

ITSY 2330 – Part II Syllabus – Spring 2012 Flex II

Intrusion Detection

Online
Section 002
CRN 81568
3 Credits

Instructor: Brian McDaniel Office Hours: By Appointment
Voice Mail: 210-588-1451 E-Mail: bmcdaniel@alamo.edu (1 Day Reply)
Office Phone: 210-486-3310 BBV: <https://vista.alamo.edu/webct/logon/2744850813011>

Course Description

Part I syllabus available at:

<http://www01.alamo.edu/pac/faculty/acardenas/syllabi/ITSY2330.htm>

Prerequisite: (ITSC 1307 “Unix Operating System I” and ITSY 1342 “Information Technology Security”) or (ITSY 1300 “Fundamentals of Information Security” and ITSY 1342 “Information Technology Security”)

Computer information systems security monitoring, intrusion detection, and crisis management. Includes alarm management, signature configuration, sensor configuration, and troubleshooting components. Emphasizes identifying, resolving, and documenting network crises and activating the response team.

This course examines the major network security tools in use today, with the idea that firewalls are most effective when backed by thoughtful security planning, well-designed security policies, and integrated support from anti-virus software, intrusion detection systems, and related tools. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The course will provide numerous realistic projects and cases incorporating cutting-edge technology and current trends, giving students the opportunity to hone and apply the knowledge and skills they will need as working professionals. Students will also learn about relevant National Institute of Standards (NIST) and Technology guidelines that are used by businesses and information technology professionals.

Upon successful completion of this course, the student should be able to: discuss the physical security of file servers and other network components using NIST guidelines and best practices; develop backup procedures to provide for data security; use network operating system features to implement network security; discuss the nature of computer and network threats and vulnerabilities and methods to prevent their effects; use relevant tools to provide for network security; and use encryption techniques to protect network data.

ITSY 2330 – Part II Syllabus – Spring 2012 Flex II

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 accommodation from the Disability Services office. Instructors(s) are required to follow only those accommodations and/or services outlined in the letter of accommodation. For further information, please contact the Disability Services office at 210-486-3020 or visit the office located in the Palomino Center building, Rm. 116. If you have specific needs, please discuss them privately with your instructor.

Course Materials

Required Text: Guide to Firewalls and VPNs, Third Edition; Whitman, Mattord, Green; Course Technology (Cengage Learning); Boston, Massachusetts; Copyright 2012; ISBN-10: 1-111-13539-8; ISBN-13: 978-1-111-13539-3; <http://www.cengage.com/coursetechnology>

Recommended Text: Build Your Own Security Lab: A Field Guide for Network Testing; Gregg; Wiley Publishing, Inc.; Indianapolis, Indiana; Copyright 2008; ISBN-10: 0-470-17986-4; ISBN-13: 978-0-470-17986-4; <http://www.wiley.com>

Academic Code

You are expected to complete quizzes and examinations without assistance. You cannot submit someone else's assignment for grading, including the alteration of computer files from another student or any instructor. Refer to the *Student Code of Conduct* published in the Palo Alto College Student Handbook for specific directions.

Assignments

Chapter review questions and case projects will be assigned from material covered in each chapter. These assignments are due one week after they are assigned, and must be submitted in the prescribed format and manner. Late assignments may be accepted with a valid excuse, at the discretion of the instructor. Refer to the *Assignment Policy* for specific directions.

Quizzes

There are five quizzes scheduled throughout the semester. Quizzes will be taken online, outside the classroom, without instructor supervision, and have a time limit. There will be up to a one week window of opportunity to take a quiz. A missed quiz cannot be made up. Your lowest quiz score of the semester will be dropped.

ITSY 2330 – Part II Syllabus – Spring 2012 Flex II

Exams

There will be two exams plus a cumulative final. Exams will be taken online, outside the classroom, without instructor supervision, and have a time limit. There will be up to a one week window of opportunity to take an exam. A missed exam can only be made up with a valid excuse, and at the discretion of the instructor. No exams are dropped or curved.

Course Grade

Your course grade is composed of the following items, and their weights.

Item	Percentage of Course Grade
Assignments	40%
Quizzes	10%
Exam 1	15%
Exam 2	15%
Final Exam	20%

Grading Scale

Your course letter grade will be determined by calculating the percentage of your total points earned out of the total points possible and using the following grading scale.

Greater Than Or Equal To	But Less Than	Letter Grade
90%	NO LIMIT	A
80%	90%	B
70%	80%	C
60%	70%	D
0%	60%	F

ITSY 2330 – Part II Syllabus – Spring 2012 Flex II

Calendar of Events

Date	Event
March 23	Class Begins
March 26	Census Date
April 6	Exam 1
April 6-8	College Closed – Easter Holiday
April 26	Last Day to Withdrawal
April 27	Exam 2
April 27	College Closed – Fiesta Holiday
May 4	Class Ends
May 11	Final Exam

Topic and Assignment Schedule

Date	Topic	Review Questions	Case Projects
March 23	Introduction to Information Security ⇒ Chapter 1: p. 1-24 Security Policies and Standards ⇒ Chapter 2: p. 33-61	Chapter 1 ⇒ p. 24-25: 1-20 Chapter 2 ⇒ p. 61-62: 1-20	Chapter 1 ⇒ p. 28-30: 1-4 Chapter 2 ⇒ p. 65: 1-2
March 30	Authenticating Users ⇒ Chapter 3: p. 67-86 Introduction to Firewalls ⇒ Chapter 4: p. 97-132	Chapter 3 ⇒ p. 86-87: 1-20 Chapter 4 ⇒ p. 132: 1-20	Chapter 3 ⇒ p. 94-95: 1-2
April 6	Exam 1		Chapter 4 ⇒ p. 135-141: 1-56
April 13	Packet Filtering ⇒ Chapter 5: p. 143-165 Firewall Configuration and Administration ⇒ Chapter 6: p. 179-203	Chapter 5 ⇒ p. 165-166: 1-20 Chapter 6 ⇒ p. 204: 1-20	Chapter 5 ⇒ p. 171-177: 1-75
April 20	Working with Proxy Servers and Application-Level Firewalls ⇒ Chapter 7: p. 209-229 Implementing the Bastion Host ⇒ Chapter 8: p. 237-254	Chapter 7 ⇒ p. 229-230: 1-20 Chapter 8 ⇒ p. 254-255: 1-20	Chapter 6 ⇒ p. 207-208: 1-13
April 27	Exam 2		Chapter 7 ⇒ p. 234-236: 1-39
May 4	Encryption—The Foundation for the Virtual Private Network ⇒ Chapter 9: p. 261-281 Setting Up a Virtual Private Network ⇒ Chapter 10: p. 293-318	Chapter 9 ⇒ p. 281-282: 1-20 Chapter 10 ⇒ p. 318: 1-20	Chapter 9 ⇒ p. 290-291: 1-2
May 11	Final Exam		