Coursework 1: Set Exercises - PCAP Analysis

Github Link: <https://github.com/Mattrfish/COMP3010-SecOps-and-Incident-Management.git>

Youtube Walkthrough Link:

# Introduction

This incident report presents a detailed analysis of a provided PCAP file to investigate a suspected intrusion on the network. The purpose of this analysis is to identify the infected system, determine how the infection occurred, describe what type of attack was involved, and highlight the key indications of compromise (IOCs).

This report is structured as follows: The methodology section outlines what tools and techniques that will be used throughout the analysis and explains how they were applied to investigate the intrusion. The results section presents the key findings that I have gathered from the PCAP analysis, supported by evidence and screenshots. Finally, the conclusion summarises the overall findings and discusses prevention strategies to mitigate similar incidents in the future, and it reflects on any issues or challenges that were encountered during the investigation.

# Methodology

# Results

# Conclusion

# References

# Appendix