[redacted]

SIT327 - Network Forensics

Pass Task 4: Snort Analysis Task

Overview

This task is designed to introduce you to the fundamentals of analyzing alerts generated by Snort, a widely used Network Intrusion Detection System (NIDS). Examine the provided alert notifications and conduct research to discern their significance. Determine the criticality of the two alerts presented in the dataset and identify the specific Snort rules that triggered these alerts. Discuss the operational mechanics of these rules.

Report Submission:

Your report should address the following queries:

- Highlight the alerts you deem significant and provide justification for their importance.
- Describe the two Snort rules involved, detailing how each rule operates and leads to the generation of an alert.