IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 6 (June. 2019), ||S (I) || PP 65-68

Survey in Anomaly and Misuse Intrusion Detection System

Mohamed Elmubark[1], Abdelrahman Karrar[2], Nafeesa Hassan[3]
[1]*Department of Computer Science, Computer Science and Information Technology College, Al-Neelain University, Khartoum, Sudan*
m.a.almobark@hotmail.com
[2]*Department of Computer Science, College of Computer Science and Engineering, Taibah University, Al-Madinah Al-Munawarah, Saudi Arabia*
akarrar@taibahu.edu.sa
[3]*Department of Computer Science, Computer Science and Information Technology College, Al-Neelain University, Khartoum, Sudan*
dr.nafeesa@outlook.com

Abstract: An intrusion detection system is a security attack detection/prevention mechanism, it can be implemented into software module or hardware module for the purpose of monitoring the systems or network for malicious activities.The Intrusion Detection System (IDS) detection models is categorized into anomaly and misuse. Misuse Intrusion Detection define database of the well-known attacks, normally using a set of rules, In the other hand the Anomaly Intrusion Detection uses a Dynamic Approach, the rules are set considering the abnormal activity on your network. This paper studied and discussed several works on anomaly, and misuse models, then compare them in regard of performance and detection rate.

Date of Submission: 27-05-2019 Date of acceptance: 13-06-2019

I. INTRODUCTION

An intrusion detection system is a security attack detection/prevention mechanism, it can be implemented into software module or hardware module for the purpose of monitoring the systems or network for malicious activities [1]. IDS monitoring and analysing network traffic for each inbound/outbound packet and observe abnormal activity. The advantage of this service is that it protect user even if he or she is absent in the time of the attack occur, in advance this service can generate alerts and notify user when discovering any malicious activities, as a result the damage can be responded and recovered quickly, furthermore IDS allow to determine attacker behaviour and mechanisms so patches can be developed quickly and system become immune against novel attacks. Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication services as a second line of defences that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defences system. First, most of the developed applications and systems usually do not consider the security as important factor. Sometimes, in the cross platform applications and systems, the intrusion detection system is implemented to increase the security and to discover any security violations.

Also even if the protection system is able to secure the systems its desirable to identify the types of security violation happened or happening, which will lead to understand the security threats and risks that may affect the systems, and for good prepare for such violations[1].

In regard of the IDS importance it is not considered as a replacement for security prevention mechanisms, such as firewalls, authenticity or authorization systems. Moreover, IDS not provide real protection or prevention from security attacks but instead it detect and notify the attacks and the reaction to the attacks should be done through appropriate complementary security systems, and so IDS should be implemented along with other prevention security methods as a part of a comprehensive security system[2].

Main role of the IDS is to record any traffic that pass through system network then apply predefined rule that can be used to distinguish normal from malicious activity, this rule can be setup after previous analysis and classifying the normal behaviour, in some types of IDS first it get into train phase to make IDS able

to distinguish between normal and abnormal behaviour ,another types make a decision about activities depend on threshold if some user exceed it then IDS automatically generate an alarm, following we introduce different IDS types and show how its work.

II. INTRUSIONS DETECTION TYPES

Considering the resources they monitor, IDSs can also be differentiated into the following popular categories:

2.1 Host-Based Intrusion Detection System (HIDS)

HIDS utilizes the sensors located on workstations and servers to protect against attacks on specific device or machine.HIDS can scan network traffic deeply and based on predefined settings it can take appropriate decisions. The settings can be defined per OS and log data. The role of sensor is collection of necessary data for IDS analysis, and the sensors is usually located near or on a host, like server, workstation or service. Each event on the host is correlated by sending the event data to services which in turn record and correlate the events [3]. HIDS sensors or agents is located on several host types. The applications servers and client host is monitoring using the HIDS sensors. A server considered as standalone computer responsible of launching services that the client used to receive, send or connect to the data, like Web, FTP or mail servers. The client host is defined as laptop or desktop which allow the user to connect other devices and machines. The HIDS focus on monitoring machine mainly instead of the network traffic, the agent or sensor must be placed as software module in the host [3]. Furthermore, there is another type of IDS which known as hybrid IDS which is a combination of NIDS and HIDS.

2.2 Network-Based Intrusion Detection System (NIDS)

A Network Intrusion Detection System (NIDS) is one of theIDS categories. Unlike the HIDS which is monitor the host, the NIDS scan and analyze the network traffic and it decides based on the traffic purpose, whether the traffic is malicious or normal. Malicious activities is identified by scanning and monitoring the network traffic for specific segment or machine and analysing the network and application protocol activities. The NIDS is mostly placed between networks such as proxies, firewalls or routers [3].

III. INTRUSION DETECTION TECHNIQUES

Intrusion detection system use several technique to detect malicious activity, all these technique depend on fact that intruder activity is different from normal activity and its divided into following categories.

3.1 Signature Based Detection

Signature based detection is one of the IDS detection methodologies, in the signature model the network traffic is scanned according to series of malicious packet sequence or bytes [1]. The main advantage of signature technique is the simplicity of implementation if we have a clear model for the network behavior we trying to protect. For example it can be use the signature to search for a particular pattern within exploit particular buffer overflow vulnerability.

When the signature based IDS find any matching in malicious signatures with the scanned activities it rises the alerts. The matching process can be done more efficiently using the modern computers, so the cost of the power required to perform this matching can be very low. For example, if the system we need to protect only use DNS, ICMP and SMTP, then the other signatures can be ignored during matching [4].

