Initial Plan:

Creating a Machine Learning Model to detect DoS attacks on various Network Topologies

Author: Francesco Zucchelli

Supervisor: Amir Javed

Moderator: Jose Camacho Collados

Module Code: CM3203

Module Name: Individual Project

Credits: 40

Project Description

Denial of Service (DoS) attacks are an ever-growing problem in the networking industry. They are used to "Deny service" of the internet to the user through overwhelming their network bandwidth. Victims of these attacks range from individuals to large corporations, making it important to find new ways to combat them.

Currently, there has been a lot of research surrounding this topic [1][2][3][4]. These studies all conclude that machine learning models can be used to effectively detect when DoS attacks occur on a network. DoS attacks can be used to attack all types of businesses including banks, healthcare institutions and important public resources. Making sure we are able to detect incoming DoS attacks is important because they cause monetary loss and can disrupt services that need to be constantly running. Furthermore, DoS attacks can lead to loss and theft of data, which organisations are against as they try to maintain the integrity and security of their confidential data.

I will simulate various network topologies running on a Linux virtual machine using a cyber range. I will simulate DoS attacks and collect network traffic and process data. Furthermore, I will run these simulations multiple times, letting me validate the data I am collecting. By validating the data and simulating multiple network topologies many times, I aim to have a generalised model that is able to detect DoS attacks on a wider range of networks.

Project Aims

This project aims to create a machine learning model that can detect DoS attacks on different network topologies.

Project Objectives

<u>Core Objectives:</u>

1. Create a dataset using virtual machine simulations of network topologies.
2. Create a machine learning model that is able to detect DoS attacks on network topologies on one operating system.
    a. Specifically able to detect at least one type of DoS attack.
    b. Using the traffic and processing data that was taken from various types of network topologies. Traffic and processing data is likely to contain:
        i. Date and time
        ii. IP address of the device
        iii. The protocol the packet was sent over.

    This will help the AI read for irregularities in the traffic and identify potential attacks.

<u>Desirable Objectives:</u>

1. Multiple types of DoS attacks are detected by the ML model
2. Over 5 types of network topologies with real-life use cases.
3. Detection can occur across various operating systems

Challenges

University Equipment Reliability:

A potential challenge I face is the university equipment not working. I plan to use the University's cyber range to simulate network topologies and gather data. If the cyber range were to stop working, my project would face a major hurdle.

