Project Description

Computer Security attacks aim to compromise the main principles of computing systems: availability, authority, confidentiality, and integrity. These attacks 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 dataset which consists of a wide variety of intrusions simulated in a military network environment. It created an environment to acquire raw TCP/IP dump data for a network by simulating a typical US Air Force LAN