Network Intrusion Detection and its strategic importance

Conference Paper · April 2013

DOI: 10.1109/BEIAC.2013.6560100

CITATIONS
10

READS
980

5 authors, including:

Muhammad Kamran Asif
King Saud University
9 PUBLICATIONS **25** CITATIONS
SEE PROFILE

Talha ALI Khan
King Saud University
9 PUBLICATIONS **20** CITATIONS
SEE PROFILE

Talha Ahmed Taj
King Saud University
14 PUBLICATIONS **58** CITATIONS
SEE PROFILE

Muhammad Sufyan
University of Malaya
10 PUBLICATIONS **14** CITATIONS
SEE PROFILE

Network Intrusion Detection and its Strategic Importance

Muhammad K. Asif, Talha A. Khan,
Talha A. Taj, Umar Naeem
Department of Electrical Engineering,
King Saud University, Riyadh, Saudi Arabia.
Email: mkasif@ksu.edu.sa, talha.ali@ieee.org
ttaj@ksu.edu.sa, umar.n85@gmail.com

Sufyan Yakoob
Department of Electrical Engineering,
University of Malaya,
Kuala Lumpur, Malaysia.
Email: Sufyan.yakoob@hotmail.com

***Abstract*—In computer network security, a Network Intrusion Detection (NID) is an Intrusion Detection mechanism that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. There are many areas of research in this vast field of Network Intrusion Detection (NID) but in this survey paper, we will focus on its technology, development & strategic importance. Virus attacks, unauthorized access, theft of information and denial-of-service attacks were the greatest contributors to computer crime, a number of techniques have been developed in the past few years to help cyber security experts in strengthening the security of a single host or the whole computer network. Intrusion Detection is important for both Military as well as commercial sectors for the sack of their Information Security, which is the most important topic of research for the future networks.**

***Index Terms*—Network Intrusion Detection, Intrusion Detection System, Intrusion Detection.**

I. INTRODUCTION

Attacks on the network infrastructures are the big problem of the networks of today's world, with the swiftly growing illegal activities in the networking world; the network security becomes a big challenge which is neither hopeless nor solved. In the early days Firewalls are the only principle line of defense for the security of networks, the first internet wide attack and penetration was occurred by Morris Worm on 2nd November 1988 in Send mail program, since then methods have been developed to overcome it and to provide the networks with better security. In the initial days, one of the most common ways that the vendor companies used was to ship the username and password along with the equipment to overcome the risk of penetration. For the very first time in the mid 1980's the first publication of the known Denning's work about Intrusion Detection (ID) was developed. Denning assumes that intrusive activities are different from the usual activities [1] and that the IDS main job is to discover the appropriate models for normal behavior so that intrusive activity can easily be differentiated. Intrusion detection is the most recent and important research area in the field of computer networking. ID is the hot topic of the research area and many prototypes have been developed which works on different approaches both for commercial as well as military applications. ID is based on the combination of intrusion and brute force techniques. These days an IDS (Intrusion Detection System) is a vital part of the network security as it gives full protection of the network, IDS identifies both successful and unsuccessful attempts of intrusion. The purpose of the IDS is to report all the abnormal behavior of the system and negatively identify all the non-attacks. A deep study on the behaviors and the signature of the intrusion detection, IDS can give a real time response of all such intrusion events. IDS can also perform the following tasks.

- Keep an eye on the system and user activities.
- Verification of the system errors.
- Evaluating the integrity of systems and data files.
- Note down any abnormal behavior make statically records.

978-1-4673-5968-9/13/$31.00 ©2013 IEEE

- Recognition activity model mapping known attacks and alerts.

The purpose of IDS is not only preventing the attack to be happened but to identify and report it to the network administrator, there are some IDS that respond to the illegal intrusion in the system by terminating the network connection [2].Primary criterions of measurement for IDS are as follows.

- TRUE POSITIVE: legitimate attack (IDS gives alarm).
- FALSE POSITIVE: no attack (IDS gives alarm).
- FALSE NEGATIVE: legitimate attack (IDS gives no alarm)
- TRUE NEGATIVE: no attack (IDS gives no alarm).

Secure and protected network systems should provide the following services.

- Data confidentiality
- Data and communications integrity
- Assurance against denial-of-services attacks

Data confidentiality does not disclose data against any unauthorized person and allow access along with the secure connection, so no intruder can harm it. Data and communications integrity service is concerned with the accuracy, fidelity, without damaging the chunks of information, and believability of information transfer between networks and outside world. All this service must ensure perfect operation of the system hardware and software and it should protect against unauthorized modification of data. Denial-of-service is a website hacking attacks and risk. It occurs when access to a (remote) entity is unavailable. While such attacks are not completely avoidable but we can reduce the probability of these attacks. The common approach to secure a computer or network system is to build a protective cover around it in terms of security settings. Intruders who need to enter the system must recognize and verify themselves through some security checks [3].

II. TECHNOLOGY AND APPROACHES OF INTRUSION DETECTION

In this section we present the approaches of the ID that includes the categories of IDS and techniques of ID.

