ITCC 2343 COURSE SYLLABUS

COURSE DESCRIPTION:
Prepares Cisco-qualified students to take two Cisco certification exams: Managing Cisco Network Security and Cisco Secure PIX Firewall. Includes configuring secure Cisco routers and PIX firewalls. Focuses on overall network security processes.

PREREQUISITES, CO-REQUISITES and OTHER REQUIREMENTS:
Students should have a valid CCNA certification or have completed ITCC 2410 (CCNA 4).

TEXTBOOKS and REQUIRED MATERIALS/RECOMMENDED READINGS:
Cisco Online Curriculum at http://cisco.netacad.net

No Textbooks Required - Optional Books Below:

Required reading: Chapter 1 through Chapter 9

COURSE CONTENT:
CCNA Security equips students with the knowledge and skills needed to prepare for entry-level security specialist careers. This course is a hands-on, career-oriented e-learning solution that emphasizes practical experience. CCNA Security is a blended curriculum with both online and classroom learning. CCNA Security aims to develop an in-depth understanding of network security principles as well as the tools and configurations available. The following tools are covered:
● Protocol sniffers/analyzers
● TCP/IP and common desktop utilities
● Cisco IOS Software
● Cisco VPN client
● Packet Tracer (PT)
● Web-based resources

STUDENT LEARNING OUTCOMES:
Select appropriate security hardware, software, policies, and configurations based on an organization's assessment of its security vulnerabilities; perform advanced installation, configuration, monitoring, troubleshooting, maintenance, and recovery on Cisco IOS and PIX firewalls; configure intrusion detection feature on the Cisco IOS router and PIX firewalls; install and configure CSACS for AAA service on Cisco IOS and PIX firewalls; configure site-to-site VPNs between Cisco devices; and configure remote access VPNs between Cisco device and client's device to assure privacy and confidentiality.

PERFORMANCE OBJECTIVES:
● Describe the security threats facing modern network infrastructures
• Secure network device access
• Implement AAA on network devices
• Mitigate threats to networks using ACLs
• Implement secure network management and reporting
• Mitigate common Layer 2 attacks
• Implement the Cisco IOS firewall feature set
• Implement the Cisco IOS IPS feature set
• Implement site-to-site IPSec VPNs
• Administer effective security policies

METHODS OF MEASUREMENT (grade requirements):

Each chapter is followed with an Exam given online by the Cisco Academy System. The exams are graded by Cisco and scores are given immediately. Labs and study guides will be considered as a part of your attendance. Cheating, texting, IMing, and idly surfing the web will not be tolerated.

Online Chapter Exams 10%
Quizzes, Homework, etc 20%
Online Final Exam 25%
Skill-Based Final Exam 30%
Daily Grade & Labs 15%

100%

<table>
<thead>
<tr>
<th>Semester Average</th>
<th>NVC Grade</th>
<th>Cisco Academy</th>
<th>Status – Advance to next Academy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>90 – 100</td>
<td>A</td>
<td>A</td>
<td>Pass – Advance to the next level</td>
</tr>
<tr>
<td>80 – 89</td>
<td>B</td>
<td>B</td>
<td>Pass – Advance to the next level</td>
</tr>
<tr>
<td>70 – 79</td>
<td>C</td>
<td>C</td>
<td>Pass – Advance to the next level</td>
</tr>
<tr>
<td>60 – 69</td>
<td>D</td>
<td>F</td>
<td>Fail Cisco Academy – Retake current level</td>
</tr>
<tr>
<td>Below 60</td>
<td>F</td>
<td>F</td>
<td>Fail NVC and Cisco Academy</td>
</tr>
</tbody>
</table>

** NOTE: A successful Cisco Academy student will pass the Online Final Exam with a 70% or better grade and the Skills Based Final exam with an 80% or better. An opportunity to retake an alternate Skills Based Final Exam will be given, however, the grade for the second exam attempt will be reduced by 10% or 1 letter grade.**
**Grade Appeals Process:**

If a student has an objection to a grade received, the following is the process to dispute the grade and must be followed in this order:

