ROCK VALLEY COLLEGE
BUSINESS/COMPUTERS AND INFORMATION SYSTEMS DIVISION

Fall 2015

Instructor : Chuck Konkol
Title: Associate Professor
Office Phone : 815-921-3164
Office Hours:
T | 3:30p-4:30p/6:00p-7:00p, Th | 3:15p - 4:15p/6:00p-7:00p
E-mail: c.konkol@rockvalleycollege.edu

PCT 130 – Introduction to Network Security Fundamentals **PCS: 1.2**
IAI: None

Course Description:
This course is designed for students and professionals interested in understanding the field of network security and how it relates to other areas of Information Technology. The course covers physical security, wireless technologies, Intrusion Detection Systems, Remote Access, Web security, E-mail, authentication, cryptography and various attack methodologies such as Denial of Service (DoS), man-in-the-middle and Malware.

PREREQUISITE: PCT 101 or equivalent computer experience.

Credits: 3 semester hours **Lecture:** 3 **Lab:** 0

GENERAL EDUCATION LEARNING OUTCOMES

This course addresses the following general education learning outcome(s):

	·	Communicate effectively.
	·	Integrate technology into all fields of knowledge and expression.
X	·	Demonstrate competency in critical thinking.
	·	Respect and work effectively with persons of diverse backgrounds and abilities.
	·	Demonstrate the behaviors of ethical and socially responsible citizens.
	·	Demonstrate personal wellness

COURSE OBJECTIVES:

Upon successful completion of the course, the learner will be able to:

1. Recognize common attacks and probes against a server
2. Develop useful strategies for securing File, Web and E-mail servers.
3. Recognize and be able to differentiate and explain methods of authentication
4. Understand the concept of and know how to reduce the risks of social engineering
5. Understand the concept and significance of auditing, logging and system scanning
6. Recognize and understand the administration many types of remote access technologies including but not limited to: VPNs, IPSec, RADIUS & TACACS.
7. Recognize and understand the wireless technologies and concepts such as 802.11, WEP, and WAP technologies.
8. Understand security concerns and concepts of networking devices such as: firewalls, routers, switches, modems and workstations.
9. Be able to identify and explain the different kinds of cryptographic algorithms.
10. Understand the application of the concepts of physical security.
11. Understand the security implications of disaster recovery

Grading Rationale:

Students will be evaluated according to performance in the following categories:

1. Three exams

2. Quizzes at the instructor's discretion

3. Lab activities and hands-on performance tests

4. In-class assignments, homework, and class participation

5. A research paper and oral presentation

REQUIRED READINGS (AND SUPPLIES)

Ciampa, Security Guide to Network Security Fundamentals, Cengage, 4th Edition, ISBN: 9781111640125

Flash drive or other portable storage device

NOTIFICATION OF SERVICES FOR STUDENTS WITH DISABILITIES

"If you have a documented disability and would like to request accommodation and/or academic adjustments, contact the Disability Support Services Coordinator. You should contact the coordinator as soon as a need for accommodation is known so that implementation can occur as soon as possible. The coordinator's office is G87 in the ERC. The telephone number for this office is 921-2356."

DISCLAIMER

Circumstances may require some changes to this syllabus.

DATE SUBMITTED

Spring, 2015; C.Konkol