Log Analysis, Prevention and Detection of the System

Student’s Name

Institutional Affiliation

Log Analysis, Prevention and Detection of the System

**Project Specification Form**

|  |  |  |  |
| --- | --- | --- | --- |
| **PROJECT TITLE: Analyzing Attacker Logs and Prevent External/Internal Attacks, Prevention and Detection System** | | | |
| **Project Background**-  This projects provides an overview of log analysis in computer and network systems | | | |
| **Problem statement**  Log analysis has been discussed in many research, there seems to be a gap in handling security log management, data, and passwords in computer and network system. | **Problem area**  Computer and Network Systems | **Nature of challenge**  The nature of the challenge is very complex in nature as intrusion have become common in the modern technological world. Hence the solution provided in this paper is by use of Intrusion Detection Systems (IDS) which has automatic event log check capabilities | **Rationale**  The rationale behind this research is to provide an insights about the problem statement in this research and provide ideal solution through the use IDS in the network infrastructure, which has the capacity to perform events log checking and hence identifying possible intrusions |
| **Project Objectives**  The main objective of this paper is to provide an overview of events log analysis in computer and network systems Additionally, this project aim to identify and show how malicious attackers can be prevented from gaining access to data in the organization's system | | | |
| **Scope of the proposal**  The scope of this proposal is to research on events log analysis and intrusion detection mechanism in computer systems | | **Deliverables**  Upon completing this paper, it present a comprehensive research of the events log analysis and implementation of cyberattacks to the companies. | |
| **Literature Review**  This paper has focused on different literature materials to provide an understanding of the research and problem statement. One of the material is by Water’s (2016), who provides an overview of event log analysis and provides information to identifying various attacks on companies. Another literature material applied in this research is by Raut (2014),who in his research affirms that intrusion detection systems provides a comprehensive review of log analysis | | | |

**Introduction**

In this modern technology, people tend to use computers, networks, and information technology systems in an organization to generate records that are logged to document system activities. Computers have become part of network distributed systems for multiple buildings located thousands of miles apart. With the development of network technologies and applications, network attackers have tremendously increased. Accessing the work of Azeez et al. (2020), Intrusion detection systems, as a critical tool in both enterprise and information systems, have played a critical role in monitoring and thwarting attackers on networks and alerting administrators to take action. Through the log analysis process, an organization can easily recognize potential threats, root causes, and other problems which an organization can mitigate risks.

Log analysis is a process that examines, interprets, and comprehends computer-generated log records. Various programmable technologies, such as network devices, operating systems, and applications, are used to produce these logs. Ideally, a log is made up of a collection of messages that are ordered in time to explain the events that are taking place within the system.1og files are streamed over an active network to a log collector, where they are stored in files to be reviewed later. System logs are generated by computer systems and contain run-time information. The current run-time information system is defined in the system log, which is an output written to a file using a separate code segment. The external attack involves risks of a person from outside the business who tries to attempt to exploit the system through malicious software, hacking, and sabotage while an internal attack occurs when an individual within an organization disrupts organizational assets. Data security separated from the database and file system provides greater security among enterprises. A signature that is based on IDs monitors the packets on the network and compares them against database signatures from malicious threats. Furthermore, the intrusion system's identification and prevention attack enables the attack log to show a list of attackers to the administrator, acting as a warning mechanism in the event of attacks across the entire network. Data usage control complements the core protection by preventing and detecting data misuse through express supervision. This paper focuses on the project's analysis of attacker logs and prevention of external and internal attacks, as well as the system's prevention and detection.

**Problem statement**

1. **Balancing of a limited quantity of log management resources with a continuous supply of log data.**

With limited resources, deciding how to handle security log management functions can be challenging, especially when there are more critical changes that affect data sources. Meanwhile, the log data source must be able to support businesses when sending too much data to the system. Additionally, to effectively comprehend technology and business risks, the log management team should be aware of the organization's business processes. In current information technology deployment, it is even so crucial to return priority to security loggings.

1. **Carelessness**

Human error is something that the company must take seriously and be aware of because a simple mistake made by an employee with access to confidential data can lead to the termination of the company. When it is careless of handling data, poor handling of passwords, and use of insecure software's can lead to company lose all the important information. Sharing passwords with the employees gives malicious insiders an easy way to access data. Notably, there are some positions in the company in which employee’s routine work with a large amount of data. Those who work in such a field can sometimes leak and compromise their data out of carelessness.

