|  |
| --- |
| **Student Number:** 23070471  **Student Name:** Sandeep Kumar  **Course:** MSc Cyber Security  **Supervised by:** Vito Graffagnino  **Project Title:** Intrusion Detection using SNORT  **Module Code:** 7COM1039  **Module Title:** Advanced Computer Science Masters Project |

Chapter 1: Introduction Project Overview

In this project, an open-source Intrusion Detection System (IDS) named Snort will be studied and deployed on a network which would improve the network security. Due to the growing rates and complexity of online attacks, institutions are in need of tools that can help them track and defend their online systems. Snort presents an inexpensive, rule based detection engine, which permits real time incursion recognition of threat entities, like unauthorized access, malware and brute force applications.

Background and Context

Intrusion detection systems are very important in providing overall protection of networks because they detect possible attackers by informing about it in time. The Snort has a reputation of flexibility, open-source and active community within the IDS solutions. Its rule-based framework enables it to be modified to suit different attack vectors and thus is available in small scale deployments, as well as enterprise level systems.

Since the interconnected systems are becoming more and more of the norm and the menace of cyber threats is extremely high, it is essential to comprehend the possibilities and constraints of Snort. The project aims at checking whether Snort is helpful in detection and prevention of attacks and provides useful insights in its practical use.

Research Questions

The major research questions that will be answered in this project will be as follows:

1. What is the capability of Snort in identifying and preventing real-time cyberattack?

2. How difficult is Snort to use in small and medium networks?

The project is designed to set up Snort on a virtualized platform, develop various attack situations and test its efficiency. Through comparison of its accuracy of detection, time consumption of resources as well as flexibility, the study presents a way in which Snort can be streamlined to be effectively implemented in contemporary organizations.

Report Structure

The report is structured in such a way that it can give one a clear picture of the project and the results obtained:

Chapter 1: Background - Gives a background of intrusion detection systems where the architecture and research surrounding Snort will be considered.

Chapter 2: Literature Review –It will contain reviews from different sources from multiple authors in a detailed manner.

Chapter 3: Methodology - It explains how the virtual test environment will be prepared and explains how Snort will be configured and how it will be tested and the resulting data gathered.

Chapter 4: Implementation – Explanation of how the project will be implemented including detailed explanation of steps of implementation.

Chapter 5: Results and Analysis - Evalution of the performance of snort with detection rates, false positive and efficiency measures and comparison with other IDS products.

Chapter 6: Conclusions and Recommendations - Draws conclusions of the research, estimates the questions of research, and provides ways of improving the implementation of Snort