|  |
| --- |
| **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 |

**Detailed Project Proposal**

**Intrusion Detection Using SNORT**

**1. Hypothesis**

The hypothesis here is that using the freeware Snort will help prevent, notice, and catch unauthorized access and assaults on computer systems. Snort makes IT security better for an organization by detecting threats at once, launching a protective reaction, and leaving fewer security gaps in the system. The objective of this project is to prove Snort’s value in ratio to network security.

**2. The Problem / Short Description of Your Idea**

After using digital systems as main tools; there is an increased danger of the hackers or unauthorized people to attack the organizations. An IDS improves security since it can be used to find attacks in order to protect secret information and to safeguard the stability of the network. Since Snort is an open-source, it is inexpensive and effective as opposed to the proprietary options making it popular with many people. Due to its powerful rule based feature, it surveys the entire network traffic and allows any organization to resolve security threats at the moment they take place. Snort aids organizations to be in better cybersecurity position and keep them up to the standard of good cybersecurity without spending too much money. Snort also continues to receive community based support and updates, which means businesses of all sizes will never get outdated on their part and will be accurate to the emerging threats.

**3. The Project Aim(s)**

This project aims at implementing Snort as an IDS and measure how effective it is. In order to do so, Snort must be setup properly for different network and special rules should be applied to possible dangers. The aim of this project is to check whether Snort is able to detect real problems happened in the cyber world that includes getting into system without permission and malware. The project tries to prove how Snort can work as a dependable option for anyone who wants to improve the security of their networks by reviewing how efficient Snort actually is and how it can alter itself when introduced with new systems as well as how reliable it is. The project aims to evaluate the performance of Snort under different network circumstances and determine the limit of its capacity to lower false positives and negatives as well as the open source nature of Snort offering the capability of continuous improvements and adaptability to new emerging cyber threats in dynamic situations.

**4. The Project Objectives**

The objectives of this project include:

1. Make a secure environment to test Snort’s abilities.
2. Write and place tailor-made rules for Snort to spot SQL injection and brute force attacks.
3. Perform simulations to check how Snort works and whether it detects threats correctly.
4. Compare how well Snort is performing in terms of efficiency, how many threats it catches, and how many resources it needs with other IDS algorithms.
5. Record all the steps taken in the implementation process and make recommendations for better configuring Snort in practical cases.

**5. How You Plan to Conduct Your Research**

To conduct this research, the following steps will be undertaken:

1. **Literature Review:** Review the research that exists about intrusion detection systems (IDS) and Snort’s system to see what it is built on.
2. **Network Setup:** Create a virtualized network environment using tools such as VirtualBox or VMware to simulate realistic network traffic for testing.
3. **Installation and Configuration:** Install and configure Snort within the simulated environment, ensuring compatibility and proper setup.
4. **Rule Development:** Develop custom detection rules tailored to identify specific attack patterns, such as SQL injection or brute force attacks.
5. **Traffic Simulation:** Use tools like Metasploit or Kali Linux to generate simulated attack traffic for testing Snort’s detection capabilities.
6. **Performance Evaluation:** Analyze Snort’s effectiveness by measuring its detection rate, false positives, and false negatives.
7. **Comparison and Recommendations:** Compare Snort’s results with existing IDS research and propose optimization strategies for improved performance.

**6. Project Plan**

The project will be carried out in the following phases.

**Phase 1: Literature Review**

A complete review should be conducted of academic papers, books and online resources for understanding of the theoretical foundations of intrusion detection systems, particularly Snort’s architecture and capabilities.

**Phase 2: Environment Setup**

Use Tools like Virtual Box or VMWare to layout a virtual network environment. Configure Snort to be installed and configured in this environment so that it can be ready to experiment and test.

**Phase 3: Rule development**

Create custom Snort rules to spot SQL injection and brute force based attack patterns and match the real world threat scenarios.

**Phase 4: Data collection and Testing**

Simulate a number of network attacks and recorded Snort’s detection performance in terms of its accuracy and speed of response.

**Phase 5: Analysis and Reporting is an example of the last phase in the cycle.**

Data collected during testing should be run through Snort so as to evaluate how effective it is. A detailed project report is prepared and presented consisting of findings and optimization recommendations.

**7. References**

Day, B. (2023) *Effective Network Intrusion Detection Guide: SNORT Configuration Details*. https://linuxsecurity.com/features/network-intrusion-detection-using-snort.

Karim, I. *et al.* (2017) 'A comparative experimental design and performance analysis of Snort-Based intrusion detection system in practical computer networks,' *Computers*, 6(1), p. 6. https://doi.org/10.3390/computers6010006.

Scarfone, K.A. and Mell, P.M. (2007) *Guide to Intrusion Detection and Prevention Systems (IDPS)*. https://doi.org/10.6028/nist.sp.800-94.

*SNORT – Lightweight Intrusion Detection for networks*. *Proceedings of LISA ’99: 13th Systems Administration Conference*. https://www.usenix.org/legacy/event/lisa99/full\_papers/roesch/roesch.pdf.