www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 3, Issue – 2. April 2018

CLASSIFICATION OF IDS APPROACHES AND THEIR TECHNIQUES

1. Rajeshkumar, 2.S.Saranya, 3.N.Thangamani
1. Assistant Professor, Department of Computer Applications
2. Assistant Professor, Department of Computer Applications
3. Assistant Professor, Department of Computer Science
AJK College of Arts & Science, Coimbatore.

Abstract

Intrusion detection systems (IDS) help detect unauthorized activities or intrusions that may compromise the confidentiality, integrity or availability of a resource. This paper presents a general overview of IDSs, the way they are classified, and the different algorithms used to detect anomalous activities. It attempts to compare the various methods of intrusion techniques. It also describes the various approaches and the importance of IDSs in information security. This paper presents about various types of network attacks mainly web attacks, and different Intrusion Detection Systems(IDS) which are in use. This may pave a path to design a new type of IDS which may protect the network system from various types of network attacks.

Keywords: Intrusion Detection System, Signature, Anomaly, Host, Network.

1. INTRODUCTION

A computer network is a set of computers connected together for the purpose of sharing resources. A network attack can be perpetrated by an insider or by an outsider. In the “inside attack", the attack is initiated by an entity inside the security perimeter, the person who has complete authorization involves in the vulnerable activities, that is, the attacker tries to access some system resources for which he is not having the authorization. It is very tough to find out this type of persons. An "outside attack" is initiated from the outside that is by an unauthorized or illegitimate user of the system. In the Internet, the outside attackers may be amateur pranksters or organized criminals or international terrorists or even hostile governments. A computer network consists of two components namely hardware and software. Both of these components may have their own risks and vulnerabilities. Hardware threats are easy to detect and also it cause harm only to the device rather than the data. The Hardware threats are of four types: Physical, Electrical, Environmental and Maintenance. If the attack is in software, mainly it harms the data. Previously, only the persons with high programming skills were involved in writing of hacking programs. But now, a person who has a little knowledge of programming may become a hacker just by downloading hacking tools from the internet. Beside this, everyone wants to use the high featured software for its attracting features and it leads them to undergo the attack easily. Having high features is very much prone to lack in the security. The three goals of Software Security threat are Confidentiality, Integrity and Availability. The mostly used network and which has a large number of users is the Internet connection. This internet is almost in all the fields. Even though the attack is in all types of networks, the most challenging one is the attack in

Wide Area Network, that is the Web attack. Network security is an area where each and every user wants his system to be protected from the intruders. As the intrusion detection system increases in number, similarly the attacks are also taking a new birth or a new form. Knowing these vulnerabilities of the IDS, its advantages and disadvantages surely will help to plan and build a network security system. In turn it helps to work on the network safe.

