Wharton County Junior College

Administrative Master Syllabus

Course Information

Course Title	Intrusion Detection
Course Prefix, Num. and Title	ITSY 2330 - Intrusion Detection
Division	Technology & Business
Department	Computer Science
Course Type	WECM Course
Course Catalog Description	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.
Pre-Requisites	ITSY 2300 & ITSY 2301
Co-Requisites	None

Semester Credit Hours

Total Semester Credit Hours (SCH): Lecture Hours: Lab/Other Hours	3:2:2
Equated Pay Hours	3
Lab/Other Hours Breakdown: Lab Hours	2
Lab/Other Hours Breakdown: Clinical Hours	0
Lab/Other Hours Breakdown: Practicum Hours	0
Other Hours Breakdown	0

Approval Signatures

Title	Signature	Date
Prepared by:	Stephen Lyford Digitally signed by Stephen Lyford Date: 2020.06.08 15:41:58 -05'00'	06/08/2020
Department Head:	Stephen Lyford Digitally signed by Stephen Lyford Date: 2020.06.08 15:42:12 -05'00'	06/08/2020
Division Chair:	David Kucera Digitally signed by David Kucera DN: cn=David Kucera, o=Wharton County Junior College, ou=Division of Technology and Business, email=davidk@wcjc.edu, c=US Date: 2020.06.08 10:36:16 -05'00'	06/08/2020
Dean/VPI:	Paul J. Quinn Digitally signed by Paul J. Quinn Date: 2020.06.10 08:31:00 -05'00'	06/10/2020
Approved by CIR:	Paul J. Quinn Digitally signed by Paul J. Quinn Date: 2020.06.10 08:31:20 -05'00'	06/10/2020

Additional Course Information

Topical Outline: Each offering of this course must include the following topics (be sure to include information regarding lab, practicum, and clinical or other non-lecture instruction).

Topical Outline – Each offering of this course must include the following topics (be sure to include information regarding lab, practicum, clinical or other non-lecture instruction):
- Infrastructure Monitoring
- Intrusion Detection Systems
- Life-cycle of a Vulnerability
- Proactive Intrusion Prevention and Response via Attack Graphs
- Network Flows and Anomaly Detection
- Web Application Firewalls
- Wireless IDS/IPS
- Physical Intrusion Detection for IT
- Geo-spatial Intrusion Detection
- Visual Data Communications

Course Learning Outcomes:

Learning Outcomes: Upon successful completion of this course, students will:	**Methods of Assessment:**
1. Build IDS sensors and attach them to the network (hardware and software); 2. Install and manage a secure communication link between all sensors and the monitor; 3. Install and manage event database(s); analyze an event and trends; 4. Install, manage, and interpret syslog servers and system logs; 5. Identify legal and policy issues associated with system and network monitoring; and deploy, implement, and test IDS security plan.	Individual/Group Assignments Individual/Group Projects Reading Assignments Presentations Lab Works/Assignments Quizzes/Tests/Exams

Required text(s), optional text(s) and/or materials to be supplied by the student:

Practical Intrusion Analysis, 1st Edition, Ryan Trost, Addison-Wesley Professional PTG, 2010, ISBN: 978-0321591807

Suggested Course Maximum:

20

List any specific or physical requirements beyond a typical classroom required to teach the course.

Access to Netlab
• Computer (64 bit CPU) equipped with 12 GB RAM or more (running virtual machines), graphics card capable of supporting virtual machines, 19" or better monitor, and removable hard drive (500 GB or better) for each student and same for instructor.
• Instructor's machine needs 2 network interface cards (one to connect to WCJC network and one to connect to student pcs). And Data projector
• Cat 5 network cable, RJ-45 jacks and crimper for each student and 2 cable tester
• Router and cables to separate class from WCJC network
• Microsoft Windows 7 (or current version) (64 bit) operating system software for each pc (student and instructors)
Linux Operating system*
• Microsoft Office suite for each pc (student and instructors)
• VMWare Workstation 11 (or current version) for each student and instructor
• Antivirus software for each pc

The course maximum is set by current equipment contained in the lab.

Course Requirements/Grading System: Describe any course specific requirements such as research papers or reading assignments and the generalized grading format for the course.

Course Requirements	Grading System
Attendance and Participation 0-10%	100 -90 = A
Chapter Review Questions 0-10%	89 - 80 = B
Labs (Projects) 25-50%	79 - 70 = C
Tests 25-50%	69 - 60 = D
Final Exam / Project 10-25%	59 and below = F

Curriculum Checklist:

☐**Administrative General Education Course** (from ACGM, but not in WCJC Core)
No additional documents needed.

☐**Administrative WCJC Core Course**. Attach the Core Curriculum Review Forms

☐Critical Thinking
☐Communication
☐Empirical & Quantitative Skills
☐Teamwork
☐Social Responsibility
☐Personal Responsibility

☒**WECM Course**
If needed, revise the Program SCANS Matrix and Competencies Checklist