Ethical Hacking INFO-2650 Course Syllabus Spring 2026

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

Contents

Keys to Success: Show Up, Work Hard, Ask for Help

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, 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 Meeting Times

- **Face to Face Class Location:** Scottsbluff Campus, Room D1
- **Scheduled Online Location:** Zoom link in Blackboard
- **Time:** Tue, 9:30-10:45 am

Catalog Description

This course provides an in-depth understanding of how to effectively protect computer networks. Students learn the tools of penetration testing and network defense methodologies used by ethical hackers. The course provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber-attacks. The course shows how to find and research updated computer security resources that describe new vulnerabilities and innovative methods to protect networks.

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, network, security, penetration testing, and ethical terms and concepts.
2. Explain the role of security, risk mitigation, penetration testing, and network defense in a network environment.
3. Explain and give examples of how to prepare, document, and perform ethical penetration testing and network defense.
4. Show and demonstrate how to penetrate, test, and remediate a network in an ethical manner.

5. Explain and demonstrate how to prepare a vulnerability assessment and network defense.
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 computer, network, security, penetration testing, ethical terms, and concepts. [GE 1, 2; INFO 4]
2. Explain the role of security, risk mitigation, penetration testing, and network defense in a network environment. [GE: 1, 2; INFO 4]
3. Prepare, document, and perform ethical penetration testing and network defense in an ethical manner. [GE 1, 2: INFO 3, 4]
4. Explain and demonstrate how to prepare a vulnerability assessment and network defense. [GE 2, 3; INFO 4]
5. Explain and demonstrate how to prepare a vulnerability assessment and network defense. [GE 1, 2; INFO 4]
6. Self-direct their learning while gaining an ongoing interest in learning more about ethical security defense. [GE 5]

Instructional Materials

Hands-On Ethical Hacking and Network Defense, Simpson-Antill, Cengage Learning, Current Edition

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

Required MindTap Access Code (Includes the eBook and labs)

- 9780357700037 Cengage Unlimited (4 month access)
- 9780357700044 Cengage Unlimited (12 month access)
- 9780357700051 Cengage Unlimited (24 month access)

The textbook can be purchased at: Cougar Bookstore, Scottsbluff Campus, (308) 635-6066, or online at http://bookstore.wncc.edu

Other Materials

Computer with ability to run VirtualBox, or another virtualization software

Course Schedule

Course content and schedule may change.

Week	Learning Activities	Assignments
Week 1 01/13 - 01/19	Introduction Discussion Introduction to Course Chapter 1 Ethical Hacking Overview M 8:00-9:15 am: In Person & Online Classroom	Getting Started Activities in Blackboard Ethical Hacking Pre-Course Assessment Visualize: Introduction to Ethical Hacking Live Virtual Machine Lab Pre-Requisite Kali Linux Virtualization Install Python Chapter 1 Quiz
Week 2 01/20 - 01/26	Chapter 2 TCP/IP Concepts Review M 8:00-9:15 am: In Person & Online Classroom	Windows Virtualization Lab 3-2: Malware Threats Week 2 Linux Projects 1. Arpspoof MITM Chapter 2 Quiz
Week 3 01/27 - 02/02	Chapter 3 Network and Computer Attacks M 8:00-9:15 am: In Person & Online Classroom	Lab 4-1: Footprinting and Reconnaissance Week 3 Linux Projects Chapter 3 Quiz

