A Review on Network Intrusion Detection System

Preeti Yadav , Divakar Singh

M.Tech Department of CSE , Barkatullah University Institute of Technology , Bhopal India

Head of CSE Department , Barkatullah University Institute of Technology , Bhopal India

Abstract: Internet and computer networks are exposed to an increasing number of security threats. For new types of attacks are emerging constantly, developing flexibility and adaptability safety-oriented approaches is a serious problem. In this context, the anomaly-based network Intrusion detection techniques are valuable technology to protect the target systems and networks against malicious activities. However, despite a number of these methods described in the literature in recent years, security tools comprising detecting anomalies function is only beginning to emerge, and several important issues remain to be solved. This paper begins with the review of the best-known anomaly-based intrusion detection techniques. Then the available platforms, systems development and research projects are presented. Finally, the main issues are addressed for large deployments, anomaly-based detectors disruption, with special emphasis on the evaluation questions.

Keywords: Networks, Security, Intrusion Detection Systems.

1. Introduction

As the cost of information processing and downs availability of the Internet, organizations are still vulnerable to potential cyber threats, such as network attacks. Computer intrusion is actions that violate the security of the system. Such situation must be detected and corrected in order to guarantee the integrity, confidentiality and/or the availability of computing resources. Intrusion Detection Systems (IDS) are designed to complement other security measures, based intrusion prevention (firewalls, antivirus, etc.). The goal of IDS is to inform the administrator of suspicious activities and recommend specific measures to prevent or stop the attack (for example, near the network ports, kill the offending process, etc.). So, make it possible to implement such measures, IDS must, among other tasks, analysis of network data in order to determine whether there is evidence of an attack or whether the data are anomalous in respect normal data, the system should be sufficiently generalized in order to detect any type of attack still maintain low false positive rate. False positive action is of great importance in determining the quality of IDS [2]. So there is a need to ensure a stable and secure transaction through the use of firewalls, intrusion detection systems (IDS), encryption, authentication, and other hardware and software solutions. Many IDS variants exist which allow security managers and engineers to identify attack network packets primarily using signature detection, ie IDS "recognizes" attack packets due to its well-known "fingerprints" or signatures as those packets pass through network's gateway threshold. On the other hand, anomaly-based ID systems what is the normal operation of the network and reports abnormal traffic behavior. IDS are designed to reliably detect the probe, DOS, U2R, and R2L Data on attacks against Solaris, Sun OS, Linux

and Windows NT operating systems with low false alarm rates. However, for most installations, the complete prevention of the attack not realistically achievable due to system complexity, configuration and administrative errors and misuse by authorized users. Therefore, the attack Detection is an important aspect of the ongoing efforts of computer security [1].

2. IDS techniques

Basically two types of detection techniques are used for the implementation of IDS systems 1. Anomaly Detection 2. Signature Detection.

3. Anomaly Detection

Designed to detect abnormal patterns, IDS provides a baseline of normal use of the device, and everything, to the extent possible, deviates from it will be marked as a possible intervention. What is considered anomalies can vary, but usually we like anomaly event that occurs at frequency greater than or less than two standard deviations from the statistical norm. Identifies anomalies as deviations from "normal" behavior and automatically detects any deviation from labeling the latter as a suspect. Thus these techniques identify new types of distortion as deviations from normal use. It is an extremely powerful and novel tool, but the potential disadvantage is the high false alarms may therefore previously unseen (yet legitimate) system behavior also recognized as an abnormality, and therefore reported as a potential intrusion. If the user graphics department suddenly starts accessing accounting programs or compilation code, the system can correctly tell your manager. Following are the methods used for Anomaly Detection

3.1 Statistical Technique

In a statistical technique based, network traffic activity is captured and represents your profile stochastic behavior is created. This profile is based on these metrics as traffic speeds, the number of packets for each protocol connection speed, number of different IP addresses, etc. Two sets of data traffic are considered in the process of detection of anomalies: one side corresponds to the currently observed profile over time, and the second is for previously trained statistical profile. As network events, current profile determined and anomaly score comparability of estimation normally shows irregularity rate for certain events, such as the Intrusion Detection System marks the occurrence anomaly, when the score exceeds a certain threshold.

3.2 Machine learning

Machine learning techniques are based on the establishment of explicit or implicit model, which allows analyzing patterns be characteristic of these programs is it is necessary for the marked data train behavioral model, procedure, which puts severe demands on resources. In many cases, the application of machine learning principles organizations coincides with the statistical methods although the former is focused on building a model that improving its performance based on previous results. Therefore, machine learning has the ability to change their implementation of strategies for acquiring new information. Though this feature may make it desirable to use these systems for all situations, the main disadvantage is the expensive source nature.

