Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Recent Trends in Security Techniques for Detecting Suspicious Activities in Computer Network: A Survey

Shashikant Sharma *
M.Tech Scholar,
Department of Computer Science,
RIET, Bhankrota, Jaipur,
Rajasthan, India

Pramendra Kumar
M.Tech Scholar,
Department of Computer Science,
RIET, Bhankrota, Jaipur,
Rajasthan, India

Sachin Sharma
Asst. Prof.,
Department of Computer Science,
RIET, Bhankrota, Jaipur,
Rajasthan, India

Abstract— Over the past few decades the network based system has grown at an explosive rate with innovations in communication and information technologies. While the computer network and their related applications brought the world together by bridging the information gap among people, it has also made it easier to leads unauthorized activity not only from external attackers but also from internal attackers, such as disgruntled employees and people abusing their privileges for personal gain. The precious information is always prone to maximum attacks over the network. Intrusion may occur due to system vulnerabilities or security breaches, such as system misconfiguration, user misuse or program defects. Attackers can also combine multiple security vulnerabilities into an intelligent intrusion. Therefore an efficient intrusion detection model is needed to defence the network system. However, in this context a number of researchers have proposed their different approaches but each of them faces their own limitation, most of the common problem is that they are unable to detect the emerging attacks. In this paper we investigate the recent trends of security techniques for the task of detecting intrusion in network, which may help to the researchers to understand and builds an enhanced technique for network intrusion detection

Keywords— Security, Attacks, NIDS, HIDS

I. INTRODUCTION

Over past few decades, the trends of network based system and its applications in daily life have increases the difficulties in attacks detection at real time. The precious information is always prone to maximum attacks over the network that raised the need of computer security systems. The three most important aspects of security are confidentiality, integrity, and availability. Confidentiality implies that only authorized entities can access and modify information and resources, while unauthorized entities are denied access. Integrity means that the information being accessed is consistent, accurate and can be changed only through authorized actions. Availability for data and services implies that legitimate users should have fair and timely access, the services should be usable and the capacity provided should meet needs. Ensuring that these three aspects are provided for is the primary challenge facing security professionals today.

However, building a complete secure computer system is still a vision. This is due to the fact that, application programs will always contain unknown bugs and vulnerabilities. In addition, attackers continuously find new techniques to exploit vulnerabilities in the computer systems [1, 2]. Hence, despite the security precautions, computer attacks are continuously increasing. Intrusion detection is the technique of determining that an attempt has been made at compromising the resource, or worse the resource has been compromised. One point that needs to be made clear is that, intrusion detection systems (IDSs) do not detect intrusions; they detect evidence or manifestations of intrusions, either while the intrusion is in progress or after an intrusion has occurred. Typically, for the security of a computer system or network the implementation of an Intrusion detection system is the last mechanism. Firewalls and security policies are the first defence lines in order to protect and prevent attackers to harm computer systems or network. Attacker can be an outsider who attempts to access the system, or an insider who attempts to gain and misuse non-authorized privileges. This paper presents an investigation of recent trends of security techniques for the task of detecting intrusion in network, which may help to the researchers to understand and builds an enhanced technique for network intrusion detection.

II. TAXONOMY OF INTRUSIONS & INTRUSION DETECTION SYSTEM

An intrusion is a set of actions that try to compromise the honesty, privacy, or accessibility of a source [3]. An attack generally falls into one of four categories [4]:

1. **Denial of Service (Dos) Attacks:** these types of attacks attempts to prevent legitimate users from accessing information or services. The most common DoS attacks will target the computer's network bandwidth or connectivity.
2. **Probe Attacks:** It is an attack in which attacker scans and determines the weaknesses or the vulnerabilities in machine or network device that could be later useful for attacker.
3. **Remote to Local (R2L) Attacks:** Attackers does not have an account on the victim machine, hence tries to gain access from a remote machine and exploits this access in order to send packets over the network.

4. **User to Root (U2R) Attacks:** The User to Root (U2R) attack enables the attacker to access root privileges by unauthorized way.

For detecting an intrusions there are two techniques: Anomaly detection and Misuse detection. **Misuse** detection technique attempts to find those attacks that patterns and signatures are already known as attacks in the network traffic. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection". Today most of the commercial and research intrusion detection tools are based on attack signatures. **Anomaly** technique is different from misuse detection in contrast to the advantage of being able to detect novel attacks but might suffer higher false positive rates. It typically involves the creation of knowledge bases that contain the profiles of the monitored activities. Anomaly detection uses data mining techniques to classify an attack. However, unlike misuse detection where the learning algorithm is trained over labelled data, anomaly detection builds the models from the normal data. Once a threat has been identified, this technology allows operators to visualize good and bad or suspicious traffic, and contextualize it in relation to other traffic and historical roles.
Typically the IDSs can be classified into two categories, host-based IDSs and network-based IDSs.

