**STUDENT ID :**

**INTAKE ID :**

**STUDENT NAME :**

1. **Project Title**

Analyzing Attacker Logs and Prevent External/Internal Attacks

prevention system and detecting system

1. **Brief Description on Project Background.**

**Problem Context**

The exponential growth of internet and network connections has led to increased number of cyber-attack incidences often with ruinous and dangerous consequences. Malware is the primary weapon used by the attackers to carry out malicious activities over the internet, either through exploitation of the existing vulnerabilities in the computer systems/ network systems or through the application of unique features that comes as a result of the emerging technologies. Additionally, within this problem context, the development of excellent intrusion detection and prevention systems is a paramount and urgent requirement within the cybersecurity community, which is geared towards ensuring malware and other cyber-attacks are prevented from intrusion. Cybercriminals use innovative ways to penetrate to the computer and network systems, by establishing the available loopholes within the computing environment. Ideally, early detection of security incidences and accurate forecasting of the attack development forms the basis of efficient, timely and ideal response to cyber-attacks. Additionally, the development of the attacks is dependent on the future steps that are available to the attacker. With the loopholes available in the network and computer systems, the attackers will easily penetrate to the system. This can easily happen if there is no intrusion detection and prevention system within the computer systems and networks.

**Rationale**

Based on the problem stated above, the rationale behind analyzing the attackers logs in the computing and networks systems is to understand the activities going on within such a network, and ensuring that proper measures have been put in place to detect and prevent any intrusion. Additionally, the rationale is that through pursing persistent attacks, the attacker may come across operating systems and network systems weaknesses. Ideally, an extra level of protection may be required to ensure that security of such systems is safeguarded. Similarly, an extra level of protection that is emanating from the previous analysis steps, can be adopted to halt the attacker even when such operating system defenses have been overwhelmed. The benefits that are being accrued as a result of checking the log analysis and application of intrusion, detection, and prevention system involves the collection of attacker’s information and understand the vulnerabilities within the system.

**Nature of Challenge.**

Notably, the nature of the challenge that comes with the cyber-attacks is complex and critical. The complexity of such challenge is based on measures put in place to safeguard and prevent the attacks and any malicious activity from occurring. While developing any computing and network infrastructure, it important to put into consideration the security aspects of such systems, this would break any loophole within such environment. Additionally, what matters most is the existence of a robust intrusion, detection, and prevention system, which has the ability to detect and prevent any possible attack within the computer systems. In this project, the most challenging part will be the implementation, since the idea is to perform this operation within the Linux environment.

1. **Brief Description of the Project Objectives**

**Scope of the Proposal**

The scope of this proposal revolves around analyzing attacker logs and prevent External/Internal attacks, prevention system and detection system. In this proposal the idea is to provide a comprehensive understanding of the log analysis, as well as showing the implementation part of it together showing the implementation of mechanisms for analyzing external and internal attacks, prevention, and detection system.

**Deliverables**

Analyzing attacker logs and prevent external/internal attacks > prevention system and detecting system allow system administrators to analyze system logs to view all the network and operating system operations, with the aim of detecting and preventing any possible internal or external attacks. Such system will have the ability to block any malicious activity as well as showing any system vulnerabilities. Below are the core functions that the system is expected to deliver:

* Allow systems administrators to view log analysis based on specific timelines eg daily, weekly, etc.
* Detect any possible attacks or malicious operations within the operating system or network systems.
* Prevent any attacks by blocking the IP address of the attacker.
* Allowing systems administrators to manually configure the system preferences to prevent attacks
* Allow systems to print log report.
1. **Brief Description of Resources Needed by the Proposal**

**Hardware Resources.**

The minimum requirements of the hardware to successfully carry out the required operations and meeting the stated objectives include:

* Processor –Intel Core i5 (2.66GHz)
* Random Access Memory (RAM)-4GB
* Hard Disk-500GB
* Keyboard and Mouse
* Router, network cables and RJ45 connectors

**Software**

**Access to Information/ Expertize**

**User Involvement**

1. **Academic research being carried out and other information, techniques being learned.(i.e. what are the names of books you are going to read / data sets you are going to use)**
2. **Brief description of the development plan for the proposed project.(i.e. which software methodology and why, the major areas of functions to be developed and the order in which developed)**