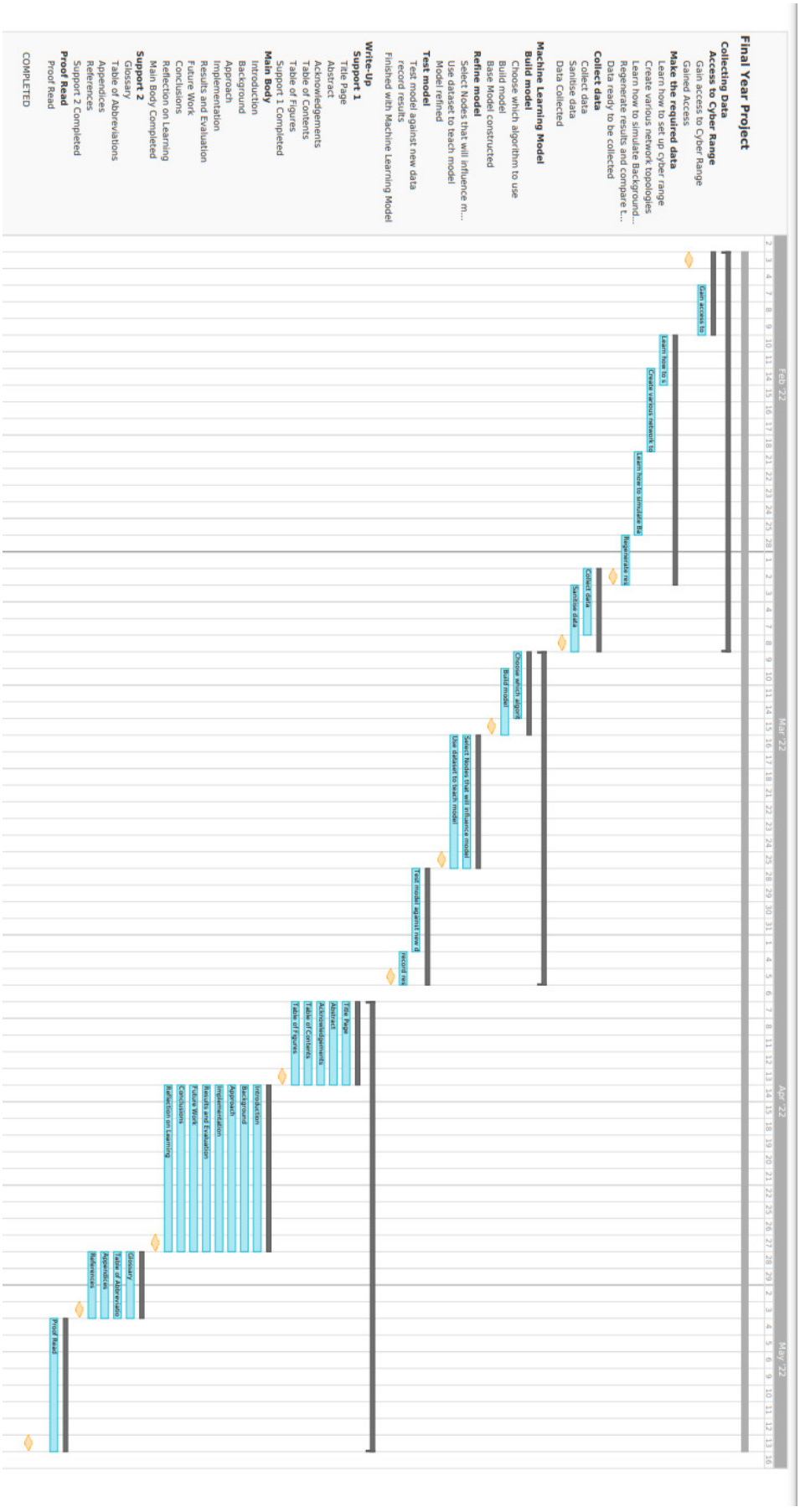
Time constraint:

In this project, I have a lot of tasks to complete that I have not done before. This may cause an overlap in how long it takes for me to do each task, leading to me possibly having issues completing the project in time.

Lack of experience:

I have never created a machine learning model. Furthermore, I have never used a cyber range. This may mean that I underestimate how long it will take for me to learn how to use the technology and bring it into practice over the next 3 months.

Work plan (ATTACHED AS SUPPORTING MATERIAL pdf)



Ethics

In this project, I find that there will be no ethical issues to discuss or evaluate. The data used in this project will not contain personal data and will be constructed artificially using a cyber range.

Supervisor meetings

I plan to have a supervisor meeting weekly either in-person or on Microsoft teams. The day of the week can change according to our schedules.

Information and studies related to my project

[1] A generalized machine learning model for DDoS attacks detection using hybrid feature selection and hyperparameter tuning
https://www.sciencedirect.com/science/article/abs/pii/S1389128621004394

[2] Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic
https://www.mdpi.com/2079-9292/10/23/2919/pdf

[3] Evaluating Machine Learning Algorithms for Detecting DDoS Attacks
https://link.springer.com/chapter/10.1007/978-3-642-22540-6_42

[4] Towards Effective Detection of Recent DDoS Attacks: A Deep Learning Approach
https://www.hindawi.com/journals/scn/2021/5710028/

[5] Types of DoS attacks https://www.fortinet.com/resources/cyberglossary/ddos-attack