Nehru E- Journal
A Journal of Nehru Arts and Science College (Autonomous)
Journal Home Page: http://nehrucolleges.net/jo.html
ISSN: 2349-9052

Research Article
Vol 6 issue 1(2018)
(Jan - July 2018)

Intrusion Detection System – A Literature Survey

Dr.V.Suganthi,[*1], P. K. Manoj Kumar [2]
[*1,2,3] Department of IT & CT, Nehru Arts and Science College, Nehru Group of Institution, Nehru Gardens, T.M.Palayam, Coimbatore-641105
***Corresponding Author:** suganthi.grd@gmail.com

Keywords:

Information,
Network,
Security,
Channel

Abstract

Intrusions detection systems (IDSs) are systems that try to detect attacks as they occur or after the attacks took place. IDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network. Intrusion detection systems can be misuse-detection or anomaly detection based. Misuse-detection based IDSs can only detect known attacks whereas anomaly detection based IDSs can also detect new attacks by using heuristic methods. In this paper, a Literature survey is conducted to study the various methodologies for hybrid approach.

Introduction

Nowadays with the spreading of the Internet and online procedures requesting a secure channel, it has become an inevitable requirement to provide the network security. There are various threat sources including software bugs mostly as the operating systems and software used becomes more functional and larger in size. Intruders who do not have rights to access these data can steal valuable and private information belonging to network users. Firewalls are hardware or software systems placed in between two or more computer networks to stop the committed attacks, by isolating these networks using the rules and policies determined for them. It is very clear that firewalls are not enough to secure a network completely because the attacks committed from outside of the network are stopped whereas inside attacks are not. This is the situation where intrusions detection systems (IDSs) are in charge. IDSs are used in order to stop attacks, recover from them with the minimum loss or analyze the security problems so that they are not repeated [1]. IDSs collect information from a computer or a computer network in order to detect attacks and misuses of the system. Many IDSs only analyze the attacks and some of them try stopping the attack at the time of the intrusion. Three types of data are used by IDSs. These are network traffic data, system level test data and system status files [2,3].

Literature Survey

A hybrid IDS is developed by combining the two approaches in one system. The hybrid IDS is obtained by combining packet header anomaly detection (PHAD) and network traffic anomaly detection (NETAD) which are anomaly-based IDSs with the misuse-based IDS Snort which is an open-source project.

A hybrid intrusion detection system combines k-Means, and two classifiers: K-nearest neighbor and Naïve Bayes for anomaly detection [4]. It consists of selecting features using an entropy based feature selection algorithm which selects the important attributes and removes the irredundant attributes. This algorithm operates on the KDD-99 Data set; this data set is used worldwide for evaluating the performance of different intrusion detection systems. The next step is clustering phase using k-Means.

KDD99 (knowledge Discovery and Data Mining) intrusion detection[5] contest is specified. This system can detect the intrusions and further classify them into four categories: Denial of Service (DoS), U2R (User to Root), R2L (Remote to Local), and probe. The main goal is to reduce the false alarm rate of IDS1.

Highlights

•The proposed method hierarchically integrates a misuse detection model and an anomaly detection model [6].

•C4.5 decision tree algorithm for building a misuse detection model is used.

• Decomposition of the normal training data into smaller subsets is performed using the model.

• Build multiple one-class SVM models for the decomposed subsets.

•This approach results in high detection performance and reduces the detection time complexity.

IDS types

There are two approaches to analyzing of events using IDSs. These are misuse-based and anomaly-based approaches. Misuse-based IDSs aim to distinguish events that violate system policy. Anomaly-based IDSs try analyzing abnormal activities and flag these activities as attacks. Both approaches have advantages and disadvantages when compared to each other [1,2,5]. Snort is the most commonly used signature-based intrusion detection system. Snort is a network intrusion detection system that runs over IP networks analyzing real-time traffic for detection of misuses [6].

Snort depends on a template-matching scheme and makes content analysis. It has the ability to flag alerts depending on pre-defined misuse rules and saves packets in tcpdump files or in plain text files. Snort is preferred to be used in academic research projects as it is an opensource tool and for this reason we have also chosen Snort as the signature-based intrusion detection system in our work. Anomaly detection based intrusion detection systems are separated into many sub-categories in the literature including statistical methodologies [7–10], data mining [11,12], artificial neural networks [13], genetic algorithms [14] and immune systems [15,16]. Among these sub-categories, statistical methods are the most commonly used ones in order to detect intrusions by analyzing abnormal activities occurring in the network. PHAD [17] and NETAD [18] statistical methods are chosen as the anomaly-based intrusion detection systems in this paper.

