Revised Summer 2016

ITN 262
Network Communication, Security and Authentication

COURSE OUTLINE

Prerequisites:

Prerequisites: TEL 151

Course Description: (must be word-for-word from the College Catalog)
Covers an in-depth exploration of various communication protocols with a concentration on TCP/IP. Explores communication protocols from the point of view of the hacker in order to highlight protocol weaknesses. Includes Internet architecture, routing, addressing, topology, fragmentation and protocol analysis, and the use of various utilities to explore TCP/IP.

Semester Credits: 4 **Lecture Hours: 4**

VIRGINIA WESTERN COMMUNITY COLLEGE
PO Box 14007
Roanoke, VA 24038
(540)-857-7273

Revised Summer 2016

ITN 262 Network Communication, Security and Authentication

Course Objectives

At the completion of this course, the student should be able to:

- Explain network threats, mitigation techniques, and the basics of securing a network
- Secure administrative access on Cisco routers
- Secure administrative access with AAA
- Implement firewall technologies to secure the network perimeter
- Configure IPS to mitigate attacks on the network
- Describe LAN security considerations and implement endpoint and Layer 2 security features
- Describe methods for implementing data confidentiality and integrity
- Implement secure virtual private networks
- Implement an ASA firewall configuration using the CLI
- Implement an ASA firewall configuration and VPNs using ASDM
- Test network security and create a technical security policy

VIRGINIA WESTERN COMMUNITY COLLEGE
PO Box 14007
Roanoke, VA 24038
(540)-857-7273

Revised Summer 2016

ITN 262 Network Communication, Security and Authentication

Required Materials:

Primary Text: Cisco Online Curriculum: CCNA Security 2.0. Students enrolled in this course will have password-restricted access to the curriculum.

Packet Tracer Software (provided by netacad.com)

VIRGINIA WESTERN COMMUNITY COLLEGE
PO Box 14007
Roanoke, VA 24038
(540)-857-7273

ITN 262 Network Communication, Security and Authentication

Topical Description: (Outline chapters and sections to be covered in the book – may include timeline)

- Chapter 1. Modern Network Security Threats
  - 1.1 Securing Networks
  - 1.2 Network Threats
  - 1.3 Mitigating Threats

- Chapter 2. Securing Network Devices
  - 2.1 Securing Device Access
  - 2.2 Assigning Administrative Roles
  - 2.3 Monitoring and Managing Devices
  - 2.4 Using Automated Security Features

- Chapter 3. Authentication, Authorization and Accounting
  - 3.1 Purpose of AAA
  - 3.2 Local AAA Authentication
  - 3.3 Server-Based AAA
  - 3.4 Server-Based AAA Authentication
  - 3.5 Server-Based AAA Authorization and Accounting

- Chapter 4. Implementing Firewall Technologies
  - 4.1 Access Control Lists
  - 4.2 Firewall Technologies
  - 4.3 Zone-Based Policy Firewalls

- Chapter 5. Implementing Intrusion Prevention
  - 5.1 IPS Technologies
  - 5.2 IPS Signatures
  - 5.3 Implement IPS

- Chapter 6. Securing the Local Area Network
  - 6.1 Endpoint Security
  - 6.2 Layer 2 Security Considerations

VIRGINIA WESTERN COMMUNITY COLLEGE
PO Box 14007
Roanoke, VA 24038
(540)-857-7273

- Chapter 7. Cryptographic Systems
  - 7.1 Cryptographic Services
  - 7.2 Basic Integrity and Authenticity
  - 7.3 Confidentiality
  - 7.4 Public Key Cryptography

- Chapter 8. Implementing Virtual Private Networks
  - 8.1 VPNs
  - 8.2 IPsec VPN Components and Operation
  - 8.3 Implementing Site-to-Site IPsec VPNs with CLI

- Chapter 9. Implementing the Cisco Adaptive Security Appliance
  - 9.1 Introduction to the ASA
  - 9.2 ASA Firewall Configuration

- Chapter 10. Advanced Cisco Adaptive Security Appliance
  - 10.1 ASA Security Device Manager
  - 10.2 ASA VPN Configuration

- Chapter 11. Managing a Secure Network
  - 11.1 Network Security Testing
  - 11.2 Developing a Comprehensive Security Policy