COMP2633 Competitive Programming in Cybersecurity I Syllabus (2023 Fall)

Course Description:

This is the first course out of a series of three special courses that aim to prepare interested students to join the various cybersecurity competitions. The topics discussed will be practical and related to the cybersecurity competitions.2

Prerequisite(s):

None

Note: though there is no prerequisite for the course, but a good understand of the Computer hardware/software structure is essential. A solid foundation in basic OOP languages like C++/Python, and MIPS, x86_64 instruction sets will also be very useful. Enthusiasm in actively learning and updating cybersecurity knowledge on his/her own is a MUST.

Exclusion(s):

COMP3633 and COMP4633

Course Intended Learning Outcomes (CILOs):

Upon completion of the course, students are expected to be able to:

	Course Intended Learning Outcome (CILO)
1	Be able to apply and understand ethical hacking
2	Be able to master the basic knowledge required for dealing with cybersecurity threats
3	Be able to learn the more advanced knowledge for dealing with cybersecurity threats
4	Be familiar with real-world issues related to cybersecurity in various organizations
5	Be familiar with the practical skills in fighting against cybersecurity threats

Assessments:

Pass or **Failure**

Assessment Method	Description	Weighting	CILOs to be addressed
Class attendance	Attending the classes of the semester	50%	1,2,3,4,5
CTF exercises	Assessing the ability to apply learned techniques directly to some specific cybersecurity scenarios.	50%	1,2,3,4,5

Topics (could be different from semester to semester):

Topic number	**Activities**
1	**Basic knowledge:** Introduction to CTF (Capture-The-Flag) problem solving, Introduction to Kali Linux and Linux Operation (File structure, Access Control, Piping & Redirect, Regex, SSH, Common commands like ls, cat, grep, Command Injection, Local File Inclusion, etc Introduction to Python (Logics, Conditions, IO, Pwntools Library for Socket Programming, solving PoW)
2	**Advanced knowledge:** **Track A:** - **Pwn**: Introduction to Binary Exploitation, Static Analysis, Using `objdump`, `file`, `string`, Attacks like BOF, ROP... - **Reverse Engineering**: Using IDA Disassembler, Dynamic Binary Analysis, Using `strace`, `ltrace`, `gdb`, ELF format, Assembly x86_64 **Track B:** - **Web Exploitation**: OWASP Top Ten, SQL Injection / Command Injection, Cross-site scripting (XSS), Using BurpSuite / Fiddler proxies - **Cryptography**: Cryptanalysis of various cryptosystem and cutting-edge attacks. Block cipher attacks (oracles, OCB, AEAD modes vulnerabilities), weak RSA key attacks, RSA oracles etc.

	- **Computer forensics** / Stego (optional): Using `volatility`, `binwalk`, hex editors, Using `stegsolve`, image editors, `wireshark`