A. Types of Intrusion Detection system

There are two primary categories of IDS:

- Network Based Intrusion detection system.(NIDS)
- Host based Intrusion detection system (HIDS).

HIDS make their decision based on the information they obtained from the single users; on the other hand NIDS monitor the whole traffic of the network from which the hosts are connected, it obtains data from them and make their decisions. NIDS is cost effective and gives immediate real time detection of the network attacks so it reduces and decreases the chance of the damages of the network because of the intrusion activities .On the contrary, HIDS permits the collection of the data on each and every single host which gives a better image what is going on at each host instead of monitoring the entire network. For instance, if we consider high traffic network where the loss of packets happened by the network monitoring system whereas the host monitor can report every step and event occur on each host. Other kind of the IDS is called hybrid IDS and is divided into three further categories.

- Per- Host Network IDS
- Load Balanced Network IDS
- Firewall IDS.

B. Methods and Techniques in Intrusion Detection

Intrusion Detection Systems (IDS) refers to a program used to detect an intrusion when it happens and to prevent a system from being compromised [4]. There are two types of IDS.

- Anomaly Intrusion detection
- Signature-based IDS or Misuse Detection.

1) ANOMALY INTRUSION DETECTION: Anomaly-based IDS establish a baseline of normal usage patterns, activities and any other thing that deviates from its original pattern are identified as a possible intrusion. Anomaly detection method can investigate user patterns, such as profiling the programs executed daily, executed with access to resources that are inaccessible to ordinary users. Anomaly intrusion detection depends on the pattern of computer usage. It notices the computer performance and reported if some abnormal behavior and trend occur in the network. The anomaly system depends upon the principle that the intrusive activities are completely different from non-intrusive activities. The major advantage of anomaly detection is its strength to identify novel attacks. Its disadvantage includes the necessity of training the system on noise, with the attendant difficulties of tracking natural changes in the noise distribution. Changes may cause false alarms while an intrusive activity that seems to be normal may cause missed detections. It is difficult for anomaly-based systems to classify or name attacks. It does not prevent and report if the attack is completely new; so in order to work properly it has to update its self which consume a lot of time. The main approaches of anomaly intrusion detection are as follows:

a. Neural Networks

Neural networks are made so they can identify the arbitrary patterns in input data, and compare such patterns with an outcome, which can be a binary indication of whether an intrusion has occurred.

b. Predictive Pattern Generation

Keeping in mind the results of the previous events it tries to predict the future event.

2) MISUSE DETECTION: Signature-based IDS or Misuse Detection mainly depends on identifying known signatures. This indicates that the attack can be represented in the form of the particular pattern or signature. So, the slight modifications in attack can be easily mis-detected. There are certain ways to develop a signature.

- Hard translation of attacks.
- Automatic Training.
- Learning using label sensor data.

A signature based IDS will monitor packets on the network and compare them against a database of signatures from known malicious threats. They operate in such a way same as a virus scanner, by searching for a known attack or signature for each specific intrusion event [5]. Signature-based IDS is very efficient at sniffing out known attack, it does like anti-virus software, depend on receiving regular signature updates, to keep in touch with variations in the hacker technique [6]. The most common and popular attacks can easily be identified by this approach. However one of the main problems in it is how to develop such a signature that includes all the modifications and variations of the attack. This technique is not adoptable to a slight change of the attack signature and if the attack pattern is completely unknown. The SNORT is one of the most famous an open source signature based IDS which many researchers made this IDS as a benchmark function against their IDS .Some of the approaches of the signature based IDS are as follows:

a. State Transition Tables

It describes a chain of the evidence that a hacker does in the form of a state transition diagram. When the behavior of the system matches those states, an intrusion is detected.

b. Pattern Matching

This method allow encoding of the famous signature as patterns which are then compared with the data Some of the other Intrusion Detection techniques used to detect the intrusion are as follows:

c. Genetic Algorithms

Genetic algorithms such as Particle swarm optimization algorithm used in the ID.The application of GAs in IDS research started in early 1995 and involves evolving a signature that indicates intrusion. Another similar method is the Learning Classifier System in which binary rules are evolved, that collectively recognizes patterns of

intrusion [4].

d. Fuzzy logic

It is the collection of ideas and concepts made to solve ambiguity and error. A set of principles compose to describe a relationship between the input variables and the output variables, which may identify if an intrusion has occurred.

e. Immune Systems

Immune systems mimic natural immunology as observed in biology. There are many different methods present such as negative selection, immune network model and clonal selection [7] describes that cells not only can tell the evidence for antigen presence, but also danger signals.

f. Bayesian Method

It is a graphical model which contains the set of the random variables and their conditional dependencies; in which each node represents the random variable and the non-connected node represent the variables which are independent from each other. The major benefit of this technique is to deal with the incomplete data.

g. Decision Tree

It is a model that can be used to show possible results for particular occurrences in which the conditional probabilities are assigned for each occurrence. Those occurrences of intrusions form a tree based structure that contains root node and a number of leaf nodes. Decision tree is very useful even for the large amount of data.