A. Network-based Intrusion Detection System:

A "network intrusion detection system (NIDS)" monitors attack or unauthorized activity on a network. They are also called packet-sniffers. They generally have a signature database against which they compare network packets. These systems have been incapable of operating in switched environments, encrypted networks and high-speed networks. An NIDS needs dedicated hardware, and forms a system which can check packets travelling on one or more network lines, in order to find out if any malicious or abnormal activity has taken place.

B. Host-based Intrusion Detection System

Host-based intrusion detection systems monitor activity on a host. They are best suited for internal threats because of their ability to monitor and react to specific user actions and file accesses on the host. They offer audit policy management centralization, supply forensics, statistical analysis, and evidentiary support.

C. Hybrid Intrusion Detection System

Hybrid intrusion detection systems manage both network-based and host-based systems. They are kind of a central intrusion detection system and add a logical layer to NID and HID.

On the response basis IDSs can further classified in two types: (i) Active IDS and (ii) Passive IDS. **Active Intrusion Detection Systems (IDS)** is also known as Intrusion Detection and Prevention System (IDPS). It is configured to automatically block suspected attacks without any intervention required by an operator. Intrusion Detection and Prevention System (IDPS) has the advantage of providing real-time corrective action in response to an attack. **Passive IDS** only alert the operator against attacks and potential vulnerabilities. The operator of the system takes responsive action on the base of information. A passive IDS is not capable of performing any protective or corrective functions on its own. The major advantages of passive IDSs are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

III. RELATED WORK

Since the born of intrusion detection system a number of approaches has been developed in direction to detect the network attacks. A Distributed Intrusion Detection Framework based on Autonomous and Mobile agent has been proposed by [5]. The proposed framework uses five different agents to perform the detection task. To improve the false positive rate, cost and computational time a efficient data mining algorithm has been proposed in [6]. The proposed approach performs better when applied to KDD'99 data sets. On the base of packet observation a network-based buffer overflow attack detection system called Nebula has been presented in [7]. The proposed approach built on a centralized TCP/IP architecture and incorporates a payload type identification mechanism that reduces the false positive rate. In same context a novel misuse based approach has been proposed in [8] to monitor the packets on network and informs the administrator for evasive action. [9] Presents a technique for enhanced self-Adaptive Naive Bayesian Tree (NBTree) which is used for anomalous based intrusion detection. Author has presented a new learning algorithm for Naive Bayesian Tree by which the performance of Naive Bayesian Tree (NBTree) has been enhanced and the detection has been scales up for different types of known attacks, it has also recorded a decrease in the rate of false positive alarm. A new learning algorithm for adaptive network intrusion detection using naive Bayesian classifier and decision tree have been presented in [10]. According to the author the proposed approach balance the detections and keeps false positives at acceptable level for different types of network attacks, eliminates redundant attributes as well as contradictory examples from training data that make the detection model complex. The proposed algorithm also addresses some difficulties of data mining such as handling continuous attribute, dealing with missing attribute values, and reducing noise in training data.

A new learning algorithm for adaptive intrusion detection using boosting and naïve Bayesian classifier has been presented in [11]. The approach considers a series of classifiers and combines the votes of each individual classifier for classifying an unknown or known example. According to the author, algorithm generates the probability set for each round using naïve Bayesian classifier and updates the weights of training examples based on the misclassification error

rate that produced by the training examples in each round. This algorithm addresses the problem of classifying the large intrusion detection dataset, which improves the detection rates (DR) and reduces the false positives (FP) at acceptable level in intrusion detection. In same context a novel approach has been proposed in [12] for detecting the network attack. The proposed approach detects the network attacks in unsupervised way without following the traditional way of signatures or labeled traffic. An investigation [13] presents some of the best well known Intrusion detection techniques and challenging number of attacks including unknown attacks. The paper has presents some of appropriate techniques which are proposed for intrusion detection and anomaly detection. An Adaboost algorithm for network intrusion detection system with combination of multiple weak classifiers has been proposed in [14]. The classifiers such as Bayes Net, Naıve Bayes and Decision Tree used as weak classifiers. A benchmark dataset used to demonstrate that boosting algorithm can greatly improve the classification accuracy of weak classification algorithms. According to the author the proposed approach achieves higher detection rate with low false alarm rates and is scalable for large datasets, resulting in an effective intrusion detection system.