	Think Aloud	
Week 4 02/03 - 02/09	Chapter 4 Footprinting and Social Engineering M 8:00-9:15 am: In Person & Online Classroom	Python ARP Monitor Lab 4-2: Social Engineering Reconnaissance Enumerate a Network with Nmap Week 4 Linux Projects Chapter 4 Quiz
Week 5 02/10 - 02/16	Chapter 5 Port Scanning M 8:00-9:15 am: In Person & Online Classroom Think Aloud	Lab 5-1: Scanning Networks Part 1 Video Assignment: Linux Directories Explained in 100 Seconds Python Gmail Email Python Hashing Tutorial Week 5 Linux Projects Chapter 5 Quiz
Week 6 02/17 - 02/23	Chapter 6 Enumeration M 8:00-9:15 am: In Person & Online Classroom	Python nmap Scanner 5. Bettercap Web GUI Python Email Spoofing
Week 7 02/24 - 03/02	Chapter 6 Enumeration M 8:00-9:15 am: In Person & Online Classroom Think Aloud	1. Python Network Scanner with Scapy 6. Wireshark Capture Login Information BeEF Client Side Attack Chapter 6 Quiz

Week 8 03/03 - 03/07	Chapter 7 Programming for Security Professionals M 8:00-9:15 am: In Person & Online Classroom	7. Detect ARP Spoofing Python Random Word Password Generator 2. Python Network Scanner with Scapy
03-10 – 03-16	Spring Break	
Week 10 03/17 – 03/23	Chapter 7 Programming for Security Professionals M 8:00-9:15 am: In Person & Online Classroom Think Aloud	Get Started with C++ (Thu) 3. Python Network Scanner with Scapy Install Metasploitable 2 Python Guess Password Chapter 7 Quiz
Week 11 03/24 – 03/30	Chapter 8 Desktop and Server OS Vulnerabilities M 8:00-9:15 am: In Person & Online Classroom	Linux Programming Activities (Thu) 1. Python Keylogger 4. Python Network Scanner with Scapy Nessus Vulnerability Scanner Chapter 8 Quiz
Week 12 03/31 – 04/06	Chapter 9 Embedded Operating Systems: The Hidden Threat M 8:00-9:15 am: In Person & Online Classroom Think Aloud	2. Python Keylogger (Thu) Python MITM Python Simple Network Client Server Metasploit Server Code Exploitation Chapter 9 Quiz
Week 13	Chapter 10 Hacking Web Servers	3. Python Keylogger (Thu)

04/07 – 04/13	M 8:00-9:15 am: In Person & Online Classroom	Python Ransomware Python Plain Text Password Cracker Metasploit FTP Vulnerability Whois Chapter 10 Quiz
Week 14 04/14 – 04/20	Chapter 11 Hacking Wireless Networks M 8:00-9:15 am: In Person & Online Classroom Think Aloud	4. Python Keylogger (Thu) PythonPing Network Scanner Website Security Assessment Webcam Hacking Hack a Wireless NetworkChapter 11 Quiz
Week 15 04/21 – 04/27	Chapter 12 Cryptography M 8:00-9:15 am: In Person & Online Classroom IT Career Discussion	5. Python Keylogger (Thu) Lab 12-1: Cryptography Python Hashed Password Cracker Python Cryptography Chapter 12 Quiz
Week 16 04/28 – 05/04	Chapter 13 Network Protection Systems M 8:00-9:15 am: In Person & Online Classroom Lessons Learned Discussion	6. Python Keylogger (Thu) PythonPing Network Scanner Threaded Python Port Scanner Chapter 13 Quiz
Finals 05/05 - 05/09		Chapter 14 Final Project

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)

AI is best used ethically and responsibly.

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. The aim of these assignments is to familiarize you with practical AI applications.
3. If an assignment permits AI: Include the AI name, the prompt and the result.
4. Do not pass AI work off as your own.

NOTE: If an assignment seems out of character or not in the style we have been using in class: you will receive a 0 until you contact the instructor to explain how you arrived at this code.

AI use indicators:

 No AI use: It is important for acquiring skills that you are able to do this assignment on your own.

 AI can be used as a debugger or tutor. Include the prompt and results.

 AI can be used as a code helper. Include the prompt and results.

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

As long as 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. This is where the real learning starts.

Attendance

In addition to the WNCC Attendance policy (in the WNCC Master Syllabus Contents) you are required to turn in your weekly notes to be considered attending this class.

WNCC Master Syllabus Contents

This link contains the common WNCC Syllabus policies.