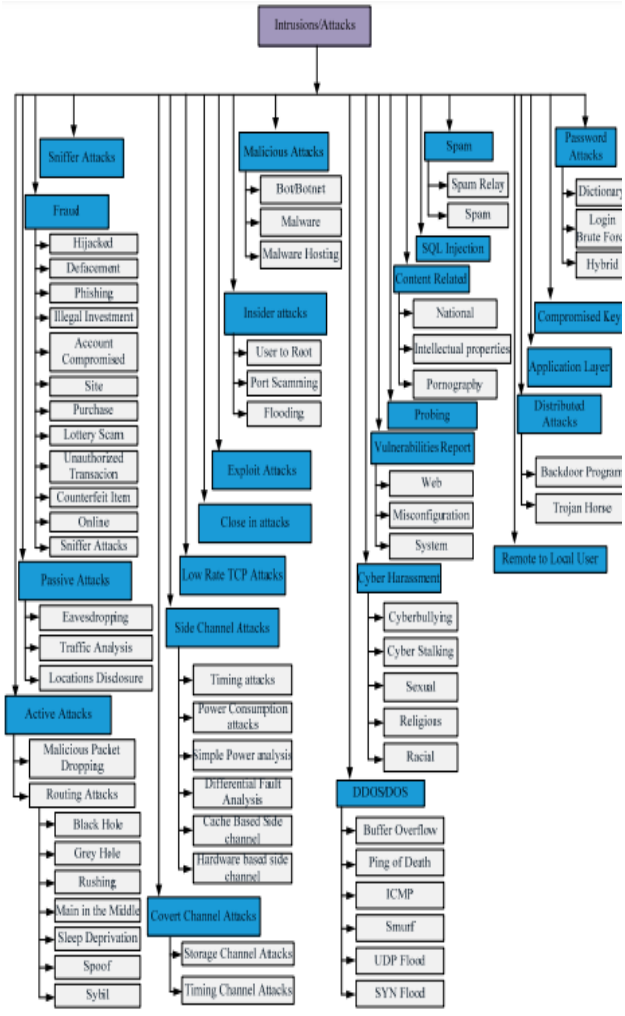

Figure 1: Type of Intrusions / Attacks

Intrusion detection is defined as identifying unauthorized use, misuse and abuse of computer systems by both inside and outside intruders. The main task of an intrusion detection system (IDS) is to defend a computer system or computer network by detecting hostile attacks on a network system or host device, monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions. Security incidents resulting from attempted attacks violate the CIA triad of computer security; Confidentiality, Integrity and Availability.

2. LITERATURE SURVEY

Dubey, Shreya, and JigyasuDubey proposed study is an investigation of IDS (intrusion detection system) and their design concept. For that purpose an intrusion detection system is developed using the analysis of KDD CUP 99's dataset. The main focus is given over classification and performance improvement of classifiers. The proposed IDS system utilizes the k-mean clustering algorithm, Bayesian classification algorithm and finally the back propagation neural network. The implementation of the desired system is performed using MATLAB IDE. In order to justify the performance outcomes, the proposed classification technique is compared with the traditional Bayesian classifier. According to the obtained performance the proposed classification technique provides optimum classification accuracy and error rate improvement over the traditional method but the performance is similar in terms of prediction time. On the other hand the memory consumption of the traditional method is better than the proposed method. Our proposed approach

provides better accuracy then the conventional kmeans, k-nearest neighbor and naive-bayes. According to the obtained performance the system is adoptable and efficient. In near future the performance of the classification is improved more as reducing the steps of algorithm which is time consuming. **Tseng, Chin-Yang, PoornimaBalasubramanyam** propose a specification-based intrusion detection system that can detect attacks on the AODV routing protocol. In a specification-based intrusion detection approach, the correct behaviours of critical objects are manually abstracted and crafted as security specifications, and this is compared with the actual behaviour of the objects. Intrusions, which usually cause object to behaviour in an incorrect manner, can be detected without exact knowledge about them. This approach can, thus, address unknown attacks as well. The IDS presented in this paper is built on a distributed network monitor architecture that traces AODV request-reply flows. Network monitors audit every RREQ, RREP and RERR in order to build and update complete request-reply session trees and corresponding forwarding tables. Constraints on the request-reply flow are specified using finite state machines. It describes procedures for constructing and processing the session trees, and present examples of detecting attacks successfully. This research is the first effort to apply specification-based detection techniques to detect attacks in the routing within ad hoc networks. The work illustrate that our algorithm can effectively detect most of the serious AODV routing attacks effectively, and with low overhead. **Faisal, Mustafa Amir, Zeyar Aung** proposed in this paper, proposed architecture for the comprehensive IDS in AMI, which is designed to be reliable, dynamic, and considering the real-time nature of traffic for each component in AMI. Then, it conducts a performance analysis experiment of the seven existing state-of-the-art data stream mining algorithms on a public IDS data set. Finally, it is elucidate the strengths and weaknesses of those algorithms and assess the suitability of each of them to serve as the IDSs for the three different components of AMI. This has been observed that some algorithms that use very minimal amount of computing resources and offer moderate level of accuracy can potentially be used for the smart meter IDS. On the other hand, the algorithms that require more computing resources and offer higher accuracy levels can be useful for the IDSs in data concentrators and AMI head ends. **Roesch, Martin** proposed in this paper Snort was designed. This proposed design is used to fulfill the requirements of a prototypical lightweight network intrusion detection system. It has become a small, flexible, and highly capable system that is in use around the world on both large and small networks. It has attained its initial design goals and is a fully capable alternative to commercial intrusion detection systems in places where it is cost inefficient to install full featured commercial systems. **Debar, Herve, Monique Becker** proposed in this paper, intrusion detection system has been proposed. The user model which is developed in this paper is the complement of a statistical model, because neural networks cannot adequately handle all the available data. The tight coupling between the neural net and the expert system is necessary to analyses the output of the net and propose explanations and a clear diagnosis to the security administrator.

