CSCE 5210: Fundamentals of Artificial Intelligence

Team members:

- Mohammed Abdul Moin
- Syed Araib Karim
- Shabbab Algamdi
- Fouzan Uddin

Github: https://github.com/fouzanuddin/IntrusionDetection

Project Proposal:
A network-based intrusion detection system (NIDS) monitors a network for harmful traffic. In order to evaluate all traffic, including all unicast traffic, NIDS typically require promiscuous network access. NIDS are non-interfering devices that monitor traffic without interfering with it.

A dataset including a wide range of intrusions simulated in a military network environment was supplied for auditing. By mimicking a typical US Air Force LAN, it established an environment in which raw TCP/IP dump data for a network could be acquired. The LAN was focused as if it were a real setting, and various attacks were launched. A connection is a series of TCP packets that begin and stop at a specific time interval and allow data to flow from a source IP address to a target IP address using a well-defined protocol. In addition, each link is classified as either normal or an attack, with only one attack kind. Each connection record is around 100 bytes long.

From normal and attack data, 41 quantitative and qualitative features (3 qualitative and 38 quantitative features) are extracted for each TCP/IP connection. There are two types of classes in the class variable:

- Normal
- Abnormal

Goals and Objectives:

- Motivation:
  The goal of an IDS is to identify different kinds of malicious network traffic and computer usage, which cannot be identified by a traditional firewall. Failure to prevent intrusions could jeopardize security services' credibility, such as data confidentiality, integrity, and availability.
- Significance:
  Because it allows you to detect and respond to hostile traffic, a network intrusion detection system (NIDS) is essential for network security. The main benefit of an intrusion detection system is that it alerts IT professionals when an attack or network incursion is suspected.
- Objectives:

The Intrusion Detection System (IDS) is a detective tool that detects harmful (including policy-violating) behavior. An Intrusion Prevention System (IPS) is basically a preventive device that can both detect and block hostile activity. We can simulate an attack through the dataset and create a machine learning model to find abnormal events which can be classified as an attack.

- Features:

  The dataset contains the following features:

```
 0   duration                     25192 non-null  int64
 1   protocol_type                25192 non-null  object
 2   service                      25192 non-null  object
 3   flag                         25192 non-null  object
 4   src_bytes                    25192 non-null  int64
 5   dst_bytes                    25192 non-null  int64
 6   land                         25192 non-null  int64
 7   wrong_fragment               25192 non-null  int64
 8   urgent                       25192 non-null  int64
 9   hot                          25192 non-null  int64
 10  num_failed_logins            25192 non-null  int64
 11  logged_in                    25192 non-null  int64
 12  num_compromised              25192 non-null  int64
 13  root_shell                   25192 non-null  int64
 14  su_attempted                 25192 non-null  int64
 15  num_root                     25192 non-null  int64
 16  num_file_creations           25192 non-null  int64
 17  num_shells                   25192 non-null  int64
 18  num_access_files             25192 non-null  int64
 19  num_outbound_cmds            25192 non-null  int64
 20  is_host_login                25192 non-null  int64
 21  is_guest_login               25192 non-null  int64
 22  count                        25192 non-null  int64
 23  srv_count                    25192 non-null  int64
 24  serror_rate                  25192 non-null  float64
 25  srv_serror_rate              25192 non-null  float64
 26  rerror_rate                  25192 non-null  float64
 27  srv_rerror_rate              25192 non-null  float64
 28  same_srv_rate                25192 non-null  float64
 29  diff_srv_rate                25192 non-null  float64
 30  srv_diff_host_rate           25192 non-null  float64
 31  dst_host_count               25192 non-null  int64
 32  dst_host_srv_count           25192 non-null  int64
 33  dst_host_same_srv_rate       25192 non-null  float64
 34  dst_host_diff_srv_rate       25192 non-null  float64
 35  dst_host_same_src_port_rate  25192 non-null  float64
 36  dst_host_srv_diff_host_rate  25192 non-null  float64
 37  dst_host_serror_rate         25192 non-null  float64
 38  dst_host_srv_serror_rate     25192 non-null  float64
 39  dst_host_rerror_rate         25192 non-null  float64
 40  dst_host_srv_rerror_rate     25192 non-null  float64
 41  class                        25192 non-null  object
```

References:

- https://www.kaggle.com/sampadab17/network-intrusion-detection
- https://www.7sec.com/blog/the-purpose-of-intrusion-detection-and-prevention-systems
- https://www.alertlogic.com/blog/what-is-a-network-ids-and-why-do-you-need-it
- https://www.securityroundtable.org/the-growing-role-of-machine-learning-in-cybersecurity/