# COMPX518-22A
# Assignment 1

**Total Marks: 100: Weightage 20%**
**Due: 1st May 2022, 5.00 PM**

## Part 1: Report on an attack (30 marks)

In late 2018-early 2019, the Australian National University (ANU) was subject to a cyber attack in which the attackers gained access to internal systems for a significant period of time. This attack has been thoroughly reported so there is a lot of information available online to study how it took place. In this part, you will learn about the attack and map it to the MITRE ATT&CK Framework (MAF) (https://attack.mitre.org/). The MAF describes various activities that generally take place in a typical attack and also outlines popular methods that attackers use for those activities. The purpose of this part of the assignment is to understand how attackers launch a targeted attack. You will also learn about MAF which is a popular framework to describe an attacker's tactics, techniques and procedures (TTPs). Your task is to learn about the ANU attack and the Mitre ATT&CK framework. For each of the tactics described in the MAF, identify the techniques and where appropriate sub-techniques that were used in the attack. Keep in mind that some tactics may have been used more than once and some never. Write this as a report where you describe each MAF tactic, then describe what techniques in the tactic were used and how in the ANU attack (sub techniques if applicable). Limit your write up to 1500 words.

## Part 2: Password Based Authentication System (70 marks)

In this part you are going to design and develop a password-based authentication system. Your system will have the ability to 1) Enrol new users 2) Authenticate those users using passwords.

*1) Enrolment*

a. In the enrolment phase the system should prompt the user for a username. The username chosen by the user should conform to the following rules
   1. Usernames should be case insensitive
   2. Usernames should only use characters from this set [a-zA-Z0-9_]
   3. Usernames should not use swear words
   4. Users shouldn't be able to bypass rule 3 by substituting numbers for letters.

b. The system should also prompt the user to set a password. Use the latest NIST password guidelines to set rules for passwords. A user's password should conform to the requirements you have set.

c. The password, the user id and other appropriate information should be stored securely using methods discussed in the lectures.

*2) Verification*

a. In the verification phase the system will prompt the user for a username and password, it will then perform appropriate verification of the username and password. Based on the outcome of the verification, the system will either display a welcome or an error message.

You will need to submit the source code and an executable file for your system. You will also write a report containing the following.

1. A component/block diagram showing various parts of your system
2. A section that shows how you are imposing the requirements for usernames
3. A section listing the password rules your system imposes
4. A section describing how you are storing the username, password and other appropriate information
5. A section describing the error messages you chose to display when the verification fails.
6. Instructions for running the executable file.

Marking scheme

1. Report on the authentication system – 75%
2. Executable runs successfully – 25%

**Assignment submission**

1. Submit the writeups of both parts as a single **pdf** file.
2. Submit the source code for Part 2 as a **zip** file.
3. Submit an executable for Part 2.

**Extensions**

No extensions will be given unless approved by the Department of Computer Science (https://www.cs.waikato.ac.nz/student-resources/application-for-an-extension-of-deadline ) You can submit late. However, late submissions will be deducted **5 marks/ day.**

**Plagiarism**

Credit all sources you refer to. Students found plagiarising will be reported to the disciplinary committee. You are expected to follow the University's guidelines here: https://www.waikato.ac.nz/students/academic-integrity/student-information/plagiarism. Assignments will be checked against anti-plagiarism checkers.