

## **CYSE 280 Windows System Management and Security**

### **Course Description**

This course introduces tools and techniques for configuring, managing, and implementing Windows and its security-related features.

Students will install, configure, manage, and secure Windows client & server operating systems, and related networking environment using a variety of software tools.

This course also details how to mitigate malware threats, identify security issues using auditing and the Advanced Threat Analysis feature in Windows Server, secure your virtualization platform, and use new deployment options to enhance security.

Topics include designing Active Directory, authentication for Windows, group security and policy, service security, remote access security, planning a public key infrastructure, securing file resources, Internet Protocol Security, and additional Windows security topics.

### **Exit skills**

Upon completion of this course, students will be able to:

#### **KNOWLEDGE**

- 1.1. Describe the fundamental concepts of Operating Systems
- 1.2. Describe General Security Concepts and related terminology

#### **SKILLS**

##### **Part1**

- 2.1 Install and configure Windows Server
- 2.2 Configure Windows Active Directory
- 2.3 Configure Windows Services such as DNS, DHCP, File, and Storage
- 2.4 Managing System Reliability and Availability

##### **Part2**

- 2.5 Secure hosts, applications, and network traffic.
- 2.6 Manage malware and social engineering threats.
- 2.7 Securing and administering a Network

#### **VALUE**

- 3.1. Work collaboratively and ethically to achieve organizational goals

**Note:** Course overview and module descriptions adapted from Old Dominion University (n.d.), *Windows System Management and Security, CYSE 280 syllabus materials*.