Cyber Defense I COSC 3365  
Computer Science  
Spring 2016

A. COURSE INFORMATION

Course number/section: COSC 3365 -001  
Class meeting time: TTH 12:30 PM – 1:45 PM  
Class location: CI 230

B. INSTRUCTOR INFORMATION

Instructor: Steve Alves  
Office location: CI-305  
Office hours: MW 11:00 – 1:00  
Friday 11:00 – 12:00  
Telephone: 825-3492  
E-mail: steve.alves@tamucc.edu  
Appointments: Via email

C. COURSE DESCRIPTION

Catalog Course Description
This course proposes to introduce the student in the identification of vulnerabilities, forms of attack, appropriate countermeasures, and the detection and defense of the same. Tools and techniques for the securing of hardware, software and data, including physical security are covered. The issues and facilities available to both the intruder and administrator will be examined and evaluated with appropriate exercises to illustrate their effect.

D. PREREQUISITES AND COREQUISITES

Prerequisites  
COSC 2365

E. REQUIRED TEXTBOOK(S), READINGS AND SUPPLIES

Required Textbook(s)  
All In One CompTIA Security+  
ISBN: 978-0-07-177147-4
F. **STUDENT LEARNING OUTCOMES AND ASSESSMENT**

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

1. Capture and analyze network traffic and perform log analysis
2. Differentiate and analyze different types of malware
3. Work with cryptographic systems
4. Design ruby, python and bash shell scripts to test Linux operating systems security.
5. Design ruby, python and bash shell scripts to secure Linux operating systems.
6. Debug code with debuggers.

**Course Objective**

Describe gaining confidential information or unauthorized access through human intelligence (i.e. social engineering)

Discuss countermeasures to social engineering (training and education of users, administrators and personnel)

Describe vishing

Define organizational policies and procedures

Describe security policies (guidance provided by security policies, points of contact, roles and responsibilities, enterprise, issue specific, and system specific security policies)

Describe AIS and telecommunications systems policies (points of contact, references)

Explain change management

Explain classification of information

Describe documentation, logs, and journals

Explain acceptable use of resources, internet usage policy, and e-mail usage policy

Discuss due care, due diligence, and due process

Describe separation of duties, need to know and least privilege

Discuss transportation of media

Disposal and destruction of discarded papers/media/objects

Describe object reuse protocols

Explain privacy policy, human resources policies, code of ethics

Discuss cybercrime and cybercrime laws,

Describe ethics (SANS Institute IT Code of Ethics)

Discuss fraud, waste, and abuse

Define user, group, and role management, personnel and administrative controls/permissions

Discuss password policies

Describe centralized vs. decentralized management

Discuss auditing - privilege, usage and escalation, logging and auditing of log files, monitoring data, activity, events

Explain handling access control - mandatory access control, discretionary access control, role-based access control, rule-based access control

