COSC 481
Case Studies in Computer Security

Spring 2021

Prof. Mike O'Leary
Office: YR 317
Department of Mathematics
Office Phone: 410-704-4757
Email:moleary@towson.edu
Office Hours: By appointment; online

Prof. Alex Hornberger
Office: YR 430
Department of Computer and Information Science
Office Phone: 410-704-2633
Email: ahornberge@towson.edu
Office Hours: By appointment; online

Prerequisites: COSC 440 and COSC 450

Catalog Description: An in depth study of the practical aspects of computer security, including the study of common computer security vulnerabilities in a laboratory setting.

Course Objectives: Upon completing the course, students will be proficient with the core hands-on elements of computer security. In particular, students will be able to set up and securely manage common services, and will be able to manage common defensive measures including log servers, intrusion detection systems and firewalls.

Course Materials: The required textbook is M. O'Leary, *Cyber Operations*, Apress, February 2019. This book was custom-written for this course.

Expectations: This class is intended to help students become cyber security professionals. Students are expected to act professionally at all times.

- Always ethical, all the time. Students in this class will learn techniques for both defensive and offensive cyber-security. Students will use this knowledge in an ethical manner.
- Preparation. Students are expected to be prepared for every class. This includes having read the assigned readings in advance and being ready for each exercise.
- Respect. Students are expected to treat each other with respect at all times. Live exercises are fun, and hacking into other students systems is fun and often leads to of excitement and enthusiasm. This excitement and enthusiasm will always be respectful.
- Openness and Opportunity. This course has an open-ended design. The best students take the time to move out of their comfort zone and and learn more about areas where they are weak. A student that has extensive experience in Linux at work, should take advantage of the opportunity to learn more about Windows.

Course Structure The course is designed around a 15-week live exercise where students will work in teams to build and defend a computer network from live attackers. Students will have the opportunity to perform network attacks against other teams. External experts will be brought in to serve as attackers and to evaluate student performance.

The exercise design and scenario are explained in a second document; that document also includes the grading rubric.

Attendance: Attendance is expected; you should only miss a class for a compelling reason. If you do miss a class, you are responsible for any material that you miss. Unexcused absences can result in a lower grade.

Academic Integrity: The nature of this course requires that students adhere to accepted standards of academic integrity. Violations of academic integrity include cheating, plagiarism, falsification and fabrication, complicity in academic dishonesty, personal misrepresentation and proxy, bribes, favors and threats. Cheating is a serious offense that will have grave consequences for your academic life.

Students who violate these standards will either fail the course outright or, at the instructor's discretion, may merely receive a zero on any assignment for which the student receives inappropriate assistance. Violations of these standards will be referred to the administration for possible additional action.

Students are reminded that they must follow the University Guidelines for Responsible Computing `http://www.towson.edu/adminfinance/ots/aboutots/otspolicies/responsible.asp`.

University Policies: Students are reminded that may not repeat a course more than once without prior permission of the Academic Standards Committee.