PHAD is different than the other conventional network-based anomaly detection systems for two reasons. First, it models protocols rather than user behaviors. Second, it uses a time-based model depending on the rapid change of network statistics in short term. PHAD flags only the first anomaly it detected as an alert even if there is a series of the same anomaly recurring. This feature of PHAD helps reducing the number of false alerts. NETAD, models single packets like PHAD, uses dynamic-conditioned rules like ALAD [19], and rule verification like LERAD [20]. Its greatest contribution is modeling values that are not new. 3.1. Misuse-based IDSs Misuse detectors analyze system activities and try to find a match between these activities and known attacks having definitions or signatures introduced to the system beforehand [1,2,21]. Advantages: Misuse detectors are very efficient in detecting attacks without signaling false alarms (FA). Misuse detectors can quickly detect specially designed intrusion tools and techniques. Misuse detectors provide systems administrators an easy to use tool to monitor their systems even if they are not security experts. Disadvantages: Misuse detectors can only detect attacks known beforehand. For this reason the systems must be updated with newly discovered attack signatures. Misuse detectors are designed to detect attacks that have signatures introduced to the system only. When a well-known attack is changed slightly and a variant of that attack is obtained, the detector is unable to detect this variant of the same attack. Misuse-based IDS used in our hybrid IDS is the open-source project.

Conclusion

Signature-based systems can only detect attacks that are known before whereas anomaly-based systems are able to detect unknown attacks. Anomaly-based IDSs make it possible to detect attacks whose signatures are not included in rule files. PHAD and NETAD are added one by one to signature-based IDS namely Snort as a preprocessor in this study. IDEVAL testbed which was created in MIT Lincoln Laboratories is used to evaluate the performance of new constructed hybrid IDS.

References:

1.James P. Anderson, "Computer security threat monitoring and surveillance," Technical Report 98-17, James P. Anderson Co., Fort Washington, Pennsylvania, USA, April 1980.

2.D. E. Denning, "An intrusion detection model," IEEE Transaction on Software Engineering, SE-13(2), 1987, pp. 222-232.

3.Daniel Barbará, Julia Couto, SushilJajodia, Leonard Popyack and Ningning Wu, "ADAM: Detecting intrusion by data mining," IEEE Workshop on Information Assurance and

Security, West Point, New York, June 5-6, pp. 11-16, 2001.

4.Debra Anderson, Thane Frivold, and Alfonso Valdes, "NIDES Next-generation Intrusion Detection Expert System (NIDES)", A Summary, Computer Science Laboratory, SRI-CSL-95-07, May 1995

5.Te-Shun Chou and Tsung-Nan Chou, "Hybrid Classified Systems for Intrusion Detection," Seventh Annual Communications Networks and Services Research Conference, pp. 286-291, 2009.

6.N.B. Amor, S. Benferhat, and Z. Elouedi, "Naïve Bayes vs. decision trees in intrusion detection systems," Proc. of 2004 ACM Symposium on Applied Computing, 2004, pp. 420-424.

7.Yihua Liao and V. Rao Vimuri, "Using K-nearest Neighbor Classifier for Intrusion Detection," Department Of Computer Scinece, University Of California

8.T. S. Chou, K. K. Yen, and J. Luo, Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms," World Academic of Science, Engineering and Technology, 47, pp. 529-541, 2008.

9.Z. Muda, W. Yassin, M.N. Sulaiman and N.I. Udzir, "A K-Means and Naive Bayes Learning Approach for Better Intrusion Detection," Information Technology Journal, 10, pp. 648-655, 2011.

10.MITlinconin labs, 1999 ACM Conference on Knowledge Discovery and Data Mining (KDD) Cup dataset, http://www.acm.org/sigs/sigkdd/kddcup/index.php? section=1999

11.The KDD Archive. KDD99 cup dataset, 1999. http://kdd.ics.uci.edu/ databases/kddcup99/kddcup99.html

12.M. Tavlle, E. Bagheri, W. Lu, and A. A. Gorbani, "A detailed analysis of the KDD CUP 99 Data Set," Proc. of IEEE Symposium Computational Intelligence for Security and Defense Applications (CISDA'09), pp. 1-6, 2009.

13.Mukkamala S., Janoski G., and Sung A.H., "Intrusion detection using neural networks and support vector machines," In Proc. of the IEEE International Joint Conference on Neural Networks, 2002, pp.1702-1707.

14.J. Zhang and M. Zulkernine, "A Hybrid Network Intrusion Detection Technique Using Random Forests," Proc. of IEEE First International Conference on Availability, Reliability and Security (ARES'06), p. 8, 2006.

15.D. Md. Farid, N. Harbi, S. Ahmmed, Md. Z. Rahman, and C. M. Rahman, "Mining Network Data for Intrusion Detection through Naïve Bayesian with Clustering", World Academy of science, Engineering and Technology, 66, pp. 341-345, 2010.