3. CLASSIFICATION OF IDS

3.1 Signature based

In signature based detection mechanism the attack patterns are saved in the database. Each packet of the network traffic is compared with the attack patterns to detect abnormal behavior. Signature based intrusion detection system detects only know attacks. If attack signatures are clearly defined then it has low false positive. Requires specific knowledge of intrusion behavior and collect data before the intrusion could be out of date. Difficult to detect unknown attacks. Raises alerts regardless of the outcome. Example if a windows worm tries to attack a Linux system then the IDS sends many alerts of unsuccessful attack. The knowledge of the attacks is dependent on the specific environment.

3.2 Anomaly based intrusion detection system

Anomaly based intrusion detection system is based on the network behavior. The network behavior is defined by the administrator or is learned by the dataset during the training phase of the development of IDS. Rules are defined for normal behavior and abnormal behavior. Example, Snort and Bro-IDS are anomaly based intrusion detection system. It has the ability to detect unknown attacks. Defining the rule set for intrusion detection is difficult. Efficiency of system depends on the fitness of the rules and its testing on the testing datasets.

4. INTRUSION DETECTION APPROACHES

IDS vendors implement their products in different ways and there are consequently several ways to categorize intrusion detection systems. The first is based on the scope of the IDS's monitoring; that is, whether it is installed on and uses data from a single host computer, or is a network-based product that monitors traffic on the network as a whole, as well as analyzes data from individual computers. Another difference in implementation has to do with how the vendor markets the system, either as a software product or as an integrated hardware device (appliance).

4.1 Host-based intrusion detection

A host-based IDS is one in which the software is installed on a single system and the data from that system is used to detect intrusions. Because the host-based IDS protect the server "at the source," it can more intensely protect that specific computer. The host-based system usually examines log files on the computer to search for attack signatures. Important system files and executables may also be checked periodically for unexpected changes. A host based system will also monitor ports and trigger an alert if certain ports are accessed.

4.2 Network-based intrusion detection

A network-based IDS monitors data from network traffic as well as data from one or more host computers to detect intrusions. A network-based IDS analyzes data packets sent over the network, and generally uses a "promiscuous" network adapter (one that is capable of reading all of the packets sent over the network, rather than just those packets addressed to it). The network-based IDS examines packet headers, which are generally not seen by the

host-based IDS. This allows the detection of Denial of Service (DoS) and other types of attacks that may not be detected by a host-based IDS.

5. DETECTION TECHNIQUES

From different sources, systems like rule based expert systems, state transition analysis, and genetic algorithms are direct and efficient ways to implement signature detection. Inductive sequential patterns, artificial neural networks, statistical analysis and data mining methods have been used in anomaly detection. There are different kinds of frameworks used for anomaly-based detection. This section presents an extensive study over the various intrusion detection classifier techniques and hybrid detection techniques. A few proposed methods could be described as follows.

5.1. Bayesian Networks

Bayesian networks are probabilistic graphical models that represent sets of variables and their probabilistic independencies. Bayesian theory is named after Thomas Bayes. His theory can be explained as follows: If the events A1, A2, … and An constitute a partition of the sample space S such that $P(Ak) \neq 0$ for k = 1,2 , … , n, then for any event B such that $P(B) \neq 0$: Bayesian networks are directed acyclic graphs where the nodes represent variables and whose edges encode conditional dependencies between those variables. These are applied to anomaly detection in so many ways; for example, Valdes et al. has developed an anomaly detection system that employed naive Bayes, which is a two-layer Bayesian network that assumes complete independency between the nodes.

5.2. Genetic Algorithm (GA)

GA is a search technique that is used to find an appropriate solution to search problems. Genetic algorithms have been applied in anomaly detection in many ways, as they are flexible and a powerful search method. Some network intrusion detection approaches have used genetic algorithms for the classification of instances, while others like fuzzy data mining approach have applied this technique for feature selection. To list out an advantage of GA, it selects the best feature and has better efficiency but its method is complex.

