Sinclair Community College
444 E. Third St.
Dayton, OH 45402

Master Syllabus

CIS 2630 - Securing a Windows Network Environment

Division: Business and Public Services

Department: Computer Information Systems

Credit Hour Total: 3.0 **Lecture Hrs:** 3.0

Prerequisite(s): CIS 2510

Date Revised: February 2016

Course Description:

Successfully plan, build and secure systems for a Microsoft Windows Server environment. The primary purpose of this is course is to provide hands on experience using real enterprise class server hardware and software. Also includes sections on introductory forensics and securing servers with penetration testing.

General Education Outcomes:

- Critical Thinking/Problem Solving Competency
- Computer Literacy Competency

Course Outcomes:

Client computers
Secure client computers with file system permissions, Group Policy, and other baseline security measures.

Assessment Method: Locally developed exams
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

IPSec and SSL
Configure IPSec and SSL to help protect communication channels for both private and public servers.

Assessment Method: Locally developed exams
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Remote Access Servers (RAS), VPNs, and wireless networks
Implement security measures for RAS, VPNs, and wireless networks.

Assessment Method: Locally developed exams
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Network servers
Protect various network servers from unauthorized access.

Assessment Method: Locally developed exams
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

User and network authentication and certificates
Manage user and network authentication, certificates, and public key encryption.

Assessment Method: Locally developed exams
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Software integrity
Maintain software integrity with service packs, security updates, and hot fixes.

Assessment Method: Locally developed exams
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Network events
Monitor events, detect network intrusions, and implement prevention and recovery measures.

Assessment Method: Locally developed exams
Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Assessment Method: Simulations

Performance Criteria: Students will perform at a 75% or higher level on a locally developed rubric.

Outline:

1. Introduction to security related topics
1.1 Confidentiality, integrity and availability (CIA) of systems and data
1.2 Role of policy, education, training and awareness, and technology in CIA
1.3 Government initiatives to improve security, e.g., PDD 63
1.4 Increasing awareness of security in all networked environments
1.5 Secure coding practices
1.6 Software lifecycle management practices

2. Configuring security policies
2.1 Security based on server roles (file server, print server, web server, domain controller, etc.)
2.2 Security based on client roles (desktop, laptop, kiosk)
2.3 Using security templates
2.4 Configuring security settings

3. Deploying security policies
3.1 Understanding security templates
3.2 Deploying security templates via Group Policies, command line tools and scripting
3.3 Customizing default templates to meet local needs
3.4 Configuring security options (account lockout, password policies, audit policies, user rights, access control lists, etc.)
3.5 Analyzing security configurations using vendor provided tools (MBSA and command line tools)
3.6 Managing audit/event logs

4. Troubleshooting security policies
4.1 Security policy inheritance
4.2 Policy application order
4.3 Security group usage
4.4 Filtering application of policy
4.5 Exception to normal processing, e.g., Block inheritance and no override

5. Planning and deploying patch management
5.1 Understanding threats, vulnerabilities and attacks
5.2 Types of threats, e.g., Denial of Service, brute force, buffer overflow, man-in-the-middle, spoofing, social engineering, etc.
5.3 Software update strategies and practices
5.4 Using vendor provided tools to manage software updates, e.g., SUS, WSUS, SMS and Group Policies
5.5 Software change management
5.6 Providing updates via batch processes, e.g., slipstreaming or scripting
5.7 Backup and recovery strategies

6. Securing network communications
6.1 IPSec concepts
6.2 IPSec deployment including various modes and authentication methods
6.3 Default IPSec policies in Active Directory and on local machines
6.4 IPSec policies including encryption levels and message integrity methods
6.5 IPSec sub protocols (AH, ESP and IKE)
6.6 Using certificates and IPSec
6.7 Other issues affecting communication security

7. Troubleshooting IPSec policies
7.1 IPSec policy precedence
7.2 Using vendor supplied tools, e.g., Resultant Set of Policy (RSOP), IPSec Monitor and IPSec logging, to troubleshoot IPSec
7.3 Using IPSec and Network Address Translation (NAT) together
8. Public Key Infrastructure
8.1 Understanding terminology and fundamental concepts: hash algorithms, symmetric and asymmetric cryptography, plaintext, cipher text, digital signatures, etc.
8.2 Certification Authorities (CAs)
8.3 Understanding CA hierarchies
8.4 Using third party CAs, e.g., Verisign and Thawte
8.5 Installing certificate services and creating a CA hierarchy
8.6 Creating and managing Certificate Revocation Lists (CRLs)
8.7 Exporting and importing certificates
8.8 Creating and managing trust lists
8.9 Deploying certificates to users and/or computers

9. Securing remote access
9.1 Using SSL to secure information exchanges with web servers
9.2 Configuring a web server to use certificates and SSL
9.3 Authentication methods, e.g., PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP
9.4 Challenge response methods of authentication
9.5 Multifactor authentication, e.g., biometric, smart cards, etc.
9.6 Virtual Private Networks (VPNs)
9.7 Tunneling protocols and encryption methods
9.8 Network Address Translation and VPNs
9.9 Configuring Routing and Remote Access Server (RRAS) policies and profiles

10. Securing wireless networks
10.1 Terminology and concepts: war driving, war chalking, WEP, WPA, SSID, 802.11 standards, etc.
10.2 Authentication in a wireless network: Open, shared key, 802.1x and RADIUS
10.3 Encryption on wireless networks: WEP and 802.1x
10.4 Wireless policies in Active Directory
10.5 Configuring client support for wireless support