Inver Hills Community College

ITC 2830: Implementing Cisco Network Security (CCNA Security)

A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: 2

Lab Hours/Week: 2

OJT Hours/Week: *.*

Prerequisites:
ITC 2520 - Switching, Routing, and Wireless Essentials (CCNA 2) (Minimum grade: 2.0 GPA equivalent); OR
CNT 2520 - Routing Protocols and Concepts (CCNA 2) (Minimum grade: 2.0 GPA equivalent); OR
ITC 2515 - Introduction to Networks and Routing and Switching Essentials (CCNA 1/2)

Corequisites: None

MnTC Goals: None

Provides an introduction to the core security concepts and skills needed for installation, troubleshooting, and monitoring of network devices to maintain the integrity, confidentiality, and availability of data and devices. An emphasis on practical experience develops specialized skills for securing networks. This course assists in preparation for the Implementing Cisco Network Security (IINS) certification exam leading to the Cisco CCNA Security certification.

B. COURSE EFFECTIVE DATES: 08/26/2013 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

1. Authentication, Authorization, and Accounting (9%)
2. Implementing Firewall Technologies (9%)
3. Implementing Intrusion Protection (9%)
4. Securing the Local Area Network (9%)
5. Cryptographic Systems and Cryptography (9%)
6. Implementing Virtual Private Networks (9%)
7. Implementing and Advanced Adaptive Security Appliances (19%)
8. Managing a Secure Network (9%)
9. Securing Network Devices (9%)
10. Modern Network Security Threats (9%)

D. LEARNING OUTCOMES (General)

1. Students will practice business soft skills including written, active listening, and oral presentation.
2. Describe, configure, and troubleshoot AAA on Cisco routers using local router database and server-based ACS or Identity Service Engine (ISE)
3. Implement zone-based IOS firewall technologies to secure network perimeter
4. Implement IOS based IPS to mitigate attacks on networks
5. Describe common layer 2 and end point attacks and configure mitigation for them
6. Describe secure cryptographic systems and algorithms including hashes, HMACs, ciphers, and PKI
7. Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
8. Describe and implement secure Virtual Private Networks on IOS based devices
9. Implement a basic ASA firewall and NAT configuration using the CLI
10. Describe modern threats to a secure network
11. Implement an ASA firewall configuration and Clientless and AnyConnect VPNs using ASDM
12. Test network security and create a technical security policy
13. Configure and troubleshoot secure network devices

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

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted