Log Analysis of Attacks & Intrusion Detection

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 (Jang-Jaccard & Nepal, 2014). 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 (Doynikova et al., 2020). 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 (Ekelhart et al., 2015). 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.



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.



**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)
* RAM-4GB
* Hard Disk-500GB
* Keyboard and Mouse
* Router, network cables and RJ45 connectors

**Software**

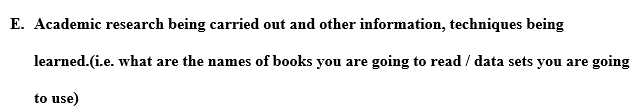
The minimum software requirement for the completion of this tasks will be as follows:

* Python
* Java Development Kit (JDK)
* MySQL version 5
* PHP 5.6
* Apache 2.4
* Visual paradigm
* Ms Word 2016

**Information Access/ Expertize**

In the development of the system under consideration, there will need a consultancy from a system administrator who will experience in developing security. The level of expertizing for the expertize on the amount of information available will depend on the tools that will be used to recognize the process and alteration of file system permission and changes to the access of the system. Apache 2.4 paradigm allows the access to log to collaborate and share ideas to expertize on security and log analysis.

**User Involvement**

Involvement of users enhances the system quality to ensure successful system implementation. The people who will be engaged are students and administrators. The effect of these users on system development will focus on attention for the information system researcher I will be the one interviewing the administrators who will be doing the system work. Accessing the work of Kajala (2003), user involvement involves designing of efficient and user friendly systems that has affirmative effects on success of the system and user satisfactions. The assessment indicates that user’s involvement as a source of information brings out the success of a project.

In carrying out various activities geared towards achieving the deliverables, there preliminary list of books that will be helpful, which include the following

**Books**

Name: Insider attack and cyber security

Author: Malek Ben Salem

Publishers: Salvatore J. Stolfo

Name: Data management, Analytics, and innovation

Author: Nureni, Taiwo, Sanjay, Adewole

**Journals**

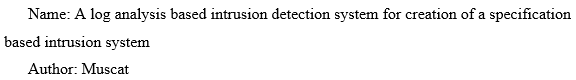
Name: Integrating attacker behavior in IT Security analysis: a discrete simulation research

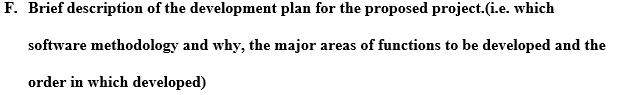
Authors: Ekelhart, Kiesling, Grill, Strauss, and Stummer

Journal Publication: Information Technology and Management.

Name: Attacker behavior forecasting using methods of intelligent data analysis

Authors: Doynicova, Novikova, and Kotenko.





**Software Methodology**

This project will be undertaken using agile methodology, which starts through definition of the users and through the documentation of the vision statement based on the scope of the problem. The rationale behind choosing agile in this project is based on its four key principles, which include the following:

* Individuals and interactions over tools
* Working software based on comprehensive documentation
* Customer collaboration based on contract negotiation.
* Responsive to changes over following a plan.]



This project will involve development of various modules, which will include the following:

* A module for log analysis
* A module for intrusion detection over the network.
* A module for intrusion prevention
* A module for log reports

The order of development will be as listed in the above section.

**G. Brief Description of the Evaluation of the Test Plans for the Proposed Project**

**Evaluation of Test Plans**

The proposed project for log analysis of attacks and intrusion, detection, and prevention must be properly evaluated and tested before actual implementation. Test plans must comprise of developing and documenting test cases to ensure that all aspects of this system is working as expected. Since the system will run on Linux environment, its evaluation will involving few commands and checking if it is logging and displaying any application errors. Once of the command that will be used to know the log analysis application is working as expected is ***apachectl configtest*** and another command would involve tailing of logs to see if there is any application logs. This command looks like this ***tail –f /var/log/messages.*** There are several other commands and test approaches that will be used in testing this application, This will including trying to ban IP address automatically and manually that is suspected to have been pursuing malicious operation in the computer networks.

**Success Criteria and How it will be Evaluated**

The success criteria of log analysis of attacks and intrusion, detection, and prevention system will be marked by through comprehensive testing. The success criteria will be marked through the implementation of the system that can log all the operations of the networks and server at the same time. Additionally, this will be evaluated by performing all forms of testing such as unit testing, integration testing, and system testing to ensure that the system is working as expected.

References

Doynikova, E., Novikova, E., & Kotenko, I. (2020). Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects. *Information*, *11*(3), 168.

Ekelhart, A., Kiesling, E., Grill, B., Strauss, C., & Stummer, C. (2015). Integrating attacker behavior in IT security analysis: a discrete-event simulation approach. *Information Technology and Management*, *16*(3), 221-233.

Intrusion detection and prevention systems: an updated review. *Data Management, Analytics, and Innovation*, 685-696.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.

Muscat, A. (2003). A Log analysis based intrusion detection system for the creation of a specification based intrusion prevention system.