5.3. Inductive Rule Generation Algorithms

These algorithms are one of the most famous techniques used. In this technique, we have a predictive model decision tree that maps observations of an item to conclusions about the item's target value. The decision tree (DT) is very powerful and popular data mining algorithm for decision-making and classification problems. It is also used in many real-life applications like medical diagnosis, radar signal classification, weather prediction, credit approval, and fraud detection. This decision tree can be constructed from large volume of dataset with many attributes, because the tree size is independent of the dataset size. It can process both numerical and categorical data but trees created from numeric datasets can be complex. Construction of inductive rule generation algorithms may not require any domain knowledge. It can handle high dimensional data and the representation is easy to understand. However, it is limited to one output attribute. Decision tree algorithms are unstable and most decision

tree construction methods are non-backtracking,

5.4. Outlier Detection

Outlier detection approach is based on the idea of semi-supervised learning in which the system would learn a baseline data, and consider any instances that do not fit in the normal data profile as an anomaly. Most of the anomaly detection algorithms require a set of baseline data to train the model, and they assume that anomalies can be treated as patterns never observed before. Since an outlier is defined as a data point which is very different from the rest of the data, so based on some measure, we employ several outlier detection schemes to see how efficiently these schemes may deal with the problems of anomaly detection. In statistics-based outlier detection techniques, the data points are modeled using a stochastic distribution and these points are determined to be outliers depending upon their relationship with this model.

5.5. Clustering

This technique is based on two important assumptions. First, majority of the network connections represent normal traffic and only a very small percentage of that traffic is malicious. And second, malicious traffic is statistically different from normal traffic. Anomalies will be detected based on their cluster size, i.e., large clusters are meant to be baseline data, and the rest correspond to malicious attacks. Clustering is unsupervised learning. Labeling the data is not necessary and natural patterns in the data are extracted. It does not require the use of a labeled data set for training.

5.6 Neural Networks

Neural networks are networks of computational units that jointly implement complex mapping functions. First, the networks are trained with a labeled data set. Testing instances are then fed into the network to be classified as either normal or anomalous. An example of the neural network technique which is widely used in anomaly detection is the Support Vector Machines (SVM). This method would be effective if the exact characteristics of the attack are already known. However, these intrusions are constantly changing because of the individual approaches taken by the attackers and regular changes done in the software and hardware of the targeted systems. Because of the wide variety of attacks and attackers despite their dedicated effort to constantly update the rule base of an expert system can never hope to accurately identify the variety of intrusions.

Conclusion

We have introduced an overview of the different types of intrusion detection systems, approaches, methodologies and techniques for IDSs. Each technique and class of IDS has its superiority and limitations, so we should be mindful when selecting the best approach. We compared and contrasted each technique and approach to determine which works best in a particular situation. We focused our study on the most common intrusion detection models such as NIDS and HIDS, and both the anomaly- and signature-based approach to detection.

References:

[1] Deepthy K Denatious & Anita John, “Survey on Data Mining Techniques to Enhance IntrusionDetection”, International Conference on Computer Communication and

Informatics (ICCCI 2012), Jan. 10,2012, Coimbatore, INDIA

[2] Rung - Ching Chen , Kai - Fan Cheng and Chia - Fen Hsieh,“ Using Rough Set And Support Vector Machine For Network Intrusion Detection ”,International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009

[3] David Ndumiyana, Richard Gotora and Hilton Chikwiriro, “Data Mining Techniques in Intrusion Detection: Tightening Network Security” , International Journal of Engineering Research & Technology (IJERT) , Vol. 2 Issue 5, May – 2013

[4] Roesch, Martin. "Snort: Lightweight Intrusion Detection for Networks." InLISA, vol. 99, no. 1, pp. 229-238. 2014.

[5] Debar, Herve, Monique Becker, and Didier Siboni. "A neural network component for an intrusion detection system." In Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on, pp. 240-250. IEEE, 1992.

[6] Peddabachigari, Sandhya, Ajith Abraham, CrinaGrosan, and Johnson Thomas. "Modeling intrusion detection system using hybrid intelligent systems." Journal of network and computer applications 30, no. 1 (2007): 114-132.

[7] Shah, Bhavin, and Bhushan H. Trivedi. "Improving Performance of Mobile Agent Based Intrusion Detection System." In Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on, pp. 425-430. IEEE, 2015.

[8] Rosenberg, Ishai, and Ehud Gudes. "Evading System-Calls Based Intrusion Detection Systems." In International Conference on Network and System Security, pp. 200-216. Springer International Publishing, 2016.

[9] Nápoles, Gonzalo, IselGrau, Rafael Falcon, Rafael Bello, and Koen Vanhoof. "A Granular Intrusion Detection System Using Rough Cognitive Networks." In Recent Advances in Computational Intelligence in Defense and Security, pp. 169-191. Springer International Publishing, 2016.