CPS 155: Introduction to Cyber Security

CPS 155
Introduction to Cyber Security
(3 credits)
Class Size: 10-25

Faculty: Ehat Ercanli, Associate Professor, Syracuse University
Administrative Contact: Tavish Van Skoik, Assistant Director, Project Advance

* CPS 155 is NOT accepting applications for training at this time

Course Catalog Description

Introductory concepts of: network organization and operation security. Differentiate among physical, organizational and personal security. Introduce mechanisms and history of software, hardware and OS security. Significant hands-on laboratory component with demonstrations and projects.

Course Overview

CPS 155 is a course that presents fundamental concepts of security, network organization, and operation.

It will introduce mechanisms and the history of software, hardware, and OS security. Students will differentiate between physical, organizational, and personal security. Introduction to Cybersecurity consists of two lectures per week based on reference text and course notes. In addition, two hands-on

labs will be conducted each week based on the Lab Manual for the course. Students will receive one homework assignment and one quiz each week. The homework assignment will be due the first class of the following week. There are no prerequisites for this course.

Weeks 1-3: How Does a Network Work? How Does Your Computer System Work (Hardware and OS)? Binary, hex, and information representation (ASCIIÉ); Serial Communication and modems; Network fundamentals (Chapter 9, p. 195); Wireless and instant messaging (Chapter 12, p. 287)

Weeks 4-6: What is Security? General security concepts (Chapter 2, p. 19); Operational and organizational security (Chapter 3, p. 43); Role of people in security (Chapter 4, p. 63); Computer ethics; The impact of physical security on network security (Chapter 8, p. 181); Infrastructural security (Chapter 10, p. 215)

Weeks 7-9: How Do We Detect and Respond to Attacks on the Network? Disaster recovery, business continuity, and organizational policies (Chapter 19, p. 483); Risk management (Chapter 20, p. 511); Change management (Chapter 21, p. 533); Privilege management (Chapter 22, p. 549); Computer forensics (Chapter 23, p. 569); Security and law (Chapter 24, p. 587)

Weeks 10-11: How is the Network Vulnerable, and What Are the Threats? Attacks and malware (Chapter 15, p. 395); E-mail attacks (Chapter 16, p. 423); Web-based attacks (Chapter 17, p. 439)

Weeks 12-13: How Do We Prevent Harm to the Network? Cryptography (Chapter 5, p. 77); Public key infrastructure (Chapter 6, p. 107); Intrusion detection systems (Chapter 13, p. 309); Security baselines (Chapter 14, p. 337); Software development (Chapter 18, p. 469)

Pre- / Co-requisites

- Be able to use a computer
  - Activate applications
  - Utilize the internet
  - Send and receive email
  - Have a basic literacy in computer operation
- Three years of high school mathematics
  - Basic Algebra
  - Introduction to logic
  - Problem-solving skills utilizing unknowns

Course Objectives

By the end of the course, students will be able to understand how a network functions, monitor a network's functions and performance, control a network's configuration, determine what security is and how it relates to a network, detect and respond to an attack on a network, determine if a network is vulnerable to an attack, identify the threats to a network, prevent harm to a network, and analyze the impact of the protection.

Laboratory

N/A

Required Materials

Principles of Computer Security, Comp TIA Security+ and Beyond, 4th Edition; Conklin, White,
Cothren, Williams, Davis & Schou
ISBN: 9780071835978 (McGraw-Hill, Marjie Sullivan: 315-488-4167 or 800-338-3987)
Computer Security Lab Manual, 4th Edition; Nestler, Conklin,

White & Hirsch
ISBN: 9780071836555 (McGraw-Hill, Marjie Sullivan: 315-488-4167 or 800-338-3987)

Instructor Recommendations

N/A