III. IDS MECHANISM FOR INFORMATION AND DATA COLLECTION

Data collection is very important part of any IDS. It consists of many levels of data which are collected as follows:

- Network data
- System request of operating system
- Inside of any application
- Keystrokes
- Command line of operating system

Systems that collect the data from the operating system which are subject to attack are called host based data. The other to the host-based sensing is to observe the traffic of the network that goes to and from the system or systems being monitored and look for possible attacks of intrusion in that data. The benefit of that method is that a single sensor can monitor a number of hosts and can look for attacks that target multiple hosts. The only drawback of this approach is it cannot see attacks such as those made from a system console, those made from a dial-up modem connected directly to the host.

IV. RESEARCH AND DEVELOPMENT OF INTRUSION & DETECTION

There are many techniques; some of them are discussed below:

A. IDS Based on Data Mining Technique

Data Mining (DM) is a method in which some hidden Predictive information is extracted from a large, incomplete, noisy and unclear data at random. [8] A data-mining approach is based upon the automatic extraction of features from a large set of data. It has great potential of solving the unknown patterns from the large number of audit data, the algorithms used for mining audit data are as follows:

- Classification
- Link Analysis
- Sequence Analysis

The only problem with the audit trails is that the data collection is so huge that analysis from it is very expensive. On the contrary, despite of its immense advantages, it is still an immature technique and required a lot of research to be done in it.

B. IDS Based on Data Fusing Technique

Multi sensing data technique is relatively a new method used to integrate the data from the multiple sources and sensors in order to make interferences between event, activities and situations; so we can use multiple sensors fusion technique for intrusion

detection [9]. Data fusion used known and famous ID patterns and templates; it focuses on the current state of the network with the help of the past data. The main problem of the data fusion based technique is how to combine the multiple sources in the network. Bayesian approach is one of the key method to achieve it, data fusion techniques is the most hot research field in the near future.

V. FUTURE OF INTRUSION DETECTION

In the recent years, the field of intrusion detection is of greater importance than ever before. The existing Intrusion Detection systems have many problems, for instance, lack of speed over the network, lack of support regarding IPv6 addressing scheme, high levels of false positive and false negative alarm rates, the lack of intrusion detection benchmarking, lack of accuracy in the real time detection.

In order to resolve all these issues and to make further progress, our future Intrusion detection systems must have some promising direction. The Research must focus in developing quick response techniques for decreasing system damages to minimize within best times when an information system is attacked, future work must address techniques and approaches of performing active defense to network attack behaviors, there should be a massive amount of work still to be done for tracing and obtaining evidence techniques of attach behavior and diagnosing techniques for security events.

VI. CONCLUSION

In this paper a brief overview of Intrusion Detection technology is presented and also highlights its importance by evaluation and analysis of current Intrusion Detection technology, its challenges at the moment and future promising directions of Intrusion Detection technology. At present, Intrusion detection is not a mature technology, thus having large number of available opportunities and fresh working domains for Researcher, Engineers and Scientists. Its applications are widely deployed across the globe; larger amount of military and commercial spending are now focused towards the research and development of new Intrusion Detection Systems. Since, having a greater potential attack would not disappear forever, so Intrusion Detection technology will improve endlessly.

REFERENCES

[1] D. E. Denning, "An intrusion-detection model," *Software Engineering, IEEE Transactions on*, no. 2, pp. 222–232, 1987.

[2] Y. Bai and H. Kobayashi, "Intrusion detection systems: technology and development," in *Advanced Information Networking and Applications, 2003. AINA 2003. 17th International Conference on*. IEEE, 2003, pp. 710–715.

[3] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," *Network, IEEE*, vol. 8, no. 3, pp. 26–41, 1994.

[4] M. F. Marhusin, D. Cornforth, and H. Larkin, "An overview of recent advances in intrusion detection," in *Computer and Information Technology, 2008. CIT 2008. 8th IEEE International Conference on*. IEEE, 2008, pp. 432–437.

[5] E. Nikolova and V. Jecheva, "Anomaly based intrusion detection using data mining and string metrics," in *Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on*, vol. 3. IEEE, 2009, pp. 440–444.

[6] J. McHugh, A. Christie, and J. Allen, "Defending yourself: The role of intrusion detection systems," *Software, IEEE*, vol. 17, no. 5, pp. 42–51, 2000.

[7] D. Dasgupta, "Advances in artificial immune systems," *Computational Intelligence Magazine, IEEE*, vol. 1, no. 4, pp. 40–49, 2006.

[8] S. Naiping and Z. Genyuan, "A study on intrusion detection based on data mining," in *Information Science and Management Engineering (ISME), 2010 International Conference of*, vol. 1. IEEE, 2010, pp. 135–138.

[9] M. Shankar, N. Rao, and S. Batsell, "Fusing intrusion data for detection and containment," in *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*, vol. 2. IEEE, 2003, pp. 741–746.