The Hong Kong University of Science and Technology

UG Course Syllabus (Fall 2025-26)

[Course Title] Competitive Programming in Cybersecurity I

[Course Code] COMP2633

[No. of Credits] 0-creidt

[Any pre-/co-requisites] No prerequisite, but a good understanding of the Computer hardware/software structure is essential. A solid foundation of 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

Name: Dr. Alex LAM

Email: lamngok@cse.ust.hk

Course Description

This course prepares students to take part in public Capture-The-Flag (CTF) competitions. It will introduce the students to topics like Pwn, Reverse Engineering, web exploitations, cryptography, computer forensics in the classes

Intended Learning Outcomes (ILOs)

By the end of this course, students should be able to:

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.

Assessment and Grading

This course will be assessed using criterion-referencing and grades will not be assigned using a curve. Detailed rubrics for each assignment are provided below, outlining the criteria used for evaluation.

Assessments:

Assessment Task	Contribution to Overall Course grade (%)	Deadline
Class attendance	50%	~3 days after the classes
CTF exercises	50%	~1-2 weeks after the classes

Mapping of Course ILOs to Assessment Tasks

Assessed Task	Mapped ILOs	Explanation
Class attendance	ILO1-ILO5	This task assesses students' ability to apply concepts learned in ILO1 – ILO5
CTF exercises	ILO1-ILO5	This task assesses students' ability to apply concepts learned in ILO1 – ILO5

Grading Rubrics

Course Learning Outcome	Pass	Failure	Grader
1. Be able to apply and understand ethical hacking.	Demonstrates a sufficient grasp of the idea of ethical hacking in at least some area.	Demonstrates limited understanding of the idea of ethical hacking.	This is not measured directly, but rather it is conveyed when we demonstrate all the hacking skills.
2. Be able to master the basic knowledge required for dealing with cybersecurity threats.	Demonstrates a sufficient grasp of the knowledge related to cybersecurity threats.	Demonstrates limited understanding of the knowledge related to cybersecurity threats.	This is measured by the in-class/take home exercises.
3. Be able to learn the more advanced knowledge for dealing with cybersecurity threats.	Demonstrates the ability to go deeper and understand more advanced cybersecurity threats with some assistance.	Will not be able to understand more advanced cybersecurity threats even with significant assistance.	This is measured by the in-class/take home exercises.
4. Be familiar with real-world issues related to cybersecurity in various organizations.	Demonstrates the ability to identify many of the real-world cybersecurity issues in an organization.	Will not be able to identify the real-world cybersecurity issues in an organization.	This is measured by the in-class/take home exercises.
5. Be familiar with the practical skills in fighting against cybersecurity threats.	Demonstrates the ability to apply mostly correct and precise practical skills in fighting against cybersecurity threats.	Will have limited ability to fight against cybersecurity threats.	This is measured by the in-class/take home exercises.

Final Grade Descriptors:

Grades	Short Description	Elaboration on subject grading description
Pass	Satisfactory Performance	Demonstrates sufficient grasp of the ILOs 1-5, see the grading rubrics above
Failure	Unsatisfactory Performance	Demonstrates in-sufficient grasp of the ILOs 1-5, see the grading rubrics above

Course AI Policy

This is a fundamental course, it does not allow using generative artificial intelligence tools to complete assessment tasks.

Communication and Feedback

Assessment marks for individual assessed tasks will be communicated via the course learning platform instantaneously.

Resubmission Policy

No resubmission is allowed.

Required Texts and Materials

No

Academic Integrity

Students are expected to adhere to the university's academic integrity policy. Students are expected to uphold HKUST's Academic Honor Code and to maintain the highest standards of academic integrity. The University has zero tolerance of academic misconduct. Please refer to Academic Integrity | HKUST – Academic Registry for the University's definition of plagiarism and ways to avoid cheating and plagiarism.