1. **Maliciousness**

In the real world, a system under attack takes immediate preventative measures rather than simplifying logging intrusion. It is not difficult for businesses to use logs to track intrusions and malicious behavior. It's worth noting that logging as an audit trail detects high-impact security changes, conducts impact analysis, and protects the company from repeat attacks. Additionally, these attackers use malicious codes to modify computer code and data that makes codes complicated to be analyzed by security researchers. The victims trick the organization to open some text messages and emails to open the link that freezes the system.

**Project Aim and Objectives**

The project's aim is to identify and show how malicious attackers can be prevented from gaining access to data in the organization's system. Analyzing logs mitigates against any threat or threat to the security of the organization's private data and any unauthorized access of the data. Security protocols monitor the system, detect breaches, and any attempted attack on the system that hosts any business data. The objectives of this project are:

1. To find out how to monitor network traffic for a particular network device and analyze the network of the system to identify suspicious activity
2. To identify how to maintain an authorized database that specifies the type of access to which resource is allowed to the user.
3. To find out how to implement security policies that specify who and what may have access to each specific system resource for the permit.
4. To research on how prevent and detect attackers using network intrusion detection system.
5. To find out intrusion among normal audit data to perform effective security measures and employing various techniques to provide security services.
6. To identify measures to address the internal and external threat and to understand how the employees perceive and change their security behavior.

**Literature Review**

The scope of the research is based on analyzing attacks of log and preventing internal/external attacks. The study performs a metadata analysis to compare and rank IDPs based on address and challenges. Insider threat is a type of information security issue in which users of an information system take advantage of their legitimate access to the system to commit a malicious act (Ophoff et al, 2014). Host-based intrusion detection system monitors the computer system on which it is installed to identify an intrusion or misuse by logging the activity and notifying the designated authority (Raut, 2018). Large company network contains variety of software’s to run on multiple devices for log files. In the developed countries, they recommend companies to have computer security log management to minimize attacks. According to Water's (2016), article it identifies and discusses specific information regarding individual and organization attacks as well a policy and technology companies can take for a holistic response to insider threats. Internet of things (IoT) a smart network t enables all things to the setup of connection for the exchange of system information using a pre-defined protocol. It gives the users remote access to everything at any time. For the last decade, signature-based IDs technique it sets attack pattern and signatures as references to check the existing network.

Based on research conducted by Workman, most of the researchers focus on the negative effect on insider threat of information security. Poor user security behavior reduces internal threat that influences the employees in the organization. Sometimes these securities depend on the behavior of the user's attitudes and beliefs. Additionally, many organizations have good and well-trained employees that run the network as well as security policies.

**Deliverables**

The detection approach will pave the way for the study and the tools to be used in the security framework. Different software geared toward successful attack defense would aid workers in the company in working efficiently in the face of any threats. This deliverable's work on system design and technical requirements will be used as a document for other project deliverables to gather the project's key details. Security has been described as a method of protecting devices from unauthorized access, theft, and damage by both external and internal attackers. To implement cyber-attack in a company categorization technique it creates a classification model to adapt multiple network paradigms. With fewer assaults, workers are more likely to identify with the organization's basic target. Notably, to implement an effective protection system to detect and mitigate an attack on the network, one has to consider and analyze threats and functions to protect the system. Typically, application files such as Adobe Portable Document Format(PDF) servers as weapon deliverable. When an attacker is successful can affect the file. If malware in an organization system records the password, this can prevent the attackers with the key to the information key. Additionally, the malware can be delivered onto a USB device despite computer security awareness and training of the users.

References

Azeez, N. A., Bada, T. M., Misra, S., Adewumi, A., Van der Vyver, C., & Ahuja, R. (2020). Intrusion detection and prevention systems: an updated review. *Data Management, Analytics, and Innovation*, 685-696.

Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M., & Johnston, K. (2014). A descriptive literature review and classification of insider threat research. In *Proceedings of Informing Science & IT Education Conference (InSITE)* (pp. 211-23).

Raut, U. K. (2018). Log based intrusion detection system. *IOSR Journal of Computer Engineering*, *20*(5), 15-22.

Waters, M. D. (2016). Identifying and preventing insider threats.