

CY3740 Systems Security

Fall 2021

General Information

Professors:	Jose Sierra
Classroom:	Online Sessions on Zoom & recordings on Canvas
Time:	Weekly Thursdays 5 to 7 pm
Office Hours:	See the pinned thread on Piazza for the link
Class Forum:	On [Piazza]

Course Description

Offers a practical overview of enterprise computer security, operating systems security, and related topics. Applies concepts such as authentication, access control, integrity, and audit to the modern operating system. Discusses and demonstrates system, process, memory, and file system-level defenses and the attacks against them. Also discusses topics in systems security assessment and cloud security.

Intructional Method

This section is a fully online with recorded video lectures. Although lectures will be recorded, **it is strongly advised that you attend and participate in classes synchronously.**

This course includes lectures and hands-on projects, so homework represents a very important work-load. It is very important that you follow the class daily (sessions, projects, and readings), because if for whatever reason you loose pace there is almost no time to catch up.

Prerequisites

Good understanding of the Linux command line is essential for success in this class. We will not cover these skills in class, so you need to prepare in advance. These skills include how to use SSH and SCP, write very simple shell scripts, check for running processes, kill runaway processes, create compressed archives, and edit files using command-line tools.

We will also use docker containers in some projects, if you have never worked with them is very important that you start preparing. We will introduce some fundamentals of containers during the first project that we use them.

There will be also some coding tasks that you will need to complete, we recommend to review python and C language.

Class Forum

The class forum is on [Piazza](#).

Why Piazza? Because they have a nice web interface, as well as iPhone and Android apps. Piazza is the best place to ask questions about projects, programming, debugging issues, exams, etc. To keep things organized, please tag all posts with the appropriate hashtags, e.g. #lecture1, #project3, etc. I will also use Piazza to broadcast announcements to the class.

Bottom line: unless you have a private problem, post to Piazza before writing me/the TA an email.

Ethics

In this class, you will learn about security techniques and tools that can potentially be used for offensive purposes; "hacking" in other words. **It is imperative that students only use these tools and techniques on systems they own (your personal computers) or systems that are sanctioned by the instructor. *NEVER* perform attacks against public systems that you do not control.** As we will discuss in class, it is ethically problematic to attack systems that you do not own, and may violate the law.

Lecture Format and In-class Prep

This class will use a traditional, lecture-style format, punctuated with in-class examples. Slides are available in canvas.

I recommend that students have access to a local Linux-style command line. You can rely on SSH or [PuTTY](#) to get a remote command line on the Khoury College machines, but you run the risk of Wifi connection issues leaving you unable to work. macOS users should be able to use the default Mac command line and [Homebrew](#); Windows users can install Linux in a virtual machine, or, if you have a recent version of Windows 10, you can [install the Windows Subsystem for Linux \(WSL\) and then download a copy of Ubuntu right from the Windows Store](#).

Schedule and Lecture Slides

Dates	Slides	Projects	Due date
Sept. 8-11	Welcome and Introduction		
Sept. 12-18	Threat Modeling		
Sept 19-25	Buffer Overflow	Proj1. Buffer Overflow	10/01 11:59pm
Sept. 26-02	Enterprise Authentication	Proj2. Enterprise Auth	10/09 11:59pm
Oct. 03-09	Access Control Models		
Oct. 10-16	SELinux and Root-kits	Proj3. Access Control	10/22 11:59pm
Oct. 17-23	Audit and Logging		
Oct. 24-30	Midterm	Proj4. Audit & Logging	11/05 11:59pm
Oct. 31-06	Secure Coding		
Nov. 07- 13	Compliance and Automation	Proj5. Secure Coding	11/19 11:59pm
Nov. 14 -20	Security Assessment		
Nov. 21 - 27	OS Hardening	Proj6. Security Evaluation	12/03 11:59pm
Nov. 28 - 04	Cloud Security	Proj7. CTF	12/10 11:59pm
Dec. 05 - 09	Final preparation review		
Dec. 14th	Final Quiz: 12-14-21 5:00pm		
.			

Books

This class does not require students to get textbooks. However, there may be additional readings from online articles and academic papers. These will be made available via Canvas or the slides.

Assignments

There will be 7 projects throughout the semester. **Assignments are due at 11:59:59pm on the specified date.** I highly recommend that students start assignments early!

Exams

There will be an final open-book quiz on December 14th 5:00pm . The exam will be take online and it will last for 1 hour. Although the exam is open-book, it is a timed exam, so you need to prepare meticulously for it. To do so, We will have preparation assignments and sessions.

Participation

I do not require students to attend class and I won't be taking attendance. That said, I prefer an interactive classroom, and I encourage everyone to attend, ask questions, and participate!

In my experience, those students who misses classes along the course ended disconnected, miss assignment deadlines and finally don't do well in the course.

I want to encourage the importance of participation and you will have some grade points on it. Participation in Piazza will be tracked and used to calculate the student participation points.

Grading

Course	Weight
Projects (7):	70%
Midterm (1)	14%
Final(1):	14%
Participation:	2%

Each assignment will include a breakdown of how it will be graded. Some projects may include extra credit components that can boost your grade above the maximum score :)

To calculate final letter grades, use the following scale: [0-69] F, [70-72] C-, [73-76] C, [77-79] C+, [80-82] B-, [83-86] B, [87-89] B+, [90-93] A-, [94-100] A.

Late Policy

For projects, we will use flexible slip days. Each student is given three (3) slip days for the semester. You may use the slip days on any project (1, 2, 3, 4, 5, or 6) during the semester in increments of one day. For example, you can hand in one project three days late, or three projects one day late. **The only exception is with the last final project, Project 7, because its submission cannot be extended from December 10th.**

In order to use a slip day you need to communicate it 24h in advance through piazza (#slipdayrequest).

After you have used up your three (3) slip days, any day late is 20% off your grade for that project.

Cheating Policy

It's ok to ask your peers about the concepts, algorithms, or approaches needed to do the assignments. We encourage you to do so; both giving and taking advice will help you to learn. However, what you turn in must be your own work. Looking at or copying code or homework solutions from other people or the Web is strictly prohibited. In particular, looking at other solutions (e.g., from other groups or students who previously took the course) is a direct violation. Projects must be *entirely* the work of the students turning them in. If you have any

questions about using a particular resource, ask the course staff or post a question to the class forum.

All students are subject to the Northeastern University's [Academic Integrity Policy](#). Per Khoury College policy, all cases of suspected plagiarism or other academic dishonesty *must* be referred to the Office of Student Conduct and Conflict Resolution (OSCCR). This may result in deferred suspension, suspension, or expulsion from the university.

Accommodations for Students with Disabilities

If you have a disability-related need for reasonable academic accommodations in this course and have not yet met with a Disability Specialist, please visit www.northeastern.edu/drc and follow the outlined procedure to request services. If the Disability Resource Center has formally approved you for an academic accommodation in this class, please present the instructor with your "Professor Notification Letter" at your earliest convenience, so that we can address your specific needs as early as possible.

Title IX

Title IX makes it clear that violence and harassment based on sex and gender are Civil Rights offenses subject to the same kinds of accountability, and the same kinds of support applied to offenses against other protected categories such as race, national origin, etc. If you or someone you know has been harassed or assaulted, you can find the appropriate resources [here](#).