International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 4 Issue 11 November 2017

A Survey of various Techniques for Intrusion Detection System

Priyanka Pawar[1], Harish Patidar[2]
Research Scholar (Mtech), Department of Computer Science Engineering, Lakshmi Narain College of Technology Indore M.P, India[1]
Head of Department, Department of Computer Science Engineering, Lakshmi Narain College of Technology Indore M.P, India[2]
it.priyankapawar@gmail.com[1], harish.patidar@gmail.com[2]

Abstract: *Intrusion detection is to detect or analyze attacks against a computer system and report to network administrator It is useful in business sector as well as an active area of research. In Information or Network Security, intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resources . It plays a very important role in attack detection, any security violation and network inspect. This paper presents a review of modern classification methods for intrusion detection system. Most of these techniques are based on data classification and clustering. Generally they make use of the decision tree for classification of data. Decision tree is constructed by first calculating the information gain or entropy of each attribute and then splitting the attribute sets.*

Keywords: *IDS, IDS Technique, Attacks types, classification, decision tree.*

1. INTRODUCTION

In present network scenario everyone gets connected to the Internet. It is used in business, education, medical and social networking area. The computer systems and information shared on the network, connected to the internet are under the risk of unauthorized activity or security attacks also called intrusion. Intrusions are threat to integrity, confidentiality and availability of computer resources' [1].

1.1 Intrusion Detection System

Intrusion detection is very important to identify the harmful activity or intruders who break into the system. To protect against a various network attacks and malicious activity, Intrusion Detection Systems (IDS) is used.

An IDS is a device or software application that monitors the system or network for harmful or malicious activities, or any security violation and generates alert or reports to network administrator, where it is analyzed for further prevention and detection. An intrusion detection system simply scans or monitors network traffic and alert the network administrator of any harmful activity. It is very similar to a Bulgur alarm system which will sound an alarm if an intruder attempts to break into a door or a window. For example, if an unauthorized user attempts to gain access to your computer or network, the intrusion detection system will immediately alert the network Administrator of the attempted security breach. Once reported, the Manager can find the exact location of the suspicious activity and follow the proper safety measures.

1.2 Network attacks

There are various types of attacks on the network like DoS, IP Spoofing, Sql injection, cross-site-scripting, phishing, malware, man in the middle attacks etc.

The most common attacks that occur on the network are proposed by Kendall [1], are of following four categories:

1.2.1. Denial of Service (DoS)

A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attack in which the attacker tries to make computer resource inaccessible or too full to respond to its intended users.

Examples of such attacks include Smurf, Teardrop, and Land etc.

1.2.2. Probing

Probing is an attack in which the attacker scans a network of computers to find known vulnerabilities. An attacker who knows which machines and services are available on network can use this information to look for loopholes. There are many

tools available for probe attack. Examples of probing attack are Ipsweep, Saint, Mscan, Nmap, Satan etc.

1.2.3. Remote to User

A Remote to User is an attack in which the attacker tries to gain unauthorized access from a remote machine into user account of the target system. In this type of attack, attacker sends packets to a machine over a network and then exploits some vulnerability to gain local access as a user of that machine. Examples of remote to user attack are Dictionary.

1.2.4. User to root attack

A User to Root is an attack in which the hacker or attacker starts out with access to a normal user account on the system and is able to exploit or abuse some vulnerability to gain root access to the system. Most common attack in this class of attack is buffer overflow attack. Include other attacks, Perl, Ps, Xterm etc.

2. IDS CLASSIFICATION

IDSs are classified based on the monitoring place into two sub-classes, namely network-based IDSs and host-based IDSs, that is, whether they monitor network traffic or a host system log file. IDSs are also categorized into distributed-based IDSs and hybrid-based IDSs depending on the data source. According to the detection approach, IDSs are categorized into: anomaly-detection, misuse-detection, and hybrid-detection.

2.1. Host-based IDS

In Host based intrusion detection (HIDS) individual computer system is monitored for any attack or malicious activity on which the intrusion detection system runs. Such systems make use of information specific to the operating system of the target computer like log files, configurations of system.

2.2. Network-based IDS

Network intrusion detection system (NIDS) monitors network traffic going through particular network devices. NIDS is also called as "packet-sniffers", because it captures and collects the data in the form of internet packets passing through communication medium. Traffic monitoring is done at firewall, switch and

Hub etc [2]. They are most commonly deployed on strategic point in network infrastructure such as at a networks boundary, virtual private network servers, remote access servers, and wireless networks [15].

3. IDS ANALYSIS/DETECTION TECHNIQUES

According to the detection or analysis approach, IDSs are categorized into three subcategories: anomaly-detection, misuse-detection, and hybrid-detection techniques.

3.1 Anomaly detection

Anomaly based IDS constructs the profile of normal network traffic and find any deviance in behavior of the normal traffic to detect attacks .The major problem with existing IDS is efficiency and in this approach, profiles may be established for normal behavior of users. When detection is performed, profile is compared with the actual users' data. If the threshold value is above or greater than the offset, the user's behavior is considered normal, and it is considered that there is no attack. While, if the threshold value is less than the offset, user's behavior is considered abnormal and attack can occur [7]. It defines a baseline of what is normal. Normal behavior of network should be known before its implementation [7].