To reduce the average control path latency incurred between request and response of the system as well as the increasing the detection rate of network attack groups a approach has been proposed in [15]. The projected approach categorizes the network attacks in to four groups and use independent feature set to achieve the efficiency and accuracy in detecting the network attack groups. In same context an alternative technique, which based on a combination of time series and feature spaces, for using machine learning algorithms to automatically detect anomalies in real time has been proposed in [16]. According to the author the proposed technique can work well for a real network environment, and it is a feasible technique with flexible capabilities to be applied for real-time anomaly detection. To enhance the detection rate of attack in adhoc network a novel approach has been proposed in [17]. The approach has used the Supervised Learning in Quest (SLIQ), a fast scalable classifier for detecting intrusion. In same context to enhance the detection rate of attacks a novel Fuzzy Genetic Algorithm has been proposed in [18]. The proposed approach have use supervised learning algorithm, to classify attacks in the datasets.

A hybrid detection system has been proposed in [19] by combining the Naïve Bayesian (NB) and Support Vector Machine (SVM). The Naïve Bayesian (NB) and Support Vector Machine (SVM) has been combined to maximize the accuracy, which is the advantage of NB and diminish the wrong alarm rate which is the advantage of SVM. A genetic algorithm (GA) based approach has been proposed in [20] to solve a problem of network intrusion. The GA resolve on the KDD trophy 99 facts set to construct a imperative set that preserve to recognize attacks scheduled on the system. The [21] presents the detailed investigation on learning techniques for Intrusion detection system (IDS). The survey pointed out some issues of existing intrusion detection system like: low detection rate, detailed classification of attack, large training time required to train the network

IV. ISSUES IN CURRENT IDS

However a lot of approaches have proposed by number of researchers for efficient intrusion detection system but each of them have its own limitations. One most common problem with the current attack detection system is that they are usually tuned to detect known service- level network attacks and are unable to detect every kind of attacks. This leaves them vulnerable to original and novel malicious attacks. On the other hand the current IDS approach generates false positive alarm which needs to be decreased. A false positive Occurs when normal attack is mistakenly classified as malicious and treated accordingly. Apart from these the IDS uses additional resource in the system even when there is no intrusion detecting because IDS has to be run all the time.

V. CONCLUSION

In this paper we have present the some basics of the Intrusion Detection System with the recent trends of security techniques. Furthermore, some issues with the current IDS are also pointed out in this paper, which may help to newcomers in the field of intrusion detection system and is useful for people looking for a quick review of recent development in this field.

REFERENCES

[1] Kapil Kumar Gupta, Baikunth Nath, Kotagiri Ramamohanarao, and Ashraf Kazi. Attacking Confidentiality: An Agent Based Approach. In Proceedings of IEEE International Conference on Intelligence and Security Informatics, pages 285–296. Lecture Notes in Computer Science, Springer Verlag, Vol (3975), 2006.

[2] Overview of Attack Trends,2002. http://www. cert.org/archive/pdf/attack_trends.pdf.

[3] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isacoff and E. Spafford, D. Zamboni. An architecture for intrusion detection using autonomous agents. In Proceedings of the Annual Computer Security Applications Conference, IEEE Computer Society, pages 13-24, Scottsdale, Arizona, December 1998.

[4] Mohammad Sazzadul Hoque, Md. Abdul Mukit, and M. A. N. Bikas, "An implementation of intrusion detection system using genetic algorithm," International Journal of Network Security & Its Applications (IJNSA), vol. 4, (2012).

[5] Boughaci, D. Drias, H. Bendib, A. Bouznit, Y.Benhamou, “Distributed Intrusion Detection Framework based on Autonomous and Mobile Agents”. International Conference on Dependability of Computer Systems, pp 248 – 255. 2006.

[6] Mrutyunjaya Panda and Manas Ranjan Patra, “Network Intrusion Detection using Naive Bayes”, International Journal of Computer Science and Network Security, Vol.7 No.12, pp 258-263, 2007

[7] FuHau Hsu, Fanglu Guo, Tzicker Chiueh, "Scalable Network based Buffer Overflow Attack Detection", Proceedings of ACM/IEEE symposium on Architecture for Networking and Communications Systems, 2006.

[8] Meera Gandhi and S.K.Srivatsa, "Detecting and preventing attacks using network intrusion detection systems", International Journal of Computer Science and Security, Vol.2 No.1, 2008.

[9] D. Md Farid, N.HuuHoa, J.Darmont, N.Harbi, and M. ZahidurRa hman, "Scaling up Detection R ates and Reducing False Positives in Intrusion Detection us