ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 4, pp: (1-5), Month: October - December 2017, Available at: www.researchpublish.com

# A Review of Intrusion Detection Systems

[1]Neyole Misiko Jacob, [2]Muchelule Yusuf Wanjala

[1]Jomo Kenyatta University of Agriculture and Technology
[2]Jomo Kenyatta University of Agriculture and Technology

***Abstract*: An intrusion detection system (IDS) are devices or software's that are used to monitors networks for any unkind activities that bridge the normal functionality of systems hence causing some policy violation. This paper reviews some of the intrusion detection systems and software are highlighting their main classifications and their performance evaluations and measure.**

***Keywords:* IDSs, Performance measure and Performance measures.**

## 1. INTRODUCTION

Intrusion Detection is the process of detecting actions that try to compromise the overall integrity and confidentiality of a resource. The goal therefore of intrusion detection is to identify accessors that attempt to intrude and compromise systems security controls. Current IDS examine the entire data features to detect any intrusion and misuse patterns, although some of the features may be redundant and may contribute less to the detection process [1]. Current anomaly-based intrusion detection systems and many other technical approaches have been developed and deployed to track novel attacks on systems. 98% detection rates at a high and 1% at a low alarm rate can, therefore, be achieved by using these techniques [2]. This paper review the various intrusion detection systems by evaluating their performance measures.

## II. CLASSIFICATION OF IDS

According to V. Jyothsna [3], there are three main types of intrusion detection systems: - signature-based (SBS), anomaly-based (ABS) intrusion detection systems and Network Intrusion Detection System (NIDS). SBS systems such as Snort [3] make use of pattern recognition techniques by maintaining the database of signatures of previously known attacks to compare them with newly analyzed data. An alarm is raised when similarities are established. On the other hand, ABS systems such as PAYL [4] build a statistical model to describe the normal network traffic, where any abnormal behavior that deviates from the model are identified. On the contrary, anomaly-based systems have the advantage that they can detect zero-day attacks [2].

### *A. Signature-Based Detection:*

With the explosion of internet commerce, e-business services on the web, e-banking, and other high-profile applications, organizations providing this services need to prepare themselves for the best possible protection against unauthorized penetration [5]. Signature detection involves searching network traffic for a series of malicious bytes or packet sequences. The main advantage of this technique is that signatures are very easy to develop and understand if we know what network behavior we are trying to identify. The events generated by signature-based IDS can communicate the cause of the alert. As pattern matching can be done more efficiently on modern systems, so the amount of power needed to perform this matching is minimal for a rule set. This technique can be easily deceived because they are only based on regular expressions and string matching. These mechanisms only look for strings within packets transmitting over the wire. More over signatures work well against only the fixed behavioral pattern; they fail to deal with attacks created by a human or a worm with self-modifying behavioral characteristics.

Signature-based detection system (also called misuse based), this type of detection is very effective against known attacks, and it depends on the receiving of regular updates of patterns [6]. But signature-based detection does not work well when the user uses advanced technologies like NOP generators, payload encoders, and encrypted data channels. The efficiency of the signature-based systems is greatly decreased, as it has to create a new signature for every variation. As the signatures keep on increasing, the system engine performance decreases. Due to this, many intrusion detection engines are deployed on systems with multiprocessors and multi-Gigabit network cards. IDS developers develop the new signatures before the attacker does, to prevent the novel attacks on the system. The difference of speed of creation of the new signatures between the developers and attackers determine the efficiency of the system [2].

***B. Anomaly-Based Detection:***

An anomaly-based intrusion detection system is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created [7]. The anomaly-based detection is based on defining the network behavior. The network behavior is by the predefined behavior, then it is accepted, or else it triggers the event in the anomaly detection. The accepted network behavior is prepared or learned by the specifications of the network administrators.

The important phase in defining the network behavior is the IDS engine capability to cut through the various protocols at all levels. The Engine must be able to process the protocols and understand its goal. Though this protocol analysis is computationally expensive, the benefits it generates like increasing the rule set helps in less false positive alarms. The major drawback of anomaly detection is defining its rule set. The efficiency of the system depends on how well it is implemented and tested on all protocols. Rule defining process is also affected by various protocols used by various vendors. Apart from these, custom protocols also make rule defining a difficult job. For detection to occur correctly, the detailed knowledge about the accepted network behavior needs to be developed by the administrators. But once the rules are defined, and protocol is built then anomaly detection systems work well.

***C. Network Intrusion Detection System:***

NIDS are deployed on strategic point in network infrastructure. The NIDS can capture and analyze data to detect known attacks by comparing patterns or signatures of the database or detection of illegal activities by scanning traffic for anomalous activity. NIDS is also referred as “packet-sniffers,” because it captures the packets passing through the of communication mediums [6]. The network IDS usually has two logical components: the sensor and the management station. The sensor sits on a network segment, monitoring it for suspicious traffic. The management station receives alarms from the sensor(s) and displays them to an operator.

The sensors are usually dedicated systems that exist only to monitor the network. They have a network interface in promiscuous mode, which means they receive all network traffic not just that destined for their IP address and they capture passing network traffic for analysis. If they detect something that looks unusual, they pass it back to the analysis station. The analysis station can display the alarms or do additional analysis. A fundamental problem for network intrusion detection systems (NIDSs) that passively monitor a network link is the ability of a skilled attacker to evade detection by exploiting ambiguities in the traffic stream as seen by the NIDS [8].

## III. IDS PERFORMANCE EVALUATION

The majority of published documents claiming to evaluate IDSs are conducted as comparisons, rather than evaluations. Evaluation should be considered to be a determination of the level to which a particular IDS meets specified performance targets [9]. The basic task in intrusion detection system is to classify network activities as normal or abnormal while minimizing misclassification [10]. Many problems exist in IDS and need to be addressed, such as the low detection capability against the unknown network attack, high false alarm rate, and insufficient analysis capability. Intrusion detection is targeted as a classification problem, to distinguish between the normal activities and the malicious activities [11].

According to the NSS publication “Intrusion Detection Systems Group Test (2001), the evaluation of each IDS consists of two components. The first component is a qualitative analysis of the various features and functions of each product. The comments and analysis of the various features are well considered and unbiased [12]. The group further established that

the quantitative component of consisted of four tests of the NIDSs on a controlled laboratory network. These test focused on specific performance indicators, attack recognition, performance under load, ability to detect evasion techniques and a stateful operation test.

The performance measures used by this evaluation were: a ratio of attack detection to false positive, ability to detect new and stealthy attacks, a comparison of host vs. network-based systems to detect different types of attacks, the ability of anomaly detection techniques to detect new attacks, improvements between 1998 and 1999, and the ability of systems to accurately identify attacks. The research also attempted to establish the reason each IDS failed to detect an attack or generated a false positive. Both the 1998 and 1999 evaluations identified some weaknesses with existing IDSs.

A number of these issues have since been resolved, while others are still valid. The testing process used a sample of generated network traffic, audit logs, system logs and file system information. This information was then distributed to various evaluators who would provide the appropriate data to the Intrusion Detection Systems. This ensured each system was provided with identical data while allowing proper configuration of each system.

Ranum (2001) extract established that constructing good benchmarks and tests for IDS was difficult and to accurately measure IDS complexity one needed to expand considerable efforts in designing tests by ensuring that the tests weren't inherently biased or inaccurate. This was a challenge to the IDS especially as they depend on operation environment. He further concluded that if tests were to be made, they were to base on qualitative and comparative measures. In his summary, he presented some experiences in benchmarking IDS with a focus on poorly designed tests and their effects. And a technology continues to advance the IDS management systems would become increasingly inefficient [13].

Alessandri [14] proposed the use of a systematic description scheme for regulating the descriptions used to describe IDS functions. This approach should allow for an evaluation of IDSs based upon their descriptions, without necessitating experimentation. The disadvantage of this approach is the requirement of accurate descriptions. Currently, such an approach does not exist so implementing it is not possible. This approach does hold a certain promise for the future.

## IV. PERFORMANCE MEASUREMENT CRITERIA

### *A. Ability to Identify Attacks:*

The main performance requirement of a NIDS is to detect intrusions. However, the definition of an intrusion is currently unclear. In particular, many vendors and researchers appear to consider any attempt to place malicious traffic on the network as an intrusion. In reality, a more useful system will log malicious traffic and only inform the operator if the traffic possesses a serious threat to the security of the target host. Snort is tending towards this direction with the use an alert classification ranging from 1 to 10. With 1 representing a point of interest only and 10 representing a major threat to security.

### *B. Known vulnerabilities and attacks:*

All NIDSs should be capable of detecting known vulnerabilities. However, research indicates that many commercial IDS fail to detect recently discovered attacks [15] [12]. On the other hand, if a vulnerability or attack is known all systems should be patched, or workarounds applied thus the need for a NIDS to detect these events will be removed. Unfortunately, the reality is that many systems are not patched or upgraded as vulnerabilities are discovered. This is indicated by the number of system compromises that occur every day, and the fact that most of the problems on the SANS top twenty list are predominantly old well-known problems, with fixes available.

### *C. Stability Reliability and Security:*

Any IDS should be able to continue consistently operate in all circumstances. The application and operating system should be capable of running for years without segmentation faults or memory leakage. An important function of a NIDS is to consistently report identical events in the same manner. One disadvantage of a product using signature recognition is the ability of different users to configure different alerts to provide different messages. Thus traffic on one network may trigger a different alert to the same traffic on another system of the same type.

Some efforts are currently underway to solve this problem. Both security focus and CVE provide databases of known vulnerabilities and exploits targeting them. The system should also be able to withstand attempts to compromise it. If an attacker can identify a NIDS on a network, it will prove to be a valuable asset. It is also possible the attacker will attempt to disable the system using DoS or DDoS techniques. The system should be able to withstand all of these types of attack.

***D. Ease or complexity of configuration:***

Unfortunately, the usability of a system is usually inversely proportional to the flexibility and customizability of that system. The desire for flexibility can be configurable of the system will be determined by the users of the system, the network in which it will be operating and the level of functionality required from the system. If the system is to be maintained by a network administrator who is also responsible for standard network management, he or she is unlikely to have the time available to optimize and configure the system so usability will be a primary consideration. On the other hand, if an intrusion analyst, if employed specifically to manage intrusion detection a more complex system with greater functionality, may be desired.

***E. Possible configuration options:***

The NIDS should be capable of being optimized for the systems on the network. As mentioned earlier there is no point in performing HTTP analysis if a web server is not operating on the network under inspection. The level of traffic on the network will also determine the intensity of analysis performed. A simple system suitable for a single network segment with low traffic will be able to combine the sensor and analysis functions within the single unit. A network with high levels of traffic may need to separate the sensor and analysis functions across different hosts.

***F. Scalability:***

Most organizations grow and expand over time. As they expand so do their supporting infrastructure, including computer networks. Any IDS should be capable of expanding with the network. As new network segments are added new NIDS may also be needed. Will it be possible to consolidate the reports from multiple NIDS into a single user interface? Another important question will be the storage of this information. If a small network is monitored, data storage may be possible in flat files. However as the amount of data collected grows it may be necessary to transfer this data storage into a database.

***G. Interoperability:***

Research has proven that the most effective intrusion detection requires correlating information from a range of sources. This includes NIDS, HIDS, system logs, firewall logs and any other information sources available. At the time of writing the Intrusion Detection Working Group (IDWG) had submitted some documents defining standards for communication between IDSs. It is expected that these will be released as RFCs shortly. Once these standards are implemented any IDS using the standard protocols will be able to communicate with and other IDS. This will enable an organization to implement a range of IDS from different vendors and still maintain interoperability.

***H. Vendor support:***

The level of vendor support required for an implementation will be determined by the skill levels of the staff implementing the system. However, as staff turnover rates are common in the IT industry, it is worthwhile considering the level of support that is available from the vendor.

***I. Signature updates:***

Any signature based IDS is dependent upon it signatures to detect intrusions. The abilities of these systems to detect new, or even modified intrusions has been shown to be poor (Allen 2000). For these systems to be effectively updated signatures must be available as new vulnerabilities and exploits are discovered. Many signature-based systems now allow the operator to create their signatures. This can allow the system to monitor for new alerts as they are discovered without relying on the vendor to supply updates. However monitoring vulnerabilities and writing signatures as they occur is a demanding task.

## V. CONCLUSION

Selecting and implementing a NIDS is a challenging task. There are some factors to be considered, and these factors will change from situation to situation. To ensure a successful implementation, an organization should determine its requirements and then locate a system that meets them.

## REFERENCES

[1] Srilatha Chebrolua, Ajith Abrahama, Johnson P. Thomasa,. (2005). Feature deduction and ensemble design of intrusion detection systems. ELSEVIER, Pp. 295–307.

[2] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad. (2011). A Review of Anomaly-based Intrusion Detection Systems. International Journal of Computer Applications, pp. 26-36.

[3] Shirazi, H. M. (2009). "Anomaly Intrusion Detection System Using Information Theory, K-NN, and KMC Algorithms. Australian Journal of Basic and Applied Sciences, pp. 2581-2597.

[4] Wang. K and Stolfo.S.J. (2004). Anomalous Payload-Based Network Intrusion Detection. 7th Symposium on Recent Advances in Intrusion Detection (pp. pp. 203–222). USA: LNCS Springer-Verlag.

[5] Brox, A. (2002, May 01st). THE CYBER SECURITY SOURCE. Retrieved December 20th, 2016, from SC Magazine US: https://www.scmagazine.com/signature-based-or-anomaly-based-intrusion-detection-the-practice-and-pitfalls/article/548733/

[6] Asmaa Shaker Ashoor, Prof. Sharad Gore. (2005). Importance of Intrusion Detection System (IDS). International Journal of Scientific Engineering Research, pp. 1-7.

[7] Anomaly-based intrusion detection system. (2016, July 16th). Retrieved December 20th, 2016, from Wikipedia Encyclopedia: https://en.wikipedia.org/wiki/Anomalybased_intrusion_detection_system

[8] Mark Handley, Vern Paxson and Christian Kreibich. (2001). Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics. Berkeley, CA 94704 USA: International Computer Science Institute.

[9] Wilkison, M. (2002, June 10th). FAQ: How to Evaluate Network Intrusion Detection Systems? Retrieved from SANS Technology Institute: https://www.sans.org/security-resources/idfaq/how-to-evaluate-network-intrusion-detection-systems/8/10

[10] Leila Mohammadpour, Mehdi Hussain, Alihossein Aryanfar, Vahid Maleki Raee and Fahad Sattar. (2015). Evaluating Performance of Intrusion Detection System using Support Vector Machines: Review. International Journal of Security and Its Applications, pp.225-234.

[11] Kuang, F., Xu, W., & Zhang, S. (2014). A novel hybrid KPCA and SVM with GA model for intrusion detection. Applied Soft Computing, pp. 178-184.

[12] The NSS Group. (2001, March 23rd). Intrusion Detection Systems Group Test (edition 2). Retrieved from NSS Group: http://www.nss.co.uk

[13] Ranum, M. J. (2001). Experiences Benchmarking Intrusions Detection Systems. New York City, USA: NFR Security Technical Publications.

[14] Alessandri, D. (2001). Using Rule-Based Activity Descriptions to Evaluate Intrusion Detection Systems. : RAID 2001

[15] ICSA. (2000). Intrusion Detection Systems. Japan: Information Technology Promotion Agency.