DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES
UNIVERSITY OF TORONTO MISSISSAUGA

CSC427H5S LEC0101
Computer Security
Course Outline - Winter 2018

Class Location & Time	Tue, 11:00 AM - 01:00 PM DH 3000
Instructor	Arnold Rosenbloom
Office Location	
Office Hours	
E-mail Address	arnold@cs.toronto.edu
Course Web Site	http://www.cs.toronto.edu/~arnold/427/18s/
Teaching Assistant	TBA

Course Description

Network attacks and defenses, operating system vulnerabilities, application security (e-mail, Web, databases), viruses, spyware, social engineering attacks, privacy and digital rights management. The course will cover both attack techniques and defense mechanisms. [24L, 12T]

Prerequisite: CSC290H5, 347H5, 369H5 (SCI)
Distribution Requirement: SCI

Students who lack a pre/co-requisite can be removed at any time unless they have received an explicit waiver from the department. The waiver form can be downloaded from here.

Assessment and Deadlines

Type	Description	Due Date	Weight
Class Participation	Attending lectures, evaluating presentations, attending tutorials, presenting news	On-going	10%
Term Test	Test	2018-03-06	15%
Final Exam	Final Exam	TBA	15%
Lab	Tutorial Challenges	On-going	10%
Presentations	Short presentation	On-going	15%
Presentations	Long Presentation	On-going	20%
Other	Practical Creation	On-going	15%
		Total	100%

More Details for Assessment and Deadlines

Each week, students will present a variety of topics in teams of two, as outlined below. Each student will contribute to a short presentation, a long presentation and a practical. Topics will finally be chosen by the instructor with suggestions from teams.

News: Typically a 15 minute presentation, this is a summary of the Sans Internet Storm Center podcasts, for example. These typically take 15 minutes and include brief background and pointers. The goal is to explain a few of the current news items for the week.

Tool of the week: Typically a 30-40 minute presentation, chosen from the top 125 tools, typically taken from Kali Linux. This includes a scenario setup as well as demonstration of use. The presenter should speak about typical use cases, demonstrate the tools use from the point of view of an attacker and defender, explaining options, files, configuration etc.. A mini tutorial is left on the course website as well as updates to course virtual machines left for students to explore tools further. Sample exercises/questions are left for further exploration.

OWASP top 10/Mobile top 10: Typically a 30-40 minute presentation, chosen from the OWASP top 10, 2017 list. A vulnerable scenario is presented with an explanation. One or more exploits are demonstrated. Best practices to mitigate are discussed and demonstrated via a repaired application. All of this is placed into course repo as well as all documentation and tutorial and exercises/questions (with a VM) contributed to the class.

In-Depth: Typically a 60 minute presentation on a current topic of significant interest to Information Security. While these may not involve technical issues specifically, a significant investigation of the issue should be presented. If the In-Depth report involves a technical issue, then requirements will be similar to the OWASP top 10 or Tool of the week components. In any case, the report is contributed to the course website as well as sample questions and exercises.

Presenters will be marked on how well they understand the material as well as how well they convey it and on their contribution to the course, questions, updates to VMs, report contributed to the course website. Presenters are expected to contribute to the courses dictionaries, so that by the end of the course, all students communicate effectively as information security professionals.

Each of the In-Depth, Top-10 and Tools talks are accompanied by a practical the following week. The group is to prepare and run a one hour practical session in which the class gets hands on exposure to their topic. The group is responsible for preparing the practical website, the system/VM setup, the exercises, and for running the class through the exercises.

The test/exam will require students to answer brief questions based on topics covered in class and in tutorial.

Some tutorials will be based on challenges, pitting you against your classmates for some marks. Some tutorials may involve capture the flag type challenges as well as investigations into vulnerable machines such as WebGoat.

Penalties for Lateness

10% per day of lateness. Max two days late.

Procedures and Rules

Missed Term Work

To request special consideration, bring supporting documentation to the instructor in person during office hours at least one week in advance.

In case of illness, bring a U of T medical certificate to the instructor within one week of the missed work. The certificate must specify the exact period during which you were unable to carry out your academic work.

Missed Final Exam

Students who cannot write a final examination due to illness or other serious causes must file anonline petition **within 72 hours of the missed examination**. Original supporting documentation must also be submitted to the Office of the Registrar **within 72 hours of the missed exam**. Late petitions will **NOT** be considered. If illness is cited as the reason for a deferred exam request, a U of T Verification of Student Illness or Injury Form must show that you were **examined and diagnosed at the time of illness and on the date of the exam, or by the day after at the latest**. Students must also record their absence on ACORN on the day of the missed exam or by the day after at the latest. Upon approval of a deferred exam request, a non-refundable fee of $70 is required for each examination approved.

Academic Integrity

Honesty and fairness are fundamental to the University of Toronto's mission. Plagiarism is a form of academic fraud and is treated very seriously. The work that you submit must be your own and cannot contain anyone elses work or ideas without proper attribution. You are expected to read the handout How not to plagiarize (http://www.writing.utoronto.ca/advice/using-sources/how-not-to-plagiarize) and to be familiar with the Code of behaviour on academic matters, which is linked from the UTM calendar under the link Codes and policies.

Final Exam Information

Duration:	3 hours
Aids Permitted:	None

Additional Information

Use of git to contribute to the course website will be required. Please do not alter the structure of the website, or contribute in unexpected ways, and outside of your alotted time, without the instructors permission.

Last Date to drop course from Academic Record and GPA is March 14, 2018.