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.

Pre-requisite:
COSC 1435

Student Learning Outcomes:
Upon completion of this course, students will be able to:
- Understand the potential computer violations that may occur and the attackers.
- Understand the methods used in doing reconnaissance against a computer system or network.
- Understand how to prepare and defend against cyber crimes and information theft.
- Understand the appropriate measures to be taken should a cyber crime occur.
- Understand the effects of poor security in an organization.

Course Text:
Certified Ethical Hacker

Reference Text:

Course Requirements:
This is an introductory course. However, this is a difficult course that demands all students attend all classes! Regular completion of all reading, homework, and other outside assignments, are absolutely essential for success in this course.
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
Grading Policy:
Your course grade will be decided on your performance in the homework assignments, quizzes, two mid-term exams, and the final exam. The distribution of points is as follows:

1. Homework assignments and quizzes worth 50%.
2. Two mid-term exams worth 30% (exam 1 worth 15% & exam 2 worth 15%).
3. Final exam worth 20%.

Grading scale: A: 100-90, B: 89-80, C: 79-70, D: 69-60, and F: 59-0.

Homework Assignments and Quizzes: Approximately 8-10 homework assignments will be given. No late homework assignments will be accepted. Partial credit will be given for incomplete assignments. In addition, there may be a quiz from time-to-time.

Course Organization and 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: 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. 25% penalty for 1-2 days late, 50% 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.

**Academic Honesty Policy:** You are expected to avoid all forms of academic dishonesty as defined in Catalog. In addition, students are expected to behave in an ethical manner in all class and lab activities. If you feel uncertain about a particular activity, please speak to me BEFORE problems arise. Ethical behavior is a requirement for passing this course. All work submitted for grading must be the student’s own work. Plagiarism will result in a score of 0 (zero) for the work or dismissal from the course and the Dean of Students office will be notified. No copying from another student’s work, of any class, is allowed. It is the student’s duty to allow no one to copy his or her work. Anyone found cheating and/or copying, in the exams or assignments, in the instructor’s opinion, will receive an automatic F for the course.

**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, pagers and laptop computers must be turned off during class. 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. No recording or video taping of the class is allowed.

**Student Security Statement:** Please read the [Student Security Statement](#).

**Students with Disabilities:** Texas A&M University-Corpus Christi complies with the Americans with Disabilities Act in making reasonable accommodations for qualified students with disabilities. If you suspect that you may have a disability (physical impairment, learning disability, psychiatric disability, etc.), please contact the Services for Students with Disabilities Office, located in Driftwood 101, at 825-5816. If you need disability accommodations in this class, please see me as soon as possible.
**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. The College’s Academic Advising Center is located in Faculty Center 178, and can be reached at 825-6094.

**Grade Appeal Process:** As stated in University Rule 13.02.99.C2, Student Grade Appeals, 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 Rule 13.02.99.C2, Student Grade Appeals, and University Procedure 13.02.99.C2.01, Student Grade Appeal Procedures. These documents are accessible through the University Rules Web site at [http://www.tamucc.edu/provost/university_rules/index.html](http://www.tamucc.edu/provost/university_rules/index.html). For assistance and/or guidance in the grade appeal process, students may contact the Office of Student Affairs.

**Tentative Course Schedule (Subject to change)**

08/23/12:  Introduction

08/28/12:  Chapter 1: Introduction to Ethical Hacking, Ethics, and Legality
08/30/12:

09/04/12:  Chapter 2: Gathering Target Information, Reconnaissance, Footprinting and Social Engineering, **HW1**

09/11/12:  Chapter 3: Gathering Network and Host Information: Scanning and Enumeration
09/13/12:

09/18/12:  Chapter 4: Privilege Escalation, **HW2**
09/20/12:

09/25/12:  Exam 1 Review
09/27/12:  **Exam 1**

10/02/12:  Chapter 5: Trojans, Backdoors, Viruses, and Worms, **HW3**
10/04/12:

10/09/12:  Chapter 6: Gathering Data from Networks, Sniffers, **HW4**
10/11/12:

10/16/12:  Chapter 7: Denial of Service and Session Hijacking, **HW5**
10/18/12:

10/23/12: No class, Spring Break
10/25/12: No class, Spring Break

10/30/12: Chapter 8: Web Application Vulnerabilities, HW6
11/01/12:

11/06/12: Exam 2 Review
11/08/12: Exam 2

11/13/12: Chapter 9: SQL Injection, HW7
11/15/12:

11/20/12: Chapter 10: Wireless Network Systems, HW8
11/22/12:

11/27/12: Chapter 11: Physical Site Security
11/29/12:

12/04/12: Chapter 12: Linux Systems

**Final Exam** on Tuesday, December 11, 2012 at 11:00 AM – 1:30 PM.

**Note:** This syllabus represents a general plan for the course. Deviations from this syllabus may be necessary during the semester and changes will be announced in class.