

# **CNT 5415 Practical Applied Security**

## **Catalog Description**

Hands-on training in practical installation and maintenance of secure systems, including such topics as security configuration, DMZs, firewalls, anti-virus software, and hardware security modules. (3 credits)

## **Prerequisites**

Graduate Standing

## **Type**

Required for MS-Cybersecurity

## **Course Objectives**

This course examines the major network security tools in use today, with the idea that firewalls are most effective when backed by thoughtful security planning, well-designed security policies, and integrated support from anti-virus software, intrusion detection systems, and related tools. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The course will provide numerous realistic projects and cases incorporating cutting-edge technology and current trends, giving students the opportunity to hone and apply the knowledge and skills they will need as working professionals.

## **Topics**

- Introduction to Information Security
- Security Policies and Standards
- System Hardening
- Authenticating Users
- Building DMZ infrastructure
- Introduction to Firewalls
- Packet Filtering
- Firewall Configuration and Administration
- Working with Proxy Servers and Application-Level Firewalls
- Concepts and establishing Proxy and Reverse-Proxy Servers
- Implementing the Bastion Host
- Encryption – The Foundation for the Virtual Private Network
- Setting Up a Virtual Private Network

## **Textbook**

Michael E. Whitman, Herbert J. Mattord, and Andrew Green, *Guide to Firewalls and VPNs, Third Edition*. Course Technology, Cengage Learning, 2012, ISBN-13 978-1-111-13539-3.

## **Last Update**

Alexander Pons, 1/21/2014