DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES
UNIVERSITY OF TORONTO MISSISSAUGA

CSC427H5S LEC9101
Computer Security
Course Outline - Winter 2022

Class Location & Time	Mon, 03:00 PM - 05:00 PM IB 260
Instructor	Andi Bergen
Office Location	DH-3084
Office Hours	Tue: 11am - 12 (noon) and 1pm - 3pm; Thursday 2pm - 3pm; other days by request; DH-3084 (or Zoom)
E-mail Address	andi.bergen@utoronto.ca
Course Web Site	https://q.utoronto.ca

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.

Prerequisite: CSC347H5 and CSC369H5 (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/participating tutorials/labs	On-going	10%
Presentations	Presentation	On-going	25%
Other	Practical Creation	On-going	25%
Other	Training	On-going	10%
Assignment	A1	2022-02-04	6%
Assignment	A2	2022-02-18	6%
Assignment	A3	2022-03-11	6%
Assignment	A4	2022-03-25	6%
Assignment	A5	2022-04-08	6%
		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 one hour long presentation or two half hour long presentation (Tool of the week, OWASP top 10, In-Depth). Additionally, each student will contribute to a one hour practical, usually related to their presentation. Topics will finally be chosen by the instructor and TA with suggestions from teams.

Tool of the week: Chosen from, for example, 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 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.

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

Additionally, as part of their presentations and practicals, students will provide questions for ongoing weekly assignments, giving their classmates practice with topics presented in class.

Training: Some tutorials/lectures will be based on challenges, pitting you against your classmates for some marks. This may involve capture
the flag type challenges as well as investigations into vulnerable machines such as WebGoat. Students are also expected to contribute to the creation of the events.

Penalties for Lateness

Due to timing issues, presentations and practicals can not be late. Training events may require synchronous participation.

Ten (10) grace tokens will be available to you to use with your assignment submission. Each grace token provides you an additional 6 hours, you can choose to use all grace tokens on a single assignment or spread them out across multiple assignments.

Procedures and Rules

Missed Term Work

In order to receive special consideration, you must email the course coordinator and declare your absence on ACORN. For more information, visit the Office of the Registrar website (https://www.utm.utoronto.ca/registrar/utm-absence).

To request special consideration, email supporting documentation to the course coordinator (andi.bergen@utoronto.ca) at least one week in advance. In order to receive special consideration, you must email supporting documentation to the course coordinator (andi.bergen@utoronto.ca) and you must declare your absence on Acorn.

If you are unable to complete an assessment due to major illness or other circumstances completely outside of your control, please contact the course coordinator (andi.bergen@utoronto.ca) immediately. It is always easier to make alternate arrangements before a due date, so please inform us as soon as you know that you will need accommodation.

Exact accommodations will be determined **on a case-by-case basis and will not be given automatically**. In other words, you risk getting a mark of zero (i.e., a grade of 0) for missed work unless you contact your instructor promptly.

Academic Integrity

Academic integrity is essential to the pursuit of learning and scholarship in a university, and to ensuring that a degree from the University of Toronto Mississauga is a strong signal of each student's individual academic achievement. As a result, UTM treats cases of cheating and plagiarism very seriously. The University of Toronto's Code of Behaviour on Academic Matters outlines behaviours that constitute academic dishonesty and the process for addressing academic offences. Potential offences include, but are not limited to:

In papers and assignments:

1. Using someone else's ideas or words without appropriate acknowledgement.
2. Submitting your own work in more than one course, or more than once in the same course, without the permission of the instructor.
3. Making up sources or facts.
4. Obtaining or providing unauthorized assistance on any assignment.

On tests and exams:

1. Using or possessing unauthorized aids.
2. Looking at someone else's answers during an exam or test.
3. Misrepresenting your identity.

In academic work:

1. Falsifying institutional documents or grades.
2. Falsifying or altering any documentation required, including (but not limited to) doctor's notes.

Keep in mind that the department uses software that compares programs for evidence of similar code. Below are some tips to help you avoid committing an academic offence, like plagiarism.

- Never look at another student's lab/assignment solution(s). Never show another student your lab/assignment solution. This applies to all drafts of a solution and to incomplete and even incorrect solutions.
- Keep discussions with other students focused on concepts and examples. Never discuss labs/assignments before the due date with anyone but your Instructors and your TAs.
  Do not discuss your solution publicly on the discussion board or publicly in the lab rooms/office hours.

All suspected cases of academic dishonesty will be investigated following procedures outlined in the Code of Behaviour on Academic Matters. If you have questions or concerns about what constitutes appropriate academic behaviour or appropriate research and citation methods, you are expected to seek out additional information on academic integrity from your instructor or from other institutional resources.

Plagiarism Detection

Normally, students will be required to submit their course essays to the University's plagiarism detection tool for a review of textual similarity and detection of possible plagiarism. In doing so, students will allow their essays to be included as source documents in the tool's reference database, where they will be used solely for the purpose of detecting plagiarism. The terms that apply to the University's use of this tool are described on the Centre for Teaching Support & Innovation web site (https://uoft.me/pdt-faq).

Students may wish to opt out of using the plagiarism detection tool. In order to opt out, contact your instructor by email no later than two (2) weeks after the start of classes. If you have opted out, then specific information on an alternative method to submit your assignment can be found below.

Additional Information

Use of git, quercus, and the lab machines to contribute to the course website may 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 13, 2022.