Advantage: Anomaly detection can detect unknown or new attacks easily, but its false positive is high [6].

3.2 Misuse detection

It is also called signature-based or rule-based detection [10]. In this detection technique the user activities are compared with the attackers' known behaviors. In misuse detection gathered information is analyzed and compared with previously stored databases of attacks [9].

Advantage: Misuse or signature-based detection is useful, because its detection rate is high and false alarm rate is low for known attacks [6].

Disadvantage: The main disadvantage of this system is that it is unable to detect any future or unknown attacks that don't have matched pattern stored in the signature database, detect only previously known attacks.

3.3 Hybrid detection

Misuse-detection based IDSs can detect only known attacks whereas anomaly detection based IDSs detect new or unknown attack. Some Researchers had been combined the anomaly detection approach and the misuse detection approach. 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 proposed by[10].

4. DECISION TREE

Here we discuss some data mining techniques like classification, clustering, association rule mining that is used for detection of intrusion patterns.

4.1Decision tree

Decision tree is a classification technique in data mining for predictive models. Decision tree builds classification or regression models in the form of tree structure where internal node denotes a test on an attribute, branch represents an outcome of the test and leaf node represents a class label. The final result is a tree with decision nodes and leaf nodes. The classic decision tree algorithm named C4.5 was proposed by Quinlan. Majority of the research works in decision trees concerned with the improvement in the performance using optimization techniques such as pruning. Todd et al. [13] Reports a work dealing with understanding student data using data mining Decision tree has various algorithms, some of them Include: ID3 (is introduced in 1986 by Quilan), C4.5 (is introduced in 1993 by Quilan) and C5.0. C4.5 algorithm is developed ID3.

5. RELATED WORK

Venkata et al. [11] as the cost of the data processing and Internet accessibility increases, more and more organizations are becoming vulnerable of cyber threats. Most current offline intrusion detection systems are focused on unsupervised and supervised machine learning approaches. In this system, Information Gain (IG) and Triangle Area based KNN are used for selecting more discriminative features by combining Greedy k- means clustering algorithm and SVM classifier to detect Network attacks. This system achieves high accuracy detection rate and less error rate.

Esh et al. [12] The unsupervised learning techniques using the machine learning for intrusion detection datasets, we know that Clustering is the best techniques on the efficient data mining for intrusion detection. The k-mean clustering algorithm is widely used for intrusion detection, because it gives efficient results.

Deepika et al. [13] Intrusion detection is an active area of research in a current scenario. In their work the object is to affect a method for intrusion detection using KNN classification and Dempster theory of evidence.

Prabhu et al. [14]. The proposed system is based on the adaboost algorithm with Naive Bayes classifier to detect network intrusions with high detection rates and low false-alarm rates. This results in low computational complexity and error rates.

Nagarajan et al. [15] IDS which are increasingly a key part of system defense are used to identify abnormal activities in a computer system. In general, the traditional intrusion detection relies on the extensive knowledge of security experts, in particular, on their familiarity with the computer system to be protected. To reduce this dependence, various data-mining and machine learning techniques have been used in the literature.

Nasser et al. [16] the rapid growth of Internet malicious activities has become a major concern to network forensics and security community. With the increasing use of IT technologies for managing information there is a need for stronger intrusion detection mechanisms. Critical mission systems and applications require mechanisms able to detect any unauthorized activities.

Debdutta et al. [17] in multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. A particularly devastating attack is the wormhole attack, where a malicious node records control traffic at one location and tunnels it to another compromised node, possibly far away, which replays it locally.

Dianbo et al. [18] Neural Networks approach is an advanced methodology used for intrusion detection. As a type of Neural Network, Self-organizing Maps (SOM) is getting more attention in the field of intrusion detection.

Hazem et al. [19] E-government is an important issue which integrates existing local area networks into a global network that provide many services to the nation citizens This network requires a strong security infrastructure to guarantee the confidentiality of national data and the availability of government services.

Todd Heberlein [20] proposed an intrusion detection system called network system monitor. This system is based on the concept of analyzing network instead of the system log entry.

Teng, Chen, And Lu [21], proposed time based inductive machine to capture or store user behavior. Inductive generalization is also a part of the process.

Anderson D, Lunt TF, Javitz H, Tamaru A, Valdes [22], proposed a network intrusion detection expert system. This system learns from the training data and predicts the test data.

Lee W. and Stolfo S. and Mok [23] propose a novel data mining based framework for intrusion detection. This model is based on the concept of the utilizing the contents of the audited programs.

Debar, H., Dacier, M., And Wespi [24] proposes taxonomy of the intrusion detection systems. This classification is done according to the property of the intrusion detection system.