1. Informal resolution with the instructor
2. Written appeal to the instructor
3. Written appeal to the department chair
4. Written appeal to the college committee

**Student Responsibilities:**

**A. Attendance**

Effective Spring Term 2010, student absences will be recorded from the first day the class meets. Regular and punctual attendance in all classes and laboratories, day and evening, is required. Students who are absent for any reason should always consult with their instructors. Course syllabi must provide specific information regarding attendance, including, for courses involving the internet, online activity that constitutes “attendance.” Also, both tardiness and early departure from class may be considered forms of absenteeism. In all cases, students will be held responsible for completion of course requirements covered in their absence. Additionally, it is the student’s responsibility to drop a course for nonattendance.

Course instructors establish policy with regard to attendance in their respective syllabi and may drop a student for excessive absences. Absences are considered excessive when more than 12.5 percent of the total contact hours of instruction in a semester, including lecture and lab, are missed. For example, in a three-credit-hour lecture class, students may be dropped after more than six contact hours of absences. In a four-credit-hour lecture/lab class, students may be dropped after more than eight contact hours of absences. Absences are counted regardless of whether they occur consecutively. In special programs with additional accreditation or certification standards, additional attendance requirements may be enforced but faculty must clearly explain these policies in their syllabi.

Students who stop attending class for any reason should contact the instructor and the college registrar to officially withdraw from the class. Students may be required to consult with an advisor or designee before dropping. Failure to officially withdraw may result in a failing grade for the course. It is the student’s responsibility to withdraw officially from a class by submitting a completed Withdrawal Form to the Admissions and Records Office.

**Additional Instructor Requirements:**

**College Policies:**

**A. All of the Alamo Colleges are tobacco free.**

**B. Alamo Colleges DPS Emergency Phone Numbers:**

- Emergency Phone: (210) 222-0911
- General Phone: (210) 485-0099
- Weather Phone: (210) 485-0189 (For information on college closures)

**Disability Access Statement** – In accordance with the Americans with Disabilities Act (ADA) and Section 504 of the Rehabilitation Act, it is the responsibility of the student to self-identify with the campus Disability Services office. Only those students with appropriate documentation will receive a letter of
The Alamo Colleges do not discriminate on the basis of race, religion, color, national origin, sex, age, or disability with respect to access, employment programs, or services. For further information, please contact the Disability Services office at (210) 486-4466 or visit the office located in the Cyprus Campus Center, Rm. 204. If you have specific needs, please discuss them privately with your instructor.

**GENERAL DESCRIPTION OF THE SUBJECT MATTER OF EACH LECTURE OR DISCUSSION:**

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Goals</th>
<th>WEEKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Modern Network Security Threats</td>
<td>Explain network threats, mitigation techniques, and the basics of securing a network</td>
<td>1</td>
</tr>
<tr>
<td>2. Securing Network Devices</td>
<td>Secure administrative access on Cisco routers</td>
<td>2</td>
</tr>
<tr>
<td>3. Authentication, Authorization and Accounting</td>
<td>Secure administrative access with AAA</td>
<td>3</td>
</tr>
<tr>
<td>4. Implementing Firewall Technologies</td>
<td>Implement firewall technologies to secure the network perimeter</td>
<td>4</td>
</tr>
<tr>
<td>5. Implementing Intrusion Prevention</td>
<td>Configure IPS to mitigate attacks on the network</td>
<td>5</td>
</tr>
<tr>
<td>6. Securing the Local Area Network</td>
<td>Describe LAN security considerations and implement endpoint and Layer 2 security features</td>
<td>6</td>
</tr>
<tr>
<td>7. Cryptography</td>
<td>Describe methods for implementing data confidentiality and integrity</td>
<td>7</td>
</tr>
<tr>
<td>8. Implementing Virtual Private Networks</td>
<td>Implement secure virtual private networks</td>
<td>7</td>
</tr>
<tr>
<td>9. Putting It All Together</td>
<td>Given the security needs of an enterprise, create and implement a comprehensive</td>
<td>8</td>
</tr>
</tbody>
</table>
security policy