Describe permissions and rights in Windows OS
Explain concept of groups and roles (grouping of personnel and assigning permissions based on roles)
Discuss walls and guards
Describe security safeguards
Explain controls
Explain monitoring of critical areas, communications centers, information systems centers (IT/data centers), protected distributed systems, stand-alone systems, peripherals, storage areas
Describe Policies and Procedures for computers and users
Review of physical security safeguards and resulting impact on risk mitigation
Explain access controls and monitoring, access to doors and entry points, layered access, physical security perimeters and secure areas, tailgating and mantraps, CCTV systems, access/door alarms and fire alarms
Describe environmental controls, temperature and humidity, electromagnetic interference, cabling to prevent EMI, building construction (Faraday cage/shield) to prevent EMI, fire suppression
Explain and describe authentication, access tokens, biometrics, multiple-factor authentication
Explain different types of disasters - fire, natural disasters, chemical spills, gas leak, political unrest, terrorism, war
Describe disaster recovery plans/process (functions/processes, roles and responsibilities in an emergency situation), continuity of operations and contingency plan components
Define categories of Functions, critical, necessary for normal processing, desirable, and optional
Describe backups, what needs to be backed up, strategies, types of backups, backup frequency and retention, storage of backups, backout planning
Explain utilities, determining need for power, uninterruptible power supplies, backup emergency generators, preserving/restoring communications, continuing operations from a different location
Explain Secure Recovery Services
Explain High Availability and Fault Tolerance, redundant and mirrored systems, load balancing, clustering
Explain Failure and Recovery Timing, mean time to failure, mean time to restore, recovery time objective, recover point objective
Describe Recovery Plan Development and emergency destruction procedures
Describe risk management (qualitative and quantitative), assets, threats, vulnerabilities impact and controls/countermeasures
Identify exposure factor
Explain annualized rate of occurrence and annualized loss expectancy
Discuss the general Risk Management Model and its components, asset identification, threat/vulnerability assessment, impact definition and quantification, control/countermeasure design and evaluation
Explain software engineering, identify risks, analyze data and evaluate, classify, and prioritize risks
Discuss software engineering plan and implement mitigating actions
Describe monitor risks, mitigation plans, and corrections
Explain qualitative vs. quantitative risk assessment
Discuss risk management tools
Describe the incident response cycle - discover and report, confirm, investigate, recover, lessons learned, attribution, calling tree
Identify and explain countermeasures
Describe cover and deception (security through obscurity, administrative rename) (Chapter 1)
Describe monitoring (data and line)
Discuss evidence (standards for, types of)
Describe collecting and preserving evidence (acquiring, identifying, protecting, transporting, and sorting evidence)
Explain conducting the investigation
Explain chain of custody
Explain public key infrastructure
Distinguish between certificate authorities, registration authorities, certificate repositories
Describe trust and certificate verification
Explain digital certificates (proof of integrity/non-repudiation)
Distinguish between centralized and decentralized infrastructure
Describe hardware and storage devices
Explain private key protection
Distinguish between in-house certificate authorities, and outsourced certificate authorities
Describe trust models
Describe infrastructure devices - workstations, servers, network interface cards, hubs, bridges, switches, routers, firewalls, wireless, modems, telecom/PBX, RAS, VPN, Intrusion Detection Systems, network access control, network monitoring/diagnostic, virtualization, mobile devices
Describe infrastructure media - coaxial cable, UTP/STP (shielded vs. unshielded twisted pair), fiber, unguided media, security concerns for transmission media (physical security)
Explain removable media, magnetic media, optical media, electronic media and labeling, sanitization, transmission of media
Explain the Cloud (Saas, Paas, Iaas)
Describe security topologies components, security zones, telephony, VLANs, NAT, and tunneling
Describe EMI pickup in data cable
Describe tempest, tempest shielding protection, testing and certification
Describe tempest separation
Describe control zones and white noise, attenuation, banding, cabling, grounding, and filtered power
Explain attack surface analysis
Describe threat modeling, fuzz testing, code reviews, and bug tracking
Explain software countermeasures in security testing phase
Expanded testing methodology, white-box testing, black-box testing, grey-box testing, penetration tests
Explain broadband, baseband and line of sight
Describe microwave communication
Explain radio frequency communication
Describe satellite communication
Describe network topology
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>60</td>
</tr>
<tr>
<td>Quizzes</td>
<td>10</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>01/21/16</td>
<td>Introduction to security environment</td>
</tr>
</tbody>
</table>
| 01/26/16 | Chapter 3 Legal Issues, Privacy, and Ethics, **HW1**  
Discuss cybercrime and cybercrime laws,  
Describe ethics (SANS Institute IT Code of Ethics)  
Discuss fraud, waste, and abuse                  |
| 02/02/16 | Chapter 19 Privilege Management  
Define user, group, and role management, personnel and administrative controls/permissions  
Discuss password policies  
Describe centralized vs. decentralized management  
Discuss auditing - privilege, usage and escalation, logging and auditing of log files, monitoring data, activity, events  
Explain handling access control - mandatory access control, discretionary access control, role-based access control, rule-based access control  
Describe permissions and rights in Windows OS  
Explain concept of groups and roles (grouping of personnel and assigning permissions based on roles) |
| 02/09/16 | Chapter 2 Operational Organizational Security, **HW2**  
IA Fundamentals – Security Life Cycle:  
Describe gaining confidential information or unauthorized access through human intelligence (i.e. social engineering)  
Discuss countermeasures to social engineering (training and education of users, administrators and personnel)  
Describe vishing  
Define organizational policies and procedures  
Describe security policies (guidance provided by security policies, points of contact, roles and responsibilities, enterprise, issue specific, and system specific security policies)  
Describe AIS and telecommunications systems policies (points of contact, references)  
Explain change management  
Explain classification of information  
Describe documentation, logs, and journals  
Explain acceptable use of resources, internet usage policy, and e-mail usage policy  
Discuss due care, due diligence, and due process  
Describe separation of duties, need to know and least privilege  
Discuss transportation of media |
<table>
<thead>
<tr>
<th>Date</th>
<th>Chapter</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/16/16</td>
<td>Chapter 7 Physical Security</td>
<td>Discuss walls and guards, Describe security safeguards, Explain controls, Explain monitoring of critical areas, communications centers, information systems centers (IT/data centers), protected distributed systems, stand-alone systems, peripherals, storage areas, Describe Policies and Procedures for computers and users, Review of physical security safeguards and resulting impact on risk mitigation, Explain access controls and monitoring, access to doors and entry points, layered access, physical security perimeters and secure areas, tailgating and mantraps, CCTV systems, access/door alarms and fire alarms, Describe environmental controls, temperature and humidity, electromagnetic interference, cabling to prevent EMI, building construction (Faraday cage/shield) to prevent EMI, fire suppression, Explain and describe authentication, access tokens, biometrics, multiple-factor authentication, HW3</td>
</tr>
<tr>
<td>02/23/16</td>
<td>Exam 1</td>
<td>Chapter 13 Types of Attacks and Malicious Software, Explain attack surface analysis, Describe threat modeling, fuzz testing, code reviews, and bug tracking, Explain software countermeasures in security testing phase, Expanded testing methodology, white-box testing, black-box testing, grey-box testing, penetration tests, Secure Software Development Lifecycle</td>
</tr>
<tr>
<td>03/01/16</td>
<td>Chapter 8 Infrastructure Security, HW4</td>
<td>Describe infrastructure devices - workstations, servers, network interface cards, hubs, bridges, switches, routers, firewalls, wireless, modems, telecom/PBX, RAS, VPN, Intrusion Detection Systems, network access control, network monitoring/diagnostic, virtualization, mobile devices, Describe infrastructure media - coaxial cable, UTP/STP (shielded vs. unshielded twisted pair), fiber, unguided media, security concerns for transmission media (physical security), Explain removable media, magnetic media, optical media, electronic media and labeling, sanitization, transmission of media, Explain the Cloud (Saas, Paas, Iaas), Describe security topologies components, security zones, telephony, VLANs, NAT, and tunneling, Describe EMI pickup in data cable, Reference Text Chapter 6 Securing the Network and Environment, -- Describe tempest, tempest shielding protection, testing and certification</td>
</tr>
</tbody>
</table>
-- Describe tempest separation
-- Describe control zones and white noise, attenuation, banding, cabling, grounding, and filtered power
Reference Text Chapter 3 Infrastructure and Connectivity
-- Explain broadband, baseband and line of sight
-- Describe microwave communication
-- Explain radio frequency communication
-- Describe satellite communication
-- Describe network topology

