Montgomery County Community College
CIS 275
Network Security Fundamentals
3-2-2

COURSE DESCRIPTION:
This course will introduce students to the basic elements of establishing a secure network, including security objectives, security architecture, security models and security layers. Students will analyze what elements contribute to high quality risk management, network security policy, and security training. This course focuses on the five security keys: Confidentiality, Integrity, Availability, Accountability, and Auditability. Successful completion of this course prepares students to take appropriate industry certifications in the security field.

REQUISITES:
Previous Course Requirements
- CIS 170 Introduction to Networks (Cisco Semester 1)

Concurrent Course Requirements
None

LEARNING OUTCOMES Upon successful completion of this course, the student will be able to:	LEARNING ACTIVITIES	EVALUATION METHODS
1. Describe the typical sources of computer security breaches.	Lecture Discussion Hands-On Lab Exercises Homework Assignments (Including Written Reports) Group Projects	Hands-On Lab Exercises Quizzes and Exams
2. Explain the basic principles of user authentication and cryptography.	Lecture Discussion Hands-On Lab Exercises Homework Assignments (Including Written Reports) Group Projects	Hands-On Lab Exercises Quizzes and Exams
3. Demonstrate and apply techniques for configuring networks to prevent intrusions by hackers and cyber-terrorists.	Lecture Discussion Hands-On Lab Exercises Homework Assignments (Including Written Reports) Group Projects	Hands-On Lab Exercises Quizzes and Exams

LEARNING OUTCOMES	LEARNING ACTIVITIES	EVALUATION METHODS
4. Prepare comprehensive plans of defense strategies to secure a network from unauthorized users.	Lecture Discussion Hands-On Lab Exercises Homework Assignments (Including Written Reports) Group Projects	Hands-On Lab Exercises Quizzes and Exams

At the conclusion of each semester/session, assessment of the learning outcomes will be completed by course faculty using the listed evaluation method(s). Aggregated results will be submitted to the Associate Vice President of Academic Affairs. The benchmark for each learning outcome is that *70% of students will meet or exceed outcome criteria*.

SEQUENCE OF TOPICS:

1. Explain the basics principles of data communications including:
    a. Internet protocol (IP)
    b. Transmission control protocol (TCP)
    c. Data Link and Physical Layer Communications
    d. Domain name system (DNS)
2. Policy, Ethics, Laws and Compliance
    a. Explain the importance of risk related concepts
    b. Implement appropriate risk mitigation strategies
    c. Importance of security related risk awareness and training
    d. Security policy training and procedures
    e. Existing US and International Laws and standards
    f. Compliance with laws, best practices and standards
3. Describe methods for identifying the following attacks and vulnerabilities:
    a. Authentication attacks
    b. Identity attacks
    c. Denial of Service Attacks
    d. Malicious Code (Malware) Attacks
4. Explain cryptography methods and techniques including:
    a. Encryption algorithms
    b. Cipher blocks
    c. Public key cryptography
    d. Key distribution
    e. Digital signatures
5. Describe appropriate security procedures to control computer access and authentication
6. Discuss strategies for hardening computer systems (closing vulnerabilities)
7. Describe common procedures used to secure network infrastructure
8. Explain the principles and strategies used to establish appropriate Internet security including advanced communication protocols such as:
    a. FTP
    b. Remote access (including VPNs)
    c. Wireless networks

9. Explain the basic principles of cryptography
10. Demonstrate techniques for using and managing encryption keys
11. Discuss the principles of good operational security
12. Explain how to create a Security Policy, and procedures related to computer security
13. Explore strategies of establishing operating system security on the following operating systems:
    a. Windows
    b. Linux
    c. Novell
14. Discuss various network security professional certifications

LEARNING MATERIALS:

Ciampa, Mark. (2012). *Security+ Guide to Networking Security Fundamentals* (4th ed.). Course Technology, ISBN# 9781111640125

Cretaro, Paul. (2012). *Lab Manual for Security+ Guide to Network Security Fundamentals* (4th ed.) Course Technology ISBN 9781111640132

Other learning materials may be required and made available directly to the student and/or via the College's Libraries and/or course management system.

COURSE APPROVAL:

Prepared by: Alan Evans Date: 3/2006
VPAA/Provost Compliance Verification: Dr. John C. Flynn, Jr. Date: Fall, 2006

Revised by: Kathleen Kelly Date: 7/12/2012
VPAA/Provost or designee Compliance Verification:
Victoria Bastecki-Perez, Ed.D. Date: 9/10/2013

Revised by: Anil Datta Date: 4/12/2016
VPAA/Provost or designee Compliance Verification:
Victoria Bastecki-Perez, Ed.D. Date: 6/2/2016

This course is consistent with Montgomery County Community College's mission. It was developed, approved and will be delivered in full compliance with the policies and procedures established by the College.