Novice Threat Model using SIEM System for Threat Assessment

Arshad Khan
Department of Computer science
Qurtuba University, Peshawar
arshidkhan1991@gmail.com

Rabia Khan
Institute of Information Technology,
Kohat University of Science &
Technology, Kohat
rabia.pk123@gmail.com

Farhan Nisar
Department of Computer science
Qurtuba University, Peshawar
farhansnisar@yahoo.com

***Abstract*— Network security attacks are the major and very common problem being faced by the security researchers as well as the network users. Different solution and techniques as well as tools and technologies have been developed and tested for the complete provision of tight security of data over the network but still hundred percent securities is not assured by any tool or technology. SIEM is the latest security monitoring and evaluation tool which is alarm based and helps in figuring out the security threats over the network. This study is based on the evaluation of the performance of SIEM within a network in order to evaluate its efficiency and the frequency as well as types of the threats it can handle. The results are quite satisfactory as it even monitors those threats which are overlooked by the administrators and the analysts during their evaluation of the threats. This software is quite effective in handling the security issues over the network but requires further assessing its capabilities to make it more effective.**

Keywords*— *Network Security, SIEM, Latest security tool

I. INTRODUCTION

Meet the security standard is always challenging for the organizations. The Information Technology sector has been quite active in refining and exploring security standards for the IT services and products. International Organization for Standardization (ISO) has been considered as pioneer in defining the standards [2].

The Information Technology is being evolved consistently and there has been a considerable evolution in the threat vectors, malware mutations and software vulnerabilities which has made the traditional security mechanisms not fit to be used for the latest software or other IT products [18]. The most common security threats are identity thefts, intrusion and hacking have most widely gained the attention of public and hence highlighted the importance of information security. The information security doesn't only result in financial losses but also business disruption and reputational loss [5].

The value and importance of USB cannot be denied in the development of IT. Majority of the electronic equipment have been manufactured with the capacity to connect through USB devices for being the easy method of transporting and storing information. Since this has been widely being used and accepted so hackers are always active to target this technology especially with the intension to damage information availability, integrity and confidentiality and this is normally done by planting malware in the USB devices. It is a fact that malware generally go undetected and can easily be executed at specified time without the user coming to know about them [19].

It is a widely accepted reality that organizations are becoming more dependent on the information systems in order to perform their business functions more actively. Due to this reason, organizations keep on complaining about the information security breaches and security attacks such as corporate reputation and image destruction, digital theft, information leakage of confidential nature and industrial espionage [17]. For providing the useful services over the internet, computers are connected with different networks and also among each other for effective communication [6]. The more enhanced access features are provided through networks, the more security risks are being raised and this has also opened further doors of attacks for the attackers and intruders. In order to attack any close network, the attackers have limited support to attack it but the more a network is open, the more attack options and loop holes are available for the attackers to bring the security of the network at stack. The main purpose of any security system is to restrict the unauthorized access to the data and information over the internet either stored in datacenters or during transit. In case of an automated system that is normally connected to some network remotely, information normally moves to and from some control application which manages the sensors through the communication lines of some public internet as well as network of automated system.

Rest of the paper is organized as follows:

- Part I Introduction and Part II Literature Study in the domain.
- Part III is the Types of security issues,
- Part IV is the SIEM Solution.
- Part V is the Analysis and Results.
- Part VI is the Conclusion

I. LITERATURE STUDY

Numerous technologies have been by now developed for the detection of the particular security threat in some network at different layers of model. But it is also important to mention

here that the information which is being generated by these security devices are generally turned down by the security personnel for having no proper ratio among the correct-false information hence this hinders the detection capacity of the devices [10]. The monitoring devices have been planted over the network for about more than three decades which started with the implementation of the remote logging through syslog protocol [9]. This syslog protocol was designed mainly to help in troubleshooting the application issues particularly on the remote servers. But later on the administrators found more uses of it and today it is being used in the network security devices, network storage, printers, routers and network switches [16]. This syslog protocol worked for about thirty years but its standard is not properly defined and is very vague and open for the interpretations.

The early work done on the security monitoring and intrusion detection is that of Dorothy Denning's "An Intrusion Detection Model" [7]. This paper highlighted the need for the development of real time intrusion detection system and also identified six components which are to be present in the intrusion detection system such as activity rules, anomaly record, profiles, audit records, objects and subjects. A famous study was conducted on providing standard data for the intrusion detection systems. The data in more a network is open, the more attack options and loop holes are available for the attackers to bring the security of the network at stack. The main purpose of any security system is to restrict the unauthorized access to the data and information over the internet either stored in datacenters or during transit. In case of an automated system that is normally connected to some network remotely, information normally moves to and from some control application which manages the sensors through the communication lines of some public internet as well as network of automated system.

This study was then analyzed by different intrusion detection technology companies for evaluating the efficacy of the existing security systems besides evaluating the experimental intrusion detection algorithms. The results of this study indicated that there is still no reliable intrusion detection system to detect all types of attacks which were investigated during the study. Even those system which are considered best in detection specific attacks' families are also not successful in monitoring majority of the attacks of same families [20]. This study paved the path for the development of the attack signatures [13].as well as the probabilistic models especially for the prediction of the anomalous activities in some network data [26].

Numerous researchers then conducted their studies to target the large volumes of the aggregated network security data which are linked with the harmless network traffic and hence termed as the false-positive alarm rate for the intrusion detection systems [11]. It is also understood that the intrusion detection systems are attacked by the hackers easily disguising themselves as the legitimate users and hence this also leads to the failure of the system to detect the malicious activities of those users [3].It has also been evaluated that if there exists a proper correlation among data from different sensors so it is very much possible to reduce the number of the generated alarms as well as limiting the false-positive ratio as observed in a network. But in an attempt to only combing the similar data as generated from the dissimilar sensors just on the basis of the similar Meta data can be at times beneficial in decreasing the large volume of the notifications but this would not necessarily result the enriched data that could be presented to the analysts. But even then some researchers are of the opinion that the correlation may be present at three different levels: meta-alert fusion, sensor coupling and event aggregation [24].

Aggregation actually is combination of the different low-level events like audit records and TCP connection. Such events have very little meta data or may be not of forensic value while analyzed separately. But the aggregation of this data brings additional highlights for any scope of some attack like denial of the services in bulks, scanning TCP at different available ports and the services at an endpoint. This means analyzing individual data from different TCP connections may not generate any significant results and may not generate the alarm for the analyst but the more connections and correlations there would be so they would generate an alarm. Even individual events may generate threads in which the parent thread may not be as damaging as the child thread. So this would generate a tree and helps in the identification of the threat in more detailed way highlighting the units and services being damaged by them.

The coupling of sensors is actually the degree in which the sensors are well aware of especially each other and are very much helpful and contributing to generating the threat alarms in the additive fashion. Generally in an ideal situation, the additive alarms would bring very little difference but they would very strongly provide an evidence of some potential threat. This phenomenon is termed as Alarm Fusion [25]. If the related events are not combined in this way so this would bring unnecessary and overwhelming alerts to the analysts and analysts also may skip the necessary and important alerts so discrimination would become very difficult. But there are numerous challenges in the effective correlation. Nature of attack, meta data obtained from the sensors and the network topology all these contribute to bring challenges in the correlation numerous data points to some single event. Aggregating the data from different dissimilar sensors is not an easy and simple job as this is always hindered by the lack of the standardization in the log formats of the sensor alarms [1].

Numerous dimensions are there for the intrusion detection system if the sensor is being deployed in the network throughout [15]. The deployment of the host based sensors and the network at numerous locations in some network actually increases probability of the corroborating alerts generation for generating the meta alarms, and hence better reports for the intrusion can be obtained. Since the frequency related to the security of the network breaches as well as the damage to the network has increased drastically within past few years. A report published in 2003 on the information security breach shows that in majority of the cases, the

disclosed information security breach did not have put any negative impact on the company's stock value [4]. Information security breach of Target Corporation in 2013 brought about $162 million damage to the corporation. For assisting in preventing the similar incidents to occur again in future, numerous regulatory committees have taken tough penalties to those entities who process the sensitive data and are not capable to prove their diligence in monitoring complete security architecture of the organization. So the security of any network would not get complete until the discussion to the security regulations have put forward. Citing any single authority for the rules and regulations for the network security breach would not be fair sine different industries follow different regulations all across the world. Most common of those regulations are NIST Cyber Security Framework, PCIDSS, ISO 27001 and COBIT [23].

Payment Card Industry Data Security Standard (PCIDSS) mainly was designed to enforce the minimum standard for the information system security for reducing the risk of the processing of the data of the credit card. This is quite simple standard and its requirements are only 12 but majority of these requirements are actually open for the interpretations and no clear interpretation has been put forward. Numerous researchers have actually criticized this standard for its leniency and ambiguity which it provides to the administrators who would interpret them as per their conscious. Even though it is wide accepted standard and also offers tough penalties for nonconformance to the standard but still the credit card data breaches have increased in the world [14].

