attack Surfaces and Controls	Review: Chapter 2 PowerPoints, Reinforce, Practice Simulation 2-1: Exploring the National Vulnerabilities Database Examine Data Breaches Are You a Victim? Phishing Test Kali Linux Virtualization Chapter 2 Quiz
Week 3 09/01 - 09/07	Module 3 Fundamentals of Cryptography	Watch: Module 3 Video Review: Chapter 3 PowerPoints, Reinforce, Practice Simulation 3-1: Using OpenPuff Steganography Simulation 3-2: Running an RSA Cipher Demonstration SSL Server and Client Tests Stenography with SilentEye Encrypting Files Chapter 3 Quiz
Week 4 09/08 - 09/14	Module 4 Advanced Cryptography Think Aloud	Review: Chapter 4 PowerPoints, Reinforce, Practice Simulation 4-2: Creating and Installing a Digital Certificate QR Codes Hashcat Password Testing

		Netdiscover Chapter 4 Quiz
Week 5 09/15 - 09/21	Module 5 Endpoint Vulnerabilities, Attacks, and Defenses	Watch: Module 5 Video Review: Chapter 5 PowerPoints, Reinforce, Simulation 5-1: Downloading and Running Microsoft Safety Scanner Simulation 5-2: Analyzing Files and URLs for File-Based Viruses Using VirusTotal ZenMap Enumerate a Network with Kali Ransomware Sites Chapter 5 Quiz
Week 6 09/22 - 09/28	Module 6 Mobile and Embedded Security Think Aloud	Watch: Module 6 Video Review: Chapter 6 PowerPoints, Reinforce, Practice Linux System Monitoring with top Multifactor Authentication Chapter 6 Quiz Semester Project
Week 7 09/29 - 10/05	Module 7 Identity and Access Management (IAM)	Watch: Module 7 Video Review: Chapter 7 PowerPoints, Reinforce, Practice Simulation 7-1: Using an Online Password Cracker Simulation 7-2: Using a Password Manager Application

		MAC Address Spoofing with Windows MAC Address Spoofing with Kali Linux Zphisher Phishing Tutorial Chapter 7 Quiz Semester Project
Week 8 10/06 – 10/12	Module 8 Infrastructure Threats and Security Monitoring	Watch: Module 8 Videos Review: Chapter 8 PowerPoints, Reinforce, Practice Sentiment Analysis Hping3 IP Address Spoofing Disaster Recovery Plan Pentbox Honeypot Semester Project Chapter 8 Quiz
Week 9 10/13 - 10/19 Fall Break	Module 9 Infrastructure Security	Watch: Module 9 Video Review: Chapter 9 PowerPoints, Reinforce, Practice Simulation 9-1: Using GlassWire Firewall Keylogger Wireless Router Configuration Chapter 9 Quiz Semester Project

Week 10 10/20 - 10/26	Module 10 Wireless Network Attacks and Defenses The Social Dilemma Discussion	Watch: Module 10 Video Review: Chapter 10 PowerPoints, Reinforce, Practice Wireless Network Scanning Hosts File Attack ARP Poisoning Browser Passwords Semester Project Chapter 10 Quiz
Week 11 10/27 - 11/02	Module 11 Cloud and Virtualization Security	Review: Chapter 11 PowerPoints, Reinforce, Practice Watch: Module 11 Video Online Backup Services TryHackMe Linkedin Chapter 11 Quiz Semester Project
Week 12 11/03 - 11/09	Module 12 Vulnerability Management Think Aloud	Watch: Unit 12 Video Review: Chapter 12 PowerPoints, Reinforce, Practice Common Vulnerabilities and Exposures (CVE) National Vulnerabilities Database (NVD) Labex.io Part 1 Chapter 12 Quiz

		Semester Project
Week 13 11/10 - 11/16	Module 13 Incident Preparation and Investigation	Review: Chapter 13 PowerPoints, Reinforce, Practice Simulation 13-1: Using Windows File History to Perform Data Backups Password Management Program Password Strength Testing nmap Network Enumeration Semester Project Module 13 Quiz
Week 14 11/17 11/23 Thanks giving	Module 14 Oversight and Operations	Module 14 Videos Review: Chapter 14 PowerPoints, Reinforce, Practice Simulation 14-1: Using a Nonpersistent Web Browser Simulation 14-2: Local Security Policy Password Cracker Online Online Backup Services Greenbone Vulnerability Scanner Chapter 14 Quiz
Week 15 11/24 - 11/30	Module 15 Information Security Management Week 15 Discussion: Lessons Learned Discussion	Semester Project

Week 16 12/01 - 12/07	Module 15 Information Security Management Week 16 Semester Project Presentation Discussion	Review: Chapter 15 PowerPoints, Reinforce, Practice Annual Credit Report Suritaca IDS IPS Module 15 Quiz
Finals 12/08 - 12/12		CyberSecurity Post Assessment Semester Project Final Submission

Academic Integrity

The academic integrity policy for this course includes the Institutional Academic Integrity Policy listed at the end of this document.

1. Do your own work.
2. You can ask for help if you get stuck. It is OK to have a study buddy to help with problems or issues. It is not OK to turn in the same assignment as someone else.
3. If you use someone else’s work for a small quote or reference, cite the source.
4. Use your own words.
5. Do your own work. We are here to learn. You can’t learn without doing the work.

Artificial Intelligence (AI)

1. AI (ChatGPT, etc.) is a tool, just like a pencil, a computer, or Google. All work submitted must be your own. You may not submit any work generated by an AI program as your own.
2. You will be working with AI in the workplace. Certain homework assignments will involve the use of AI technologies. Give credit to the source you use. The aim of these assignments is to familiarize you with practical AI applications.

Minor Violations: First offense: Grade of 0 for the assignment.

Major Violations: Second offense: Grade of F for the class.

Do your own work.

Assignment Creativity

If your assignment submission meets the requirements of the tutorial or assignment, you are free to embellish the resulting work as much as you wish before submission.

WNCC Master Syllabus Contents

This link contains the common WNCC Syllabus policies.