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/08/16</td>
<td>Chapter 9 Authentication and Remote Access</td>
</tr>
<tr>
<td>03/15/16</td>
<td>Spring Break</td>
</tr>
<tr>
<td>03/22/16</td>
<td>Chapter 4 Cryptography, <strong>HW5</strong></td>
</tr>
<tr>
<td>03/29/16</td>
<td>Chapter 4 Cryptography</td>
</tr>
<tr>
<td>04/05/16</td>
<td><strong>Exam 2</strong></td>
</tr>
<tr>
<td></td>
<td>Chapter 5 Public Key Infrastructure, <strong>HW6</strong></td>
</tr>
<tr>
<td>04/12/16</td>
<td>Chapter 5 Public Key Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Explain public key infrastructure</td>
</tr>
<tr>
<td></td>
<td>Distinguish between certificate authorities, registration authorities, certificate repositories</td>
</tr>
<tr>
<td></td>
<td>Describe trust and certificate verification</td>
</tr>
<tr>
<td></td>
<td>Explain digital certificates (proof of integrity/non-repudiation)</td>
</tr>
<tr>
<td></td>
<td>Distinguish between centralized and decentralized infrastructure</td>
</tr>
<tr>
<td></td>
<td>Describe hardware and storage devices</td>
</tr>
<tr>
<td></td>
<td>Explain private key protection</td>
</tr>
<tr>
<td></td>
<td>Distinguish between in-house certificate authorities, and outsourced certificate authorities</td>
</tr>
<tr>
<td></td>
<td>Describe trust models</td>
</tr>
<tr>
<td>04/19/16</td>
<td>Standards and Protocols, <strong>HW7</strong></td>
</tr>
<tr>
<td>04/26/16</td>
<td>Standards and Protocols</td>
</tr>
<tr>
<td>05/03/16</td>
<td>Final Exam Review</td>
</tr>
</tbody>
</table>

**Final Exam** see TAMUCC Sail web page

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

  • 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. Please consult with the instructor before you decide to drop to be sure it is the best thing to do. Just stopping attendance and participation **WILL NOT** automatically result in your being dropped from the class. Should dropping the course be the best course of action, visit the Office of the University Registrar for the Course Drop Form that must submitted. No student is eligible to receive a W without completing the official drop process by this deadline. Please consult the Academic Calendar ([http://www.tamucc.edu/academics/calendar/](http://www.tamucc.edu/academics/calendar/)) for the last day 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](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](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**
  The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring an accommodation, please call (361) 825-5816 or visit Disability Services in Corpus Christi Hall 116.

  If you are a returning veteran and are experiencing cognitive and/or physical access issues in the classroom or on campus, please contact the Disability Services office for assistance at (361) 825-5816.

  [http://disabilityservices.tamucc.edu/](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 & Engineering 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. Meetings are by appointment only; advisors do not take walk-ins. Please call or stop by the Advising Center to check availability and schedule an appointment. The College’s Academic Advising Center is located in Center for Instruction 350 or can be reached at (361) 825-3928.

**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.