COURSE INFORMATION FORM

DISCIPLINE: Computer Science/Information Systems
COURSE TITLE: Network Security II

CR.HR: 4.0  LECT HR: 3.0  LAB HR: 2.0  CLIN/INTERN HR: 0  CLOCK HR: 0

CATALOG DESCRIPTION
This course focuses on the overall security processes in a network with particular emphasis on hands-on skills in the following areas: Security policy design and management; Security technologies, products and solutions; Firewall and secure router design, installation, configuration, and maintenance; Intrusion Detection System (IDS) implementation using routers and firewalls; Virtual Private Network (VPN) implementation using routers and firewalls.

PREREQUISITES
CSIS 272

EXPECTED STUDENT OUTCOMES IN THE COURSE
Upon completion of this course, the student will be able to:
1. Explain advanced security vulnerabilities.
2. Explain and apply various cryptography measures to ensure privacy and confidentiality.
3. Describe and configure intrusion detection and monitoring on the routers and PIX Firewalls.
4. Demonstrate the ability to configure site-to-site VPNs on routers and PIX firewalls.
5. Demonstrate the ability to configure remote access VPNs between Cisco VPN Clients, routers and PIX Firewalls.
6. Design a network using appropriate security hardware, software, and configurations to protect against vulnerabilities and threats.
CLASS-LEVEL ASSESSMENT MEASURES

Student accomplishment of expected student outcomes will be assessed using the following measures. (Identify which measures are used to assess which outcomes.)

- End of chapter assessments (1 - 3)
- Final Exam (1 - 3)
- Skills Based assessment (3 - 6)

PROGRAM-LEVEL OUTCOMES ADDRESSED

General Education Outcomes
Specify which general education outcomes, if any, are substantially addressed by the course by completing the “Course/Program Assessment Matrix” to show the relationship between course and program outcomes and assessment measures.

Occupational Program Outcomes
Specify which occupational program outcomes, if any, are substantially addressed by the course by completing the “Course/Program Assessment Matrix” to show the relationship between course and program outcomes to assessment measures.
Individual instructors may order this outline as fits the needs of their individual courses. In addition, they may place more emphasis on some areas than on others. What is assured is that this particular list is covered in the course. Other topics may be added to a course as the instructor sees fit, and as time and interest allow. An *asterisk can be used to mark an item as optional.

I. Intrusion Detection and Prevention Technology
   A. Overview of Intrusion Detection and Prevention
   B. Inspection Engine
   C. Cisco IDS Devices

II. Configure Network Intrusion Detection and Prevention
   A. Cisco IOS Intrusion Prevention System
   B. Configure Attack Guards on the PIX Security Appliance
   C. Configure Intrusion Prevention on the PIX Security Appliance
   D. Configure Shunning on the PIX Security Appliance

III. Encryption and VPN Technology
   A. Encryption Basics
   B. Integrity Basics
   C. Implementing Digital Certificates
   D. VPN Topologies
   E. VPN technologies
   F. Internet Protocol Security (IPSec)

IV. Configure Site-to-Site VPN using Pre-Shared Keys
   A. Prepare a Router for Site-to-Site VPN using Pre-shared Keys
   B. Configure a Router for IKE Using Pre-shared Keys
   C. Configure a Router with IPSec Using Pre-shared Keys
   D. Testing and Verifying IPSec Configuration
   E. Configure a PIX Security Appliance Site-to-Site VPN using Pre-shared Keys

V. Configure Site to Site VPN using Digital Certificates
   A. Configuring Certificate Authority (CA) Support on a Cisco Router
   B. Configure an IOS Router Site-to-Site VPN Using Digital Certificates
   C. Configure a PIX Security Appliance Site-to-Site VPN Using Digital Certificates
VI. Configure Remote Access VPN
   A. Introduction to Cisco Easy VPN
   B. Configure the Easy VPN Server
   C. Configure Easy VPN Remote for the Cisco VPN Client 4.x
   D. Configure Cisco Easy VPN Remote for Access Routers
   E. Configure the PIX Security Appliance as an Easy VPN Server
   F. Configure a PIX 501 or 506 as an easy VPN client
   G. Configure the Adaptive Security Appliance to Support WebVPN

VII. Secure Network Architecture and Management
   A. Layer 2 Security Best Practices
   B. SDM Security Audit
   C. Router Management Center (MC)
   D. Simple Network Management Protocol (SNMP)

VIII. PIX Security Appliance Contexts, Failover, and Management
   A. Configure a PIX Security Appliance to Perform in Multiple Context Mode
   B. Configure PIX Security Appliance Failover
   C. Configure Transparent Firewall Mode
   D. PIX Security Appliance Management