3.2 Anomaly Based Detection

The anomaly model is based on defining the network normal behaviour into a profile. The network traffic is classified in accordance with the predefined normal profile, then it is accepted or else it triggers the event in the anomaly detection. The accepted network behaviour is prepared or learned by the specifications of the network administrators. The important phase in defining the network behaviour is the IDS engine capability to cut through the various protocols at all levels. The Engine should have the ability to understand protocols and it purposes. Though this protocol analysis is computationally expensive, the benefits it generates like increasing the rule set helps in less false positive alarms. Profile generating is a process of creating network normal behaviour and stores it into appropriate format. The profile is generated from network log that contain normal traffic, this process is done in training mode. [4].

6. IDS Comparison

Any IDS scheme must provide acceptable level of performance, accuracy, completeness, timeliness and must be secured on itself from any attacks that can stop its functionality or make unauthorized modification. IDS techniques are branched into anomaly and misuse. The anomaly detection models the normal behavior into profile or overall threshold and then compares any occurred events with this model, any deviation from this model is considered as anomaly and alerts is generated. Overall threshold approach models the normal behavior by determining maximum number of events that can occur in a specific time. if the event exceeds the threshold then it candidate to be intruder, this approach can be effective if it implemented into a single host or system that that have identical tasks, but this logic is not usually true specially into multiple users or services since each user or each service can generate events that not identical into counts in period of times, and that may produce a large number of false alarms. Profile approach uses the historical of normal events and the generate profile for each entity which may be user, protocol, network or others and then compare each entity events with their profiles, then based on this matching the event is categorize as attack or normal, also profile modelling can generate large number of false positive alarm since user may change his behavior. The disadvantage of the anomaly detections approach that it generating large number of false positive alerts, but anomaly detection has advantages in that it can detect unknown attacks.

The misuse detections models the malicious behavior and then compare any events with this models any matching is considered as attack and alert is generated otherwise the events is considered as normal. Misuse detection can models the malicious behavior using rules, signatures, state transition. These methods has a disadvantages on that the attacker can evade such methods by changing his behavior or changing attack signatures, the another issue misuse methods cannot detect zero day attacks models database needed to be updated frequently to deal with more attacks. In the other hand misuse methods produce few or no false positive alerts since it model the attack using unique characteristics. But it generates large false alerts.

Methodology comparative	
Anomaly Method	**Misuse Method**
define normal profile of users and systems as a model	define malicious behavior of known attacks as a model
any deviation from this normal model is considered as potential attack	any event matching this model is considered as attack and alert is generated
The model is defined by determining the maximum number of events that can occur in a specific time. if the event exceeds the threshold then it candidate to be intruder	The model is defined by the malicious behavior using rules, signatures, state transition.

Advantages and Disadvantages		
	Advantages	**Disadvantages**
Anomaly Method	it can detect unknown attacks	it may produce a large number of false alarms
	can be effective if it implemented into a single host or system that that have identical tasks	It is difficult to define the normal model specially into multiple users or services since each user or each service can generate events that not identical
Misuse Method	it produce few or no false positive alerts	attacker can evade such methods by changing his behavior
	Can be effective even if user behavior and system host changed.	it cannot detect zero day attacks models unless the database updated frequently to deal with new attacks

IV. CONCLUSION

This paper surveys the IDS detection methodology Anomaly approach and Misuse approach. The two methods was compared and the advantages and disadvantages of each one has been explored. This paper conclude that neither anomaly nor misuse alone can provide satisfy performance in term of false alerts, based on this fact the hybrid model has been proposed in order to reduce the false alerts and to increase IDS performance and accuracy.

REFERENCES

[1]. Bangerter, E., Barzan, S., Krenn, S., Sadeghi, A.R., Schneider, T. and Tsay, J.K., 2009, April. Bringing zero-knowledge proofs of knowledge to practice. In International Workshop on Security Protocols (pp. 51-62). Springer, Berlin, Heidelberg.

[2]. Jain, G., 2008. Zero knowledge proofs: A survey. University of Pennsylvania.

[3]. Barak, B., 2007. Lecture 15: Zero Knowledge Proofs. Computer Science Department–Princeton University, p.1.

[4]. Simari, G.I., 2002. A primer on zero knowledge protocols. Universidad Nacional del Sur, 6(27), pp.1-12.

[5]. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, D.E., 2002. SPINS: Security protocols for sensor networks. Wireless networks, 8(5), pp.521-534.

[6]. Raffo, D., 2002. Digital Certificates and the Feige-Fiat-Shamir zero-knowledge protocol. Master of Science in Computer Science Thesis, Université de Marne la Vallée, France. July 11, 2002.

[7]. PADMINI, M. and KUMAR, P., APPROACH TOWARDS SAFETY IN WSN: A SURVEY.

[8]. Knapp, J., 2009. Overview of Zero-Knowledge Protocols.

[9]. C. P. Schnorr, ”Schnorrs Protocol,” 1991.

[10]. Baldoni, M.W., Ciliberto, C. and Cattaneo, G.M.P., 2009. Elementary number theory, cryptography and codes (Vol. 2). Berlin: Springer.

[11]. Robinson, S., 2003. Still guarding secrets after years of attacks, rsa earns accolades for its founders. SIAM News, 36(5), pp.1-4.

[12]. Stein, W., 2005. Elementary Number Theory.

[13]. Tuttle, M., 1990. Knowledge and distributed computation (No. MIT/LCS/TR-477). MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE.