Project Description

Computer Security attacks aim to compromise the main principles of computing systems: : availability, authority, confidentiality, and integrity. These attach deploy a wide variety of techniques that is difficult to detect as they mostly simulate normal traffic connections. However using their collective behavior in terms of packet characteristic, port numbers, and protocols may provide a chance to detect these attacks with a certain probability.

The objective of this project is to use tools and techniques provided in the NETW504 course to identify the stochastic traffic characteristics of these attacks and use them to identify the probability of an attack. The techniques used can be classified as machine learning techniques. The project will use a data set provided by the University of Nevada - Reno Intrusion Detection Dataset (UNR-IDD), a NIDS dataset.

1- The data set for this project can be found at https://www.kaggle.com/datasets/tapadhirdas/unridd-intrusion-detection-dataset
2- The project will be in groups of 2 students. Please use the following form to send your group members https://forms.gle/kXdFUaP7nGkAYGpaA
3- The project will be done using Python and will mainly use the following Pandas, numpy and matplotlib python library tools.
4- The project will consist of a number of assignments that would be evaluated by the course instructor