## BUILDING AN INTRUSION DETECTION SYSTEM:-

## Problem Description:

The competition task is to build a network intrusion detector, a predictive model capable of distinguishing between ''bad'' connections, called as intrusions or attacks, and ''good'' or normal connections. The dataset includes a wide variety of intrusions simulated in a military network environment.

### What is an INTRUSION DETECTOR?

Intrusion detector is a software used to detect network intrusions. It protects a computer network from unauthorized users, including perhaps insiders.

### How the data was collected?

The 1998 DARPA Intrusion Detection Evaluation Program was prepared and managed by MIT Lincoln Labs. The objective was to survey and evaluate research in intrusion detection. A standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment, was provided. The 1999 KDD intrusion detection contest uses a version of this dataset.

Lincoln Labs set up an environment to acquire nine weeks of raw TCP dump data for a local-area network (LAN) simulating a typical U.S. Air Force LAN. They operated the LAN as if it were a true Air Force environment, but peppered it with multiple attacks.

The raw training data was about four gigabytes of compressed binary TCP dump data from seven weeks of network traffic. This was processed into about five million connection records. Similarly, the two weeks of test data yielded around two million connection records.

A connection is a sequence of TCP packets starting and ending at some well defined times, between which data flows to and from a source IP address to a target IP address under some well defined protocol. Each connection is labeled as either normal, or as an attack, with exactly one specific attack type. Each connection record consists of about 100 bytes.

### Different Categories of the Attacks:-

###### *Denial-of-service (DOS) :-*

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.e.g. syn flood;

###### *Remote 2 Local (R2L) attack:-*

Remote to local attack (r2l) has been widely known to be launched by an attacker to gain unauthorized access to a victim machine in the entire network.

###### *User to root attack (U2R) attack:-*

This attack is usually launched for illegally obtaining the root’s privileges when legally accessing a local machine. , e.g. guessing password, various "buffer overflow" attacks;

###### *Probing:-*

Probing is an attack in which the hacker scans a machine or a. networking device in order to determine weaknesses or. vulnerabilities that may later be exploited so as to. compromise the system. e.g., port scanning.

# References:

* For determining the performance metric and classifiers used, download PDF:- <https://www.researchgate.net/publication/309038723_A_review_of_KDD99_dataset_usage_in_intrusion_detection_and_machine_learning_between_2010_and_2015>
* <https://arxiv.org/pdf/1811.05372>

## Dataset and Task Description:-

<http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>