**Objectives**

The main objective of this assignment is for the students to understand the security mechanisms in Unix-like operating systems and their interplay with software security, in particular:

* to learn practical **access control mechanisms** in Unix operating system, such as files and folder permissions and SUID programs, and how application security is affected by them;
* to learn how software vulnerabilities can be exploited to circumvent security mechanisms in both applications and operating systems.

**Format**

This assignment uses a 'Capture the Flag' (CTF) style challenges, commonly used for cyber security training and education. Each challenge contains a 'flag' you need to discover, exploiting weakness in the program and relevant access control features of the system. This assignment has six challenges that students need to solve in the same lab VM that we have been using for the labs.

To do this assignment, you need to download a program that will install the actual challenge problems (that consist of executables and related files). Details of how to install the challenges and a brief description of each challenge can be found in the 'Assignment 1 -- Artefact' quiz link below. The description for each challenge is intentionally brief; some exploration of the given code and executable binaries are expected and are an essential part of the challenge.

**Submission requirements**

* **The artefact component (10%)**: The artefact for each challenge is the flag associated with the challenge: The flags must be submitted through the 'Assignment 1 -- Artefact' quiz link on Wattle. No other forms of submissions are allowed. This will be marked automatically on Wattle. The artefact component accounts for 10% of the total mark for this assignment.
* **The report component (90%)**: For each challenge, you are required to:
  + explain in detail your exploration of the challenge,
  + the analysis of its vulnerabilities,
  + and the exploitation steps to obtain the flag that are reproduceable.