Control Objectives for Information and Related Technology (COBIT) was created by the Information Systems Audit and Control Association for providing some general framework especially for the synergies of the information technology solutions within business processes. It mainly highlighted the importance of the Information Technology Governance concept. It mainly offers the generic guidelines for the establishment of the information technology governance along with control objectives for measuring the compliance towards the secure implementation of the mature information technology programs [21]. Though COBIT is more suitable for the establishment of the effective security framework for the security monitoring system but still it is very much ambiguous by now to be applied across different organization.

International Standardization Organization (ISO) standard number 27001 actually is derived from the previous existing best information security practices as being circulated among the community of the information security. It has series of objectives and control along with highlighting the importance of the continuously monitoring system for the security solutions. ISO 27001 is highly praised especially for providing an effective security focused standard, along with specific measures and control criteria for the enforcement of the standard [22].

II. Types of Security Issues

Before proceeding to formal security monitoring procedure, it is important to understand the different types of threats as well as the threat methodologies for establishing the accurate ontological framework especially for the analysis and alert triage. There are different types of hackers who are sitting on the network to sniff away the crucial data from the network. The most dangerous types of hackers are discussed below:

A. *Prestige Hackers*

The prestige hackers often focus on the development of techniques or code with an intention to furthering computer science, networking bodies, or the electrical engineering knowledge. This group of hackers mainly though are benign in their activities but are mainly involved in the discovery of the tools, technologies, techniques, exploits and vulnerabilities which can then be deployed by different and more dangerous groups of hackers. This group mainly doesn't use any technique itself with intension to breach the security but actually perform the in-depth analysis of the specialized sections of every single system on the network.

B. *Publicity Hackers*

They are also known as Hacktivists due to the nature of their activities which are both of activists and hackers. They mainly focus on defacing the publically available information for manipulating the media coverage through ideologically relevant activities. Though their activities are sophisticated and try to avoid the detection till their activities are revealed. While on the other hand, the unsophisticated hacktivists are actively involved in evident the denial of service campaign against the public facing website.

C. *Profit Hackers*

The profit hackers mainly manipulate the information security breaches for mere the financial gains. This involves huge number and categories of the malicious actors who focus on the development of the malware as well as involved in the organized crimes. Professional hackers, petty thieves and virus writers generally belong to this category. Mainly this group use an established mechanism for the reaping the financial benefits of the economic scales. The victims are indiscriminately targeted and same techniques normally are applied numerous times for damaging a large number of the systems to increase their profitability. They use normally well-known techniques and tools as well as same victims again and again for proving them vulnerable. It is very important to compromise the number of systems is more valuable than avoiding the detection. The comprise instances are quite rapid in this category and prevention of this category of attacks can only be prevented by proper detection system.

D. *Persistence Hackers*

They are most difficult as well as most dangerous category of hackers in detection perspective. The main goal of this group is to actually breach the network security as well as maintaining a persistent threat in some targeted environment for collecting the information. They use methodological and sophisticated approach for penetrating within a network also avoids reusing of the tools and techniques which got detected in past. Their action seems like some routine traffic of the network and also remains bellows the threshold of the detection sensors.

Normally there are four major categories of attacks namely: interruption, modification, interception and fabrication. Interruption: through this type of attacks the assets of the system get destroyed, interception: through this type of attack some unauthorized party tries to gain access to information through snooping in the communication channel, modification: here not only the information gets intercepted but also it also gets modified during transit from source to destination, fabrication: through this attack, some attacker inserts the fogged objects in the system [12].

Though there are numerous systems which provide security against any of these attacks but the most dangerous part of this story is that the more networks are getting diverse and dense, the more attackers are getting smart and more new threat types are getting introduced into the system. This is making the security more tough job on the networks. Even the sensors attacked to the networks are not delivering perfect alerts. We have a hope still and it is in shape of Security Information and Event Management System (SIEM). SIEM has the capacity to focus on the both the real time correlation and monitoring [8].