List of the machine learning techniques used for anomaly detection and their properties.

Technique	Speed	Accuracy
Neural Network [12]	Fast	Average
Support Vector Machine [13]	Average	High
Genetic Algorithm [14]	Fast	Average
Markov Models [15]	Average	Average
Bayesian networks [16]	Slow	Average
Clustering [17]	Fast	Low
Fuzzy Logic Techniques [18]	Fast	Average

3.3 Knowledge-based

The so-called expert system approach is one of the most widely used knowledge-based IDS systems. However, as other-NIDS methodology can also be expert systems included in other, different categories. Expert systems are intended to include audit data according to a set of rules involves three steps. First, different attributes and classes are estimated from the training data. Secondly, a set of classification rules, parameters and procedures are derived. Third, the audit data are divided accordingly.

4. Signature Detection

Here each instance in a data file is labeled as "normal" or "annoying" and learning algorithm is trained over labeled data. These techniques are able to automatically retrain intrusion detection models on various input data, which include new types of attacks as long as were labeled accordingly. Unlike signature-based IDS, patterns of abuse are created automatically and can be more complicated and more accurate than manual signature creation. They have high accuracy in detecting known attacks and variants thereof. Their disadvantage is that they cannot detect unknown attacks and they rely on signatures extracted by human experts. This method uses specifically known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures. Host based for intrusion detection, one example of a signature is "three unsuccessful login." For intrusion detection, signature can be as simple as a specific pattern that corresponds to the network packet. Signatures such as packet content and / or header content signatures may indicate unauthorized actions, such as incorrect FTP signature does not necessarily real attempt to gain unauthorized access. Depending on the robustness and the severity signature that is triggered if some alarm, response or notification shall be sent relevant authorities.

4.1 Signature Basics

Network IDS signature is a pattern that we find in operation. To get an idea of the various signatures, let us quickly review some examples and some of the methods that can be used to identify each of them:

- Attempting to connect from a reserved IP address. This can be easily identified by checking the source address field in the IP header.
- A packet with illegal TCP flag combination. It can be found by comparing the symptoms listed in the TCP header against known good or bad flag combinations.
- E-mail containing a specific virus. The IDS can compare the subject of each e-mail on the topic associated with the virus laden e-mail, or they can look forward to an attachment with a particular name.
- DNS buffer overflow attempt contained in the payload query. Based on the analysis of

the DNS field and control the length of each of them, the IDS can identify an attempt to perform a buffer overflow via DNS field. Another way would be to look at the sequence exploit shell code in the data section.

- Denial of Service attack on the POP3 server issuing the same command caused a thousand times. One signature of this attack would be to track how many times the command is issued, and warned that if this number exceeds a certain threshold.
- Access to file assault on the FTP server files and directories issuing commands to it without logging state tracking signature could be developed that would monitor FTP traffic for a successful login and would note that some orders were issued before the user has been authenticated correctly .

As it can be seen from this list, signatures, ranging from very simple - checking the value of the header field a very complex signatures that can actually monitor the connection status or to perform an extensive analysis of the protocol. In this article we will be looking at some of the easiest signatures and discuss the intricacies involved in the development of even the most basic signature. Note that the signature abilities vary greatly between IDS products, so some of the techniques described here may not be possible at IDS are using. For example, some network IDS products provide little ability to customize existing signatures or write your own, while other IDS products will give you the ability to customize all your signatures and write almost every sign you can think of. Another important factor is that some IDS products can only verify some header or payload values, while other products can provide you with data from any part of each packet.

4.2 Role of Signature

The different signatures have different goals. The obvious answer is, that we want be alerted when will occur to distortions attempt. That has unusual header properties and wants to write signature, which will correspond to this known pattern. Or perhaps you have a interest about configuring the IDS for identification of the abnormal or suspected communication in general, not only attacks or suction. Some signatures can say, which specific attack occurs or what vulnerability attacker is trying to use, while other signatures may just mean, that the unusual behavior occurs, without giving a concrete attack. That with often take considerably more time and resources to identify the tool, of which it causes malicious activity, but will give as more information about it, why you are was attacked, and it, what intention attack is.

