Incident Response COSC 4590  
Computer Science  
Spring 2015

A. COURSE INFORMATION

Course number/section: COSC 4590 -001  
Class meeting time: MW 2:00 PM – 3:15 PM  
Class location: CI 230

B. INSTRUCTOR INFORMATION

Instructor: Steve Alves  
Office location: CI-305  
Office hours: MW 11:00 – 1:00  
Telephone: 825-3492  
e-mail: steve.alves@tamucc.edu  
Appointments: Via email

C. COURSE DESCRIPTION

Catalog Course Description
This course focuses on the standards and technologies used to establish organization structures that will support information technology incident response, business continuity and disaster recovery efforts. This course introduces incident response, business continuity and disaster recovery planning concepts as well as tools and techniques. Topics include the development and implementation of incident response, business continuity and disaster recovery plans, attack traffic analysis, and network based and host based hardware and software. Concepts will be examined and evaluated with appropriate exercises.

D. PREREQUISITES AND COREQUISITES

Prerequisites  
COSC 2365

E. REQUIRED TEXTBOOK(S), READINGS AND SUPPLIES

Required Textbook(s)  
Principles of Incident Response and Disaster Recovery [Paperback]  
F. **STUDENT LEARNING OUTCOMES AND ASSESSMENT**

By the end of this course, students should be able to:

1. Install and configure Windows operating systems and services
2. Design PowerShell and batch scripts to install and configure server services.
3. Design PowerShell and batch scripts to secure Windows operating systems.
4. Design C++ programs to secure Windows systems.
5. Debug programs with ISE and Visual Studios

G. **INSTRUCTIONAL METHODS AND ACTIVITIES**

Instructional methods will consist of lectures, in class exercises and homework assignments.

H. **MAJOR COURSE REQUIREMENTS AND GRADING**

Student learning outcomes will be measured through the use of homework assignments, exams, and quizzes if necessary. Grading scale: A: 100-90, B: 89-80, C: 79-70, D: 69-60, and F: 59-0.

<table>
<thead>
<tr>
<th>ACTIVITY</th>
<th>% of FINAL GRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exams</td>
<td>70</td>
</tr>
<tr>
<td>Quizzes</td>
<td>TBD</td>
</tr>
<tr>
<td>Homework</td>
<td>30</td>
</tr>
<tr>
<td>Presentations</td>
<td></td>
</tr>
<tr>
<td>Lab Reports</td>
<td></td>
</tr>
<tr>
<td>Papers</td>
<td></td>
</tr>
<tr>
<td>Other activities . . .</td>
<td></td>
</tr>
</tbody>
</table>
## I. COURSE CONTENT/SCHEDULE

Tentative Course Schedule (Subject to change)

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/21/15</td>
<td>Training Environment</td>
</tr>
<tr>
<td>01/26/15</td>
<td>Incident Response: Preparation, Organization, and Prevention Bash scripting</td>
</tr>
<tr>
<td>02/02/15</td>
<td>Incident Response: Detection and Decision Making, <strong>HW2</strong> Bash scripting, <strong>HW1</strong> Bash scripting</td>
</tr>
<tr>
<td>02/09/15</td>
<td>Incident Response: Reaction, Recovery, and Maintenance PowerShell ISE</td>
</tr>
<tr>
<td>02/16/15</td>
<td>Network Analysis Tools PowerShell Tools for Visual Studios Python - Scapy</td>
</tr>
<tr>
<td>02/23/15</td>
<td>Network Analysis Tools Netdude, pcapr, netdude, networkMiner, ngrep, hping, <strong>Exam 1</strong></td>
</tr>
<tr>
<td>03/02/15</td>
<td>Network Analysis - SYN scans and OS Fingerprinting, <strong>HW3</strong> PowerShell Tools for Visual Studios</td>
</tr>
<tr>
<td>03/09/15</td>
<td>Network Analysis - Exploitation PowerShell with Visual Studios</td>
</tr>
<tr>
<td>03/16/15</td>
<td>Spring Break</td>
</tr>
<tr>
<td>03/23/15</td>
<td>Network Analysis - ARP Cache Poisoning and Remote Access Trojan, <strong>HW4</strong> PowerShell with Visual Studios</td>
</tr>
<tr>
<td>03/30/15</td>
<td><strong>Exam 2</strong> Wireless Analysis - Access Card Modes and AirPcap PowerShell with Visual Studios</td>
</tr>
<tr>
<td>04/06/15</td>
<td>Wireless Analysis - Packet Structure and , <strong>HW5</strong></td>
</tr>
<tr>
<td>04/13/15</td>
<td>Wireless Analysis - Security</td>
</tr>
<tr>
<td>04/20/15</td>
<td>Log Analysis, <strong>HW6</strong></td>
</tr>
<tr>
<td>Date</td>
<td>Assignment</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>04/27/15</td>
<td>Log Analysis</td>
</tr>
<tr>
<td>05/04/15</td>
<td>Log Analysis</td>
</tr>
<tr>
<td></td>
<td>Final Exam</td>
</tr>
</tbody>
</table>