III. SIEM SOLUTION

Commercially available LogRhythm SIEM software actually provides quite mature method for data aggregation as well as analysis framework for analyzing, normalizing and collecting data as provided by the network devices which if required for the implementation of ontological models. The analytical section of the software works as depicted in figure 1.1:

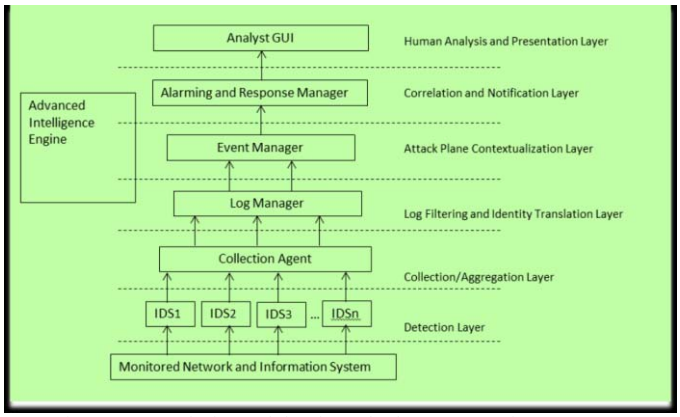

Figure 1.1: Analysis Module of Logrhythm SIEM Software

Different layers of the software works as follows:

A. *Collection Agent*

The main function of this module is to sensor, pull or receives data from different heterogeneous devices. Data encryption and compression functions mainly are conducted here before the data is being transported to log manager.

B. *Log Manager*

This unit receives and then parses the sensor data as relayed by collection agent. The parsing function entails the normalization especially in accordance with LogRhythm ontological framework besides applying the identification characteristics as per the software's entity structure. The log data may directed send to archives and may omitted basically from generating the alerts as per ontological data and similar characteristics. It helps in filtering data especially if the access to the sensor device is not granted or even device is not capable to segregation of the granular data.

C. *Advanced Intelligence Engine (AIE)*

It has numerous layers again as well as different modules for providing two major functions for establishing the multi-layer rules for attacks. The preliminary function of AIE when it appears to Log manager is to enable the primary event tracking required for the suspicion escalation. It also helps in rules aggregation as well as serial rule chaining for permitting some hierarchy of the initial attacks that are feeds to the next layer known as event manager.

D. *Event Manager*

It helps in correlation of the normalized log data from the disparate sources in some logical groups as per the rules developed within the AIE module. Such correlation helps in the enabling of the generation of the attack planes. The attack planes are generally generated depending on the data fields present within ontological framework.

E. *Alarming and Response Manager (ARM)*

It provides weighted calculations also known as Risk Based Priority (RBP) to the event data as relayed from the event manager and also determines if event warrants the elicitation or notification of the response actions. These weighting functions mainly enable the ability for establishing some global alarming threshold for excluding the alarm generation especially for the routine events of network having lower threat probabilities even then maintains the capability to collect the low level data.

F. Analyst Graphical User Interface (GUI)

It has a GUI interface addressing all the important visualization functions.

The log ontology of the software is classified in three events: security, operation and event as shown in figure 1.2:

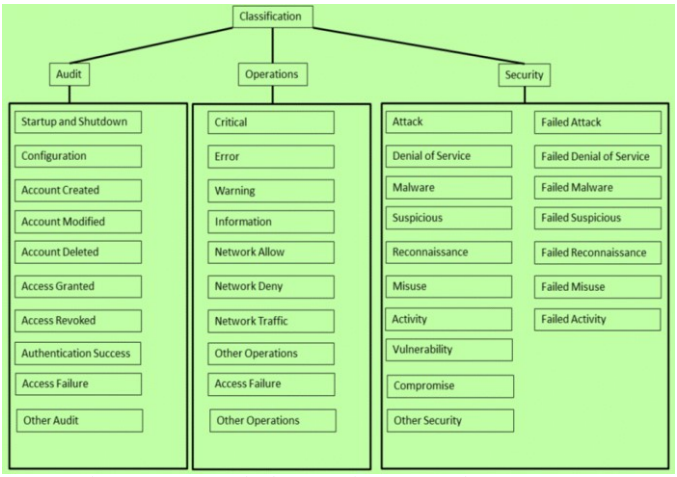

Figure 1.2: LogRhythm Security Log Ontology

IV. Analysis and Results

Different tests were performed on an organization using this software such as internal and external vulnerability tests. The external vulnerability tests performed include host identification, network route mapping, operating system identification, network services enumeration, network service exploration, vulnerability identification, vulnerability exploitation while the internal vulnerability tests conducted include SQL injection, cross-site scripting, parameter tempering, cookie poisoning, session hijacking, user privilege escalation, credential manipulation and forceful browsing. During the tests about 894 alarms were generated. About 48.7% of the alarms were known as critical condition alarms which show that the majority of the logs actually matched the generic correlation rules. 9.84% alarms generated were confirmed as the intrusion detection system while 12.64% of the alarms were counted as suspicious endpoint authentication activities.