5. Conclusion

Of course, the effectiveness of IDS depends on the environment in which they are to be used. Monitoring a large, diverse network is very different from the smaller, homogeneous environments. Models of signature analysis are best suited for medium-sized networks, who want to catch the standard threats. Administrators can draw fantastic Community support for release updated signatures and performance is not a decisive factor. However, a larger, ever-changing network might benefit from some of the strengths of Anomaly analysis: power, minimal false positives and general but more expensive solutions, the introduction of IDS includes two machines, each with a different model system. Unfortunately, very little afford such a luxury.

Reference

[1] J. Balthrop. Personal communication, November 2004.

[2] J. Balthrop, F. Esponda, S. Forrest, and M. Glickman. Coverage and generaliszation in an artificial immune system. Proceedings of GECCO, pages 3-10, 2002.

[3] J. Balthrop, S. Forrest, and M. Glickman. Revisiting lisys: Parameters and normal behaviour. Proceedings of the Congress on Evolutionary Computation, pages 1045-1050, 2002.

[4] K. Begnum and M. Burgess. A scaled, immunological approach to anomaly countermeasures (combining ph with cfengine). Integrated Network Management, pages 31-42, 2003.

[5] P. Bentley, J. Greensmith, and S.Ujin. Two ways to grow tissue for artificial immune systems. In C. Jacob, M. J. Pilat, P. J.Bentley, and J. Timmis, editors, Proceeding of the 4th International Conference on Artificial Immune Systems (ICARIS-2005), volume 3627 of Lecture Notes in Computer Science, pages 139-152, Banff, Alberta, Canada, August 2005. Springer.

[6] C. L. Blake and C. J. Merz. Uci repository of machine learning databases. http://www.ics.uci.edu/mlearn/MLRepository.html, 1998. Irvine, CA: University of California, Department of Information and Computer Science.

[7] U. Aickelin, J. Greensmith and J. Twycross "Immune System Approaches to Intrusion Detection - A Review". In Proceedings ICARIS-2004, 3rd International Conference on Artificial Immune Systems, LNCS 3239, pp 316-329, Springer-Verlag, Catania, Italy. 2004.

[8] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod. Danger theory: The link between ais and ids. In Proc. of the Second Internation Conference on Artificial Immune Systems (ICARIS-03), pages 147-155, 2003.

[9] U. Aickelin and S. Cayzer. The danger theory and its application to ais. In J. Timmis and P. J. Bentley, editors, Proceeding of the First International Conference on Artificial Immune System (ICARIS-2002), pages 141-148, University of Kent at Canterbury, U.K., Sep. 2002. University of Kent at Canterbury Printing Unit.

[10] S. Axelsson. Intrusion detection systems: A survey and taxonomy. Technical Report No 99-15, Chalmers University of Technology, Sweden, 1999.

[11] M. Ayara, J. Timmis, R. de Lemos, L. N. de Castro, and R. Duncan. Negative selection: How to generate detectors. In J. Timmis and P. Bentley, editors, Proceedings of the 1st International Conference

[12] S. Devaraju, S. Ramakrishnan "DETECTION OF ACCURACY FOR INTRUSION DETECTION SYSTEM USING NEURAL NETWORK CLASSIFIER", International Journal of Emerging Technology and Advanced Engineering Volume 3, Special Issue 1, January 2013.

[13] Razieh Baradaran and Mahdieh HajiMohammadHosseini "Intrusion Detection System based on Support Vector Machine and BN-KDD Data Set", 7thSASTech 2013, Iran, Bandar-Abbas. 7-8 March, 2013.

[14] Sreeja M. S., Aarcha Anoop 'New Genetic Algorithm Based Intrusion Detection System for SCADA", International Journal of Engineering Innovation & Research Volume 2, Issue 2, ISSN: 2277 – 5668.

[15] Megha Bandgar, Komal dhurve, Sneha Jadhav,Vicky Kayastha,Prof. T.J Parvat "Intrusion Detection System using Hidden Markov Model (HMM)", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 3 (Mar. - Apr. 2013), PP 66-70.

[16] Alma Cemerlic, Li Yang, Joseph M. Kizza "Network Intrusion Detection Based on Bayesian Networks", University of Tennessee at Chattanooga Chattanooga, TN 37403.

[17] S.A.Joshi, Varsha S.Pimprale "Network Intrusion Detection System (NIDS) based on Data Mining", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 1, January 2013.

[18] BHARANIDHARAN SHANMUGAM NORBIK BASHAH IDRIS "Anomaly Intrusion Detection based on Fuzzy Logic and Data Mining", Proceedings of the Postgraduate Annual Research Seminar 2006.