COURSE INFORMATION FORM

DISCIPLINE: CSIS
COURSE TITLE: Network Security

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

CATALOG DESCRIPTION
This course helps students develop skills necessary to meet the growing demand for network security professionals. It provides a theoretically rich, hands-on introduction to network security in a logical sequence. Extensive hands on labs emphasize the skills needed to install, troubleshoot, monitor and secure network devices. The goals of this course are to prepare students for associate-level security careers, successful completion of IT related degree programs and prepare students for the CCNA Security certification.

PREREQUISITES
CSIS 113

EXPECTED STUDENT OUTCOMES IN THE COURSE (ESO)
Upon completion of this course, the student will be able to:
1. Explain and assess the security threats facing modern network infrastructures
2. Demonstrate how to secure Cisco routers
3. Apply AAA procedures on Cisco routers using local router databases and external servers
4. Assess and defend against threats to Cisco routers and networks using ACLs
5. Design, construct, and evaluate secure network management and reporting
6. Assess and defend against common Layer 2 attacks
7. Demonstrate the Cisco IOS firewall feature set
8. Demonstrate the Cisco IOS IPS feature set
9. Construct site-to-site IPSec VPNs
GENERAL EDUCATION OUTCOMES (ESO)
Specify which general education outcomes, if any, are substantially addressed by the course. Numbers in parentheses identify the Expected Student Outcomes linked to the specific General Education Outcome.

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>ESO</th>
</tr>
</thead>
</table>

PROGRAM-LEVEL OUTCOMES

CAREER AND TECHNICAL EDUCATION PROGRAM OUTCOMES
Specify which Career and Technical program outcomes, if any, are substantially addressed by the course by completing the “Career and Technical Education template” to show the relationship between course and program outcomes to assessment measures.

The student will demonstrate:

1. The ability to use industry specific software and/or apply troubleshooting skills to solve problems. (1-9)

2. The ability to work effectively in a team environment. (1-9)

CLASS-LEVEL ASSESSMENT MEASURES
Student accomplishment of expected student outcomes may be assessed using the following measures. (Identify which measures are used to assess which outcomes.)

Chapter Assessments (1-9)
Final Exam (1-9)
Skills Based Assessment (1-9)
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. Modern Network Security Threats
   A. Mitigation methods for common network attacks; Worm, Virus, Trojan Horse and others
   B. Cisco Self Defending Network architecture
   C. Cisco SDM Security Audit
   D. Cisco SDM One-Step Lockdown

II. Securing Network Devices
    A. Securing management access to routers
    B. Logging System information
    C. Privilege levels
    D. Securing router software

III. Authentication, Authorization and Accounting
     A. Functions and importance of AAA
     B. Features of TACACS+ and RADIUS AAA protocols
     C. AAA authentication
     D. AAA authorization
     E. AAA accounting

IV. Implementing Firewall Technologies
    A. Operational strengths and weaknesses of the different firewall technologies
    B. Firewall operations
    C. Zone Based Firewall

V. Implementing Intrusion Prevention
    A. Network based vs. host based intrusion detection and prevention
    B. IPS technologies, attack responses, and monitoring options
    C. Cisco IOS IPS operations using SDM Revised 06/23/09

VI. Securing the Local Area Network
    A. Layer 2 attacks
    B. Basic Catalyst switch security features

VII. Cryptographic Systems
     A. Cryptography methods
     B. IKE Protocol

VIII. Implementing Virtual Private Networks
      A. IPSec fundamentals
      B. VPN configuration

IX. Managing a Secure Network
    A. Security Policies
    B. Access Control Lists
    C. Filtering IP traffic
    D. IP address spoofing