University of Wisconsin-Stevens Point
College of Letters and Science
Department of Computing and New Media Technologies
Computer Information Systems
Networking Track

CIS361:
Information and Network Security

Dr. Patrick Seeling, Ph. D.
Science Building, Room B243
pseeling@uwsp.edu

Course Description

The course is structured into modules, with each module covering a part of the overall course content. You will gain an understanding of the major principles of computer, information, and network security. We will approach this topic by first looking at several security and legal principles. You will then learn how these apply – first for isolated desktop computers. We will then look at networked computers, networking security, and servers. Finally, you will investigate how these principles are applied and what common security breaches in a practical student project in the lab.

- **Prerequisites: CIS360 or instructor approval**
- **Rental course text: E. Cole, R. Krutz, and W. Conley – Network Security Bible. Wiley, 2005.**

Gathered data from student activities in this course will be part of an anonymous evaluation for research purposes. Please contact the instructor if you do not wish to have your data included.

Course Goals

At the end of the course, students will have a broad understanding of security concepts, how Linux or Windows clients can be hardened, how to secure networks, and how to prepare and respond in case of security breaches.

Course Outline and Outcomes

First Lecture

This module serves as a general introduction and overview of the course. It will provide guidelines on how to successfully complete the course.

Introduction and Security Principles and Management (Weeks 1-3)

This module introduces you to security as a process, security policies, and legal issues. At the end of this module, you will be able to:

- Explain the CIA approach
- Apply the general Information Systems Security Engineering cycle to a project
- Apply common planning for disaster and business interruption
- State some common law frameworks
- Give examples for security assessment and evaluation
- Explain the differences between access control methods

Reading assignment: chapters 1, 2, 3, and 18

Labs: Initial setup

Operating System and Client Security (Weeks 4-5)

In this module you will explore vulnerabilities and hardening of typical operating systems and user programs. At the end of this module, you will be able to:

- Identify different vulnerabilities of desktop computers
- Identify and configure rules for hardening a desktop computer
- Apply tools to harden a desktop computer

Reading assignment: chapters 4, 5

Labs: Users, groups, authentication, RBAC file permissions, anti-malware, bootdisk attack

---

Secret / Covert Communication Principles (Week 6)

This module introduces you to encryption and integrity checking methods, such as hashes, and covert communication means, such as steganography. At the end of this module, you will be able to:

- Explain the principles behind encryption and covert communications
- Use steganography for covert communication

Reading assignment: chapters 14, 15

Labs: file and file system encryption, integrity checking, and steganography

---

Network Security (Week 7-9)

In this module, you will get an overview of network types and intrusion detection for networks. At the end of this module, you will be able to perform:

- Browser hardening
- Firewall
- Understand and use VPN (IPSec/OpenVPN)
- Understand PKI

Reading assignment: chapters 6, 7, 8, 13, 16

Labs: network risks, firewalls, browser hardening,

Server Security (Week 10-11)

Servers are the typical heart of networks and you will be introduced to securing servers in this module. At the end of this module, you will be able to:

- Identify different vulnerabilities of servers
- Identify and configure rules for hardening a server
- Apply tools to harden a server

Chapters: 7, 9, 10

Labs: centralized user/group management, auditing, logging, HIDS

Detection and Response (Weeks 12-15)

This module introduces a broad variety of different attack possibilities, detection, and, finally, how to respond to them. At the end of this module, you will be able to:

- Use different security scanning tools
- Implement intrusion detection
- Apply all previously covered principles in a project

Chapters: 17, selective other readings

Labs: Network probing and monitoring, complete system configuration

Course Activities

Student Projects

Depending on the course, different student projects will be offered, some of them require you to have lab access, while others can be performed completely at home (you may have to install required software). Student projects are group-based and you are to work as a team – every team member has to know what and how the project goals were fulfilled. Questions will be asked from each team member.

You are encouraged to develop your own ideas for projects!

Online Discussions and Chats

The course will utilize online discussions/forums and chats during the course and especially for the student projects. Please limit your discussions to the appropriate sections. You are to solemnly use the online discussion and/or chat to communicate for your projects using the assigned project spaces in the discussion/chat areas of D2L.

The instructor will monitor conversations for appropriate content and reserves the right to delete inappropriate postings.

Professional Responsibilities

Upon graduation, you will be the amongst less than 30% of Americans that hold an academic degree. It is part of the responsibilities and duties of that degree to uphold high ethical and moral standards in society.

You should follow the outlined reading, class activities, and homework assignments, and be prepared for class. You are solely responsible for class attendance and participation and you are responsible for anything you missed. No make-up examinations will be given unless approved before the scheduled date or for validated medical or personal emergencies.

All assignments, quizzes, and lab sheets have a due date. You will typically have several days for their completion. If you do not complete items by the assigned due date, you have 2 days to submit late, but with reduced grade, see below.

Please see the University of Wisconsin-Stevens Point Student Academic Standards document for an overview of the university's policies and requirements. Also, refer to the professional societies of our area for definitions and how to properly cite other people's work:

- The IEEE: The Five Levels Of Plagiarism
- The ACM: ACM Policy and Procedures on Plagiarism

Written assignments will be checked for plagiarism and collaboration. Unless noted, you are to complete your assignments individually.

> ***If you use other people's work, you have to clearly point this out in any submitted work. Cheating and plagiarism will not be tolerated.***

Assessment, Points, and Grading

Each section of the course will have one or more online quizzes, which you are required to take in the allotted time frame, a maximum of 15 minutes. By their nature, online quizzes are open-book, which means that you are assumed to have fulfilled all reading assignments and know the content. Each quiz will be made available online at the end of a module and is worth 10 points. The quizzes will be available for multiple days; no submissions are allowed after the due date.

There will be several hands-on experiences allowing you to use your theoretical knowledge in a practical context. Each of these labs has additional graded questions and/or exercises. Lab worksheets will be made available online and the questions will have to be answered online as well. Each lab will be worth 10 points and you will have several days after the lab to complete the questions online; no submissions are allowed after the due date.

There will be one writing assignment worth 10 points for the initial course module. You have two days to submit after the due date, whereby the points you can earn are 50% on late day one, 25% on late day two, and 0% from day three onwards.

There is a comprehensive final exam, which will be completely online and cover the entire material of the course, including assignments and labs. The final exam will allow you to earn up to 3 points for each module, which will be added to your previous points for that module, up to the maximum number of points that were achievable per module.

Let q_i denote the points for quiz i you achieved out of Q quizzes, worth at most p_i points. Furthermore, let f_i denote the final exam part covering the same content as quiz q_i. The total points for the quizzes are then calculated after the final as

$$\sum_{i=1}^{Q} \min(p_i, q_i + f_i)$$

Mapping to Letter Grade

Your final letter grade will be awarded according to the following mapping scheme, based on the percentage of points that you have earned during the course. Please do not ask me to calculate this percentage for you – it's straightforward as follows.

Let P_t denote the maximum number of points that you could have achieved up to the current point in time during the course t and A_t denote the points that you actually achieved. Your current percentage of points is then calculated as

$$\frac{P_t}{A_t} \cdot 100$$

When mapped to letter grades, the following fixed mapping scheme will be applied.

Letter Grade	*Percent of Points*
A	>= 94
A-	>= 90
B+	>= 87
B	>= 84
B-	>= 80
C+	>= 77
C	>= 74
C-	>= 70
D+	>= 67
D	>= 60
F	< 60