V. Conclusion

SIEM has been tested in this study for the types and frequency of threat alarms it generates. During this evaluation, fewer alarms were generated but expectation were more. This test was conducted without the prior knowledge to the security personnel of the organization and the majority of the alarms indicated by the software were merely categorized under security threats and operations events which merely go unnoticed by the administrators. But still it is required to develop a sterilized lab for evaluating the efficacy of the proposed SIEM rules hierarchy and to remove the issues as observed in the software ontology.

REFERENCES

[1] Anderson, D. F. (2002). Heterogeneous Sensor Correlation: A Case Study of Live Traffic Analysis. Third Ann. IEEE Information Assurance Workshop (pp. 28-32). IEEE.

[2] Andrew R. McGee, F. A. (2007). Using the Bell Labs Security Framework to Enhance the ISO 17799/27001 Information Security Management System. Bell Labs Technical Journal, 39-54.

[3] Axelsson, S. (1999). The Base-rate Fallacy and its Implications for the Difficulty of Intrusion Detection. 6th ACM Conference on Computer and Communications Security (pp. 1-7). ACM.

[4] Campbell, K. G. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. Journal of Computer Security, 431-448.

[5] Carol Hsu, T. W. (2016). The Impact of ISO 27001 Certification on Firm Performance. Hawaii International Conference on System Sciences, (pp. 4842-4848).

[6] Day, J. (2008). Patterns in Network Architecture: A Return to Fundamentals. Prentice Hal.

[7] Denning, D. E. (2000). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Networks and Netwars: The Future of Terror, Crime, and Militancy, 239-288.

[8] Dorigo, S. (2012, August 28). Security Information and Event Management. Security Information and Event Management. Security Information and Event Management. Security Information and Event Management. Radboud University Nijmegen.

[9] Eaton, I. (2003, Februray). The Ins and Outs of System Logging Using Syslog. Retrieved from https://www.sans.org: https://www.sans.org/reading-room/whitepapers/logging/ins-outs-system-logging-syslog-1168

[10] Flynn, J. (2012). Intrusions Along the Kill Chain. Blackhat Security, (pp. 18-22). Las Vegas.

[11] Garcia-Teodoro, P. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 18-28.

[12] George Coulouris, J. D. (1996). Distributed Systems - Concepts and Design. Harlow: Addison-Wesley.

[13] Korba, J. (2000). Windows NT Attacks for the Evaluation of Intrusion Detection Systems. Boston: Massachussetts Institute of Technology.

[14] MacCarthy, M. (2011). Information Security Policy in the U.S. Retail Payments Industry. Stanford Technology Law Review, 40-43.

[15] McHugh, J. C. (2000). Defending Yourself: The Role of Intrusion Detection Systems. IEEE Software, 42-51.

[16] Nawyn, K. E. (2003, May 28). A Security Analysis of System Event Logging with Syslog. Retrieved from https://www.sans.org: https://www.sans.org/reading-room/whitepapers/logging/security-analysis-system-event-logging-syslog-1101

[17] Nuno Teodoro, L. G. (2015). NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements. IEEE Trustcom/BigDataSE/ISPA (pp. 418-425). IEEE.

[18] O'Reilly, D. (2012, March 20). Detect and prevent today's sophisticated malware threats. Retrieved from https://www.cnet.com: https://www.cnet.com/how-to/detect-and-prevent-todays-sophisticated-malware-threats/

[19] Rajbhooshan Bhakte, P. Z. (2016). Security Controls for Monitored Use of USB Devices Based on the NIST Risk Management Framework. Annual Computer Software and Applications Conference, (pp. 461-466).

[20] Richard Lippmann, J. W. (2000). Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation. Recent Advances in Intrusion Detection, (pp. 162-182).

[21] Sheikhpour, R. &. (2012). An Approach to Map COBIT Processes to ISO/IEC 2700.1 Information Security Management Controls. International Journal of Security and Its Applications, 13-28.

[22] Shojaie, B. F. (2014). Evaluating the effectiveness of ISO 27001:2013 based on Annex A. 9th International Workshp on Frontiers in Availability, Reliability and Security , (pp. 18-22).

[23] Susanto, H. T. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences, 21-27.

[24] Valdes, A. &. (2000). An Approach to Sensor Correlation. International Sympossium on Recent Advances in Intrusion Detection, (pp. 1-11).

[25] Valeur, F. V. (2004). A Comprehensive Approach to Intrusion Detection Alert Correlation. IEEE Transactions on Dependable and Secure Computing, 146-169.

[26] Yu, D. &. (2005). Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory. 43rd annual Southeast regional conference, (pp. 142-147).