

Alexandria Technical and Community College

CVNP 2615: Security Fundamentals

A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: 2

Lab Hours/Week: 2

OJT Hours/Week: *.*

Prerequisites: None

Corequisites: None

MnTC Goals: None

This course explores the field of network security and its relationship to other areas of information technology. This course provides the theoretical and historical background necessary to understand the various types of risks as well as the hands-on, practical techniques for working in the cyber-security field in the twenty-first century.

B. COURSE EFFECTIVE DATES: 04/15/2020 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

1. Malware and social engineering attacks
2. Application and network attacks
3. Vulnerability assessment and mitigating attacks
4. Host, application, and data security
5. Administering a secure network
6. Wireless network security
7. Access control fundamentals
8. Authentication and account management
9. Basic cryptography
10. Advanced cryptography
11. Business continuity
12. Risk mitigation

D. LEARNING OUTCOMES (General)

1. The learner will explore the technologies used and principles involved in creating a secure computer networking environment.
2. The learner will understand authentication, the types of attacks and malicious code that may be used against a network, the threats and countermeasures for e-mail, web applications, remote access, and file and print services.
3. The learner will understand intrusion detection systems, firewalls, and physical security concepts and will understand the daily tasks involved with managing and troubleshooting those technologies.

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted