Computer and Information Security (TC2027)

Tecnológico de Monterrey

Unit 0 - Course Introduction and Logistics

Goals

A. Describe the goals for this course

B. Identify the main logistical aspects involved

C. Recognize the expected behavior

D. Identify the grading structure and its associated activities

Goals for this Course

- ✓Intermediate level course in the area of computing in which the student is introduced to the aspects and techniques necessary to guarantee the security of an organization's computer assets.
- ✓Requires prior knowledge of **operating systems** and **basic networking concepts**.

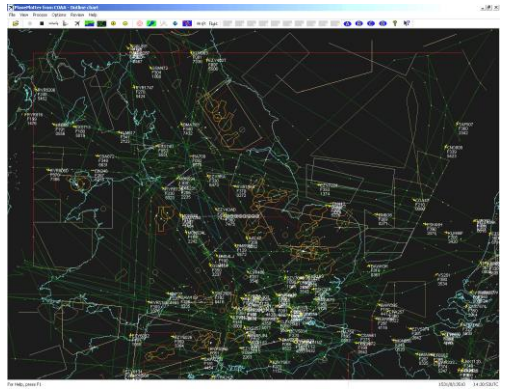
At the end of the course the student will be able to:

- ✓Have knowledge of the **general vision of the area of computer security** with the necessary fundamentals to understand the risks, threats, vulnerabilities to which computer systems are currently subjected, as well as the controls and protection methods against possible attacks, which they are necessary for the proper functioning of these systems in the modern business.
- ✓Know the current state of the laws that concern the security of computer systems at the national and international level.

Who am I?

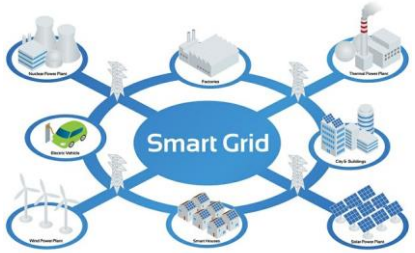
Brazilian Defense Cyber Ops

Brazilian Air Force Pilot



ATC & C2 Security Protocols Research

ATC Services



Utilities Security Architecture

Who am I?


UNIP
UNIVERSIDADE PAULISTA


UEA
UNIVERSIDADE
DO ESTADO DO
AMAZONAS


GEORGE
MASON
UNIVERSITY


UNIVERSIDADE
Nilton Lins


ULBRA
UNIVERSIDADE LUTERANA DO BRASIL


ITA

Class Details

- **Sessions:** Tuesday & Friday (12:00 - 14:00)
- **Office Hours (Mentoring):** will be provided primarily via email, or if necessary, a time can be scheduled via zoom.
- **Email:** barretoabb@tec.mx
- **Message (Remind):** https://www.remind.com/join/tc2027c.

Syllabus and another course information:

- https://experiencia21.tec.mx/courses/127251

Expected Behavior

- Attendance is essential in all sessions.
  - Not all information is provided in the course text or notes
- Good social practices to be observed
  - Enter or leave class at any time, but don't disrupt the activity going on
  - Electronic devices in silent mode
  - Should you find yourself in extreme need to answer an incoming call, just leave the room to do so.
- Assignments
  - Collaboration with peers is strongly encouraged, write-up must be your own
  - Students are responsible for keeping pace of the schedule changes
- Academic and General policies are listed in the Syllabus

Academic Integrity

- Honor code is your bible: https://mitec.itesm.mx/Paginas/mitec/index.aspx.
- Three fundamental principles to follow at all times are:
  - All work submitted be your own;
  - When using the work or ideas of others, including fellow students, give full credit through accurate citations; and
  - If you are uncertain about the ground rules on a particular assignment, ask for clarification.
- Avoid plagiarism
  - Provide an accurate and complete citation for any reference work used.
  - Paraphrased material must also be cited.
  - A simple listing of books or articles is not sufficient.
- Plagiarism is the equivalent of intellectual robbery and cannot be tolerated in the academic setting.

Course Outline

- Direct access to live and recorded sessions:
  - My classes

https://experiencia21.tec.mx/courses/127251/modules

- Activities prior to the first day of class
  - Introduction to the course
    - Welcome
    - Home page
    - Initial activities of the digital modality

Evaluation

- *The required activities do not have a numerical value. However, they may be penalized if they are ignored.*
- *To receive the activity's total points (10%), the student cannot miss any class and must perform all classroom activities, maintaining his own website on git. He will publish the codes developed in the classroom.*

Activities and evaluation	
First partial	**%**
Class Participation*	10%
Home Assignment 01 - Network Analysis	4%
Home Assignment 02 - Cryptography and Cryptanalysis	4%
Home Assignment 03 - Symmetrical and Asymmetrical Cryptography	4%
Home Assignment 04 - Public Key Encryption and Certificates	4%
Second partial	**%**
Home Assignment 05 - Firewall and Proxy	4%
Home Assignment 06 - Intrusion, Detection and Preventing System (IDPS)	5%
Home Assignment 07 - Information Gathering, Scanning, Enumeration, and Vulnerability Identification	5%
Home Assignment 08 - Buffer Overflow	5%
Home Assignment 09 - Session Hijacking	5%
Midterm Exam	10%
Final	**%**
Home Assignment 10 - C2 and Exfiltration	5%
Home Assignment 11 - Botnet	5%
Exam – Cyber Security Challenge	30%
Total	**100**

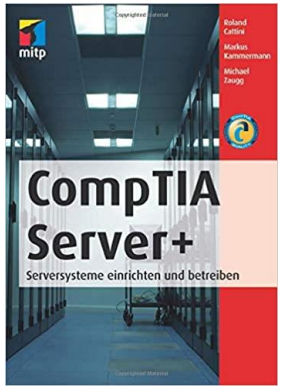
Exams and Assignments

- There will be two major exams in the course
  - Midterm: take-home (individually)
  - Final exam: take-home (group)
- Quizzes will be in-class, applied in an ad-hoc basis
- Homework will be take-home (individually), usually on a bi-weekly basis

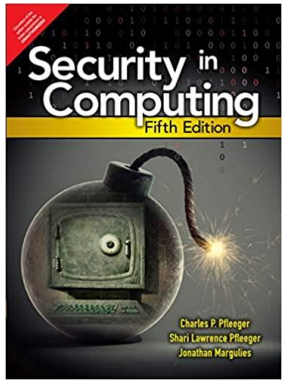
Exams and Assignments

- General Directions:
  - Unless stated otherwise, I will present the solutions at the beginning of the next class after the assignment was handed
    - Handling your assignment after it is due but before I present the solutions you can earn a max of 70 points
    - An assignment handled after the solutions are posted will yield 0 points
  - Files should be named with the following convention:
    - **TC2027**_AssigmentTypeAndWeek_LastnameFirstname.pdf
    - **TC2027**_Hwk2_DoeJohn.pdf,
    - Not-so-good student (real) examples: hm.pdf, Joe.pdf, syst687.pdf, 1.pdf, etc.
    - If the activity is workgroup, it is required to have a main page with the name of team's participants.

Course Reference



Ciampa, M. (2014). CompTIA security+ SYO-401 in depth. Nelson Education.



Pfleeger, C. P. (2002). Pfleeger, S L. Security in Computing.

- Other references distributed in class
- Lecture notes

Computer and Information Security (TC2027)

Tecnológico de Monterrey