6. CONCLUSION

Intrusion detection systems (IDSs) play an important role in computer security. IDS users relying on the IDS to protect their computers and networks, demand that an IDS provides reliable and continuous detection service. However, many of the today's anomaly detection methods generate high false positives and negatives. This paper presented a systematic survey of recent techniques for the intrusion detection system data classification. This paper also elaborated the concept of intrusion detection system. It is found that although there are many existing methods for classification of IDS data but still there is scope to improve the accuracy of classifier by using different similarity measures. Also there is scope to reduce time and space consumption by using some modern day data structures.

REFERENCES

[1] K. Kendall, "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, "Massachusetts Institute of Technology Master's Thesis, 1998.
[2] Pieter de Boer & Martin Pels, "Host-based Intrusion Detection Systems", Revision 1.10, pp.19-20– February 4, 2005
[3] K. Asif, Talha A. Khan, Sufyan Yakoob, "Network Intrusion Detection and Its Strategic Importance", IEEE Beiac, P.P 978-1-4673, September 2013.
[4] Mukherjee, Biswanath L, Heberlein T, Levitt KN.Network Intrusion detection system .IEEE Network8 (3):26-41:1994
[5] R. A. Kemmerer and G.Vigna, "Intrusion detection: a brief history and overview," Computer, vol. 35, no.4pp. 27-30, 2002.
[6] Alireza Osareh, Bita Shadgar (Computer Science Department, Faculty of Engineering, Shahid Chamran University, Ahvaz, Iran),"Intrusion Detection in Computer. Networks based on Machine Learning Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11, November 2008.
[7] Asmaa Shaker Ashoor, Prof. Sharad Gore," Importance of Intrusion Detection System (IDS)", International Journal of Scientific & Engineering Research, Vol. 2, Issue 1 Jan 2011.
[8] https://en.wikipedia.org/wiki/Intrusion_detection_system.
[9] Vangie Beal," Intrusion Detection (IDS) and Prevention (IPS) Systems", posted 2005 [07-15-2005], last updated 2010[08-31-2010].
[10] Aydın M. A., Zaim A. H., Ceylan K. G., A hybrid intrusion detection system design for computer network security, Computers and Electrical Engineering. 35,517-526, 2009.
[11] Venkata SuneethaTakkellapati,G.V.S.N.R.V Prasad," "Network Intrusion Detection system based on Feature Selection and Triangle area Support Vector Machine", International Journal of Engineering Trends and Technology-Volume3, Issue 4, 2012.
[12] Esh Narayan, Pankaj Singh and Gaurav Kumar Tak, "Intrusion Detection System Using Fuzzy C-Means Clustering with Unsupervised Learning via EM Algorithms" VSRD-IJCSIT, Vol. 2 (6), 502-510, 2012.
[13] Deepika Dave, Prof. Vineet Richhariya, "Intrusion detection with KNN classification and DS- theory", IRACST Vol. 2, No.2, April 2012.
[14] P.S. Prabhu, "Network Intrusion Detection Using Enhanced Adaboost Algorithm", International Journal of Communications and Engineering Volume 3, No.3, and Issue: 02 March 2012.
[15] R.Shanmugavadivu, Dr.N.Nagarajan,"NetworkIntrusion Detection System Using Fuzzy Logic" IJCSE Vol. 2 No. 1, 2011.
[16] Nasser S. Abouzakhar And Abu Bakar, "A Chi-Square Testing-Based Intrusion Detection Model",CFET, 2010.
[17] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks", IJNSA, Vol 1, No 1, April 2009.
[18] Dianbo Jiang, Yahui Yang, Min Xia, "Research on Intrusion Detection Based on an Improved SOM Neural Network", IEEE 2009.
[19] Hazem M. El-Bakry, Nikos Mastorakis, "A Real-Time Intrusion Detection Algorithm for Network Security", Wseas Transactions on Communications Issue12, Volume 7, December 2008
[20] Todd, H. L., Gihan V.D., Karl N.L., Biswanath, M., Jeff, W. and David, W. "A network security monitor," in Proceedings of Symposium on Research in Security and Privacy, Oakland, CA, pp. 296–304, 1990.
[21] A.Teng, H., Chen, K. and Lu, S. "Adaptive real time anomaly detection using inductively generated sequential patterns', IEEE Computer Society Symposium on Research in Security and Privacy, California, IEEE Computer Society, pp. 278-84, 1990.
[22] A.Anderson, J.B. and Mohan, S. "Sequential coding algorithms: A survey and cost analysis", IEEE Transactions on Communication, Vol.32, pp. 169-176, 1984.
[23] A.Lee, W., Stolfo, S. and Mok, K. "Adaptive intrusion detection: A data mining approach", Artificial Intelligence Review, Kluwer Academic Publishers, Vol. 14, No.6, pp. 533-S567, 2000.
[24] A. Debar, H., Becker, M. and Siboni, D. "A neural network component for an intrusion detection system," in IEEE Symposium on Research in Computer Security and Privacy, pp. 240-250, 1992.