Note: Changes in this course schedule may be necessary and will be announced to the class by the Instructor. The assignments and exams shown are directly related to the Student Learning Outcomes described in Section F.

J. **COURSE POLICIES**

**Course Syllabus:**
We will meet in lecture on Tuesday and Thursday, when new material will be presented. Non-text material may also be included in the lectures. The assignments, quizzes, and exams will be given during the class hours. You are responsible for all the material presented during the lecture.

**Exams:**
Exams will cover all lecture, assignments, quizzes and reading material. Exams must be taken on the hour they are scheduled. In the event, if you cannot attend the class to take the exam due to some emergency or some unavoidable situation (such as serious illness, death in the family, participation in university sports, religious observations, and so on) you must notify me as soon as possible before the exam and also you must validate your absence by providing me a document (e.g., with a letter from your doctor).

**Homework Assignments and Quizzes:**
Approximately 6 homework assignments will be given. Partial credit will be given for incomplete assignments. In addition, there may be a quiz from time-to-time. They will significantly be based on the material from the lectures and other material considered essential for the successful completion of this course. They will be handed out in the class during the lecture. The submission details will be provided to you along with the assignment. All the homework assignments are due at the beginning of the class on the due date. If the student is absent on the due date, it is the student’s responsibility to see to it that the assignment is submitted on the designated date. An assignment that is turned in after the class on the due date is considered one day late. There is a penalty for late submissions. 10% penalty for 1-2 days late. 25% penalty for 3-4 days late. 75% penalty for 5 days late. 100% penalty (i.e. no credit) if submitted after 5 days. If you have not completed your assignment by the due date, you should submit the work you have done for partial credit. No work will be accepted once the graded work has been returned or the solution has been disclosed to the class, except for unusual circumstances which the instructor feels reasonable. Be sure to backup your work. Note that any kind of hardware or
software failure or machine unavailability in the lab does not merit an extension on the assignment. Diskettes upon which major examinations, assignments, projects or papers submitted may be retained by the instructor as a permanent record of the student’s work.

**Grading Error:**
All questions concerning a test score or grading of a returned test or assignment must be resolved within one week. It is always a good idea to keep all of your work until the end of the semester. In case of any recording errors or doubts, you may produce them for correction or verification.

**Attendance:**
You must attend all classes. In class attendance will affect your grade. You are responsible for any materials covered or handed out or announcements made for the tests, homework assignments in your absence. Records of your attendance will be maintained and reported to the university. Students found missing classes without the instructor’s permission will be automatically withdrawn from the course.

**Absence from class:**
Students are responsible for all materials covered in class and assigned. Should a student be absent from class, it is his/her responsibility to get the notes, etc. for that missed class. More important, should there be assignments, it is the student responsibility to obtain such assignments. No excuse will be accepted for assignments not turned in because the student was absent when it was due.

**Other Policies:**
Cell phones and computers must be turned off during class. Audio and video recording of any kind is not permitted in the classroom. First violation receives a warning. All succeeding violations result in a ten point deduction off the final exam. Any violation during a quiz or exam results in a ten percent deduction off the corresponding paper. No warnings for quizzes or exams.

**COLLEGE AND UNIVERSITY POLICIES**

- **Academic Integrity (University)**
  It is expected that university students will demonstrate a high level of maturity, self-direction, and ability to manage their own affairs. Students are viewed as individuals who possess the qualities of worth, dignity, and the capacity for self-direction in personal behavior.
  See Full University Policy at [http://catalog.tamucc.edu/content.php?catoid=10&navoid=313#Academic_Integrity](http://catalog.tamucc.edu/content.php?catoid=10&navoid=313#Academic_Integrity)

- **Classroom/Professional Behavior**
  Texas A&M University-Corpus Christi, as an academic community, requires that each individual respect the needs of others to study and learn in a peaceful atmosphere. Under Article III of the Student Code of Conduct, classroom behavior that interferes with either (a) the instructor’s ability to conduct the class or (b) the ability of other students to profit from the instructional program may be considered a
breach of the peace and is subject to disciplinary sanction outlined in article VII of
the Student Code of Conduct. Students engaging in unacceptable behavior may be
instructed to leave the classroom. This prohibition applies to all instructional forums,
including classrooms, electronic classrooms, labs, discussion groups, field trips, etc.

- **Statement of Civility (can be in place of classroom/professional behavior)**
  Texas A&M University-Corpus Christi has a diverse student population that
  represents the population of the state. Our goal is to provide you with a high quality
  educational experience that is free from repression. You are responsible for
  following the rules of the University, city, state and federal government. We expect
  that you will behave in a manner that is dignified, respectful and courteous to all
  people, regardless of sex, ethnic/racial origin, religious background, sexual
  orientation or disability. Behaviors that infringe on the rights of another individual
  will not be tolerated.

- **Deadline for Dropping a Course with a Grade of W (University)**
  The grade of W will be assigned to any student officially dropping a course by
  Friday, April 10, 2015. No student is eligible to receive a W without completing the
  official drop process by this deadline. Visit the Office of the University Registrar
  for the Course Drop Form that must submitted. After April 10, 2015 a student will
  not be allowed to drop a course.

- **Grade Appeals (College of Science and Engineering)**
  As stated in University Procedure 13.02.99.C2.01, Student Grade Appeal Procedures, a
  student who believes that he or she has not been held to appropriate academic standards
  as outlined in the class syllabus, equitable evaluation procedures, or appropriate
  grading, may appeal the final grade given in the course. The burden of proof is upon the student to
demonstrate the appropriateness of the appeal. A student with a complaint about a grade
is encouraged to first discuss the matter with the instructor. For complete details,
including the responsibilities of the parties involved in the process and the number of
days allowed for completing the steps in the process, see University Procedure
13.02.99.C2.01, Student Grade Appeal Procedures. These documents are accessible
through the University Rules website at
http://www.tamucc.edu/provost/university_rules/index.html, and the College of Science
and Engineering Grade Appeals webpage at
http://sci.tamucc.edu/students/GradeAppeal.html. For assistance and/or guidance in the
grade appeal process, students may contact the chair or director of the appropriate
department or school, the Office of the College of Science and Engineering Dean, or the
Office of the Provost.

- **Disability Services**
  Disability Services (DS) is the hub for coordinating services and accommodations to
ensure accessibility and utilization of all programs for all Texas A&M University-
Corpus Christi students with disabilities. Our services are designed to meet the
unique educational needs of enrolled students with documented permanent or
temporary disabilities. DS provides intake and consultation services to students
seeking to register with our office. DS reviews an individual’s documentation of
disability and assesses eligibility for services and the determination of reasonable accommodations. For more information visit the Disability Services Office at 116 Corpus Christi Hall or go to http://disabilityservices.tamucc.edu/

- **Statement of Academic Continuity**
  In the event of an unforeseen adverse event, such as a major hurricane and classes could not be held on the campus of Texas A&M University–Corpus Christi; this course would continue through the use of Blackboard and/or email. In addition, the syllabus and class activities may be modified to allow continuation of the course. Ideally, University facilities (i.e., emails, web sites, and Blackboard) will be operational within two days of the closing of the physical campus. However, students need to make certain that the course instructor has a primary and a secondary means of contacting each student.

**Academic Advising:** The College of Science and Technology requires that students meet with an Academic Advisor as soon as they are ready to declare a major. The Academic Advisor will set up a degree plan, which must be signed by the student, a faculty mentor, and the department chair.

**GENERAL DISCLAIMER**
I reserve the right to modify the information, schedule, assignments, deadlines, and course policies in this syllabus if and when necessary. I will announce such changes in a timely manner during regularly scheduled lecture periods.