Inver Hills Community College

ITC 2810: CCNA Cybersecurity Operations

A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: 2

Lab Hours/Week: 2

OJT Hours/Week: *.*

Prerequisites:
This course requires both of these prerequisites
ITC 2000 - PC Hardware and Software (A+) (Minimum grade: 2.0 GPA Equivalent)
ITC 1480 - Linux Essentials

Corequisites: None

MnTC Goals: None

Provides an introduction to the knowledge and skills used by security analysts working on a Security Operations Centers (SOC) team. These teams keep a vigilant eye on security systems, protecting their organizations by monitoring, detecting, investigating, analyzing, and responding to cybersecurity threats and events. This course is designed to prepare you for the Cisco CCNA Cyber Ops industry certification exams. Prerequisites: ITC 1480 or test out, ITC 2000.

B. COURSE EFFECTIVE DATES: 08/01/2019 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

1. Cybersecurity and the SOC (7.5%)
2. Windows & Linux Operating Systems (15%)
3. Network Protocols, Services & Infrastructure (16%)
4. Principles of Network Security (7.6%)
5. Network Attack Monitoring, Analysis, and Protection (16%)
6. Cryptography and PKI (7.6%)
7. Endpoint Security & Analysis (7.5%)
8. Security Monitoring (7.6%)
9. Intrusion Data Analysis (7.6%)
10. Incident Response & Handling (7.6%)

D. LEARNING OUTCOMES (General)

1. Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
2. Explain the role of the Cybersecurity Operations Analyst in the enterprise.
3. Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
4. Explain the features and characteristics of the Linux Operating System.
5. Analyze the operation of network protocols and services.
6. Explain the operation of the network infrastructure.
7. Classify the various types of network attacks.
8. Use network monitoring tools to identify attacks against network protocols and services.
9. Use various methods to prevent malicious access to computer networks, hosts, and data.
10. Explain the impacts of cryptography on network security monitoring.
11. Explain how to investigate endpoint vulnerabilities and attacks.
12. Evaluate network security alerts.
13. Analyze network intrusion data to identify compromised hosts and vulnerabilities.
14. Apply incident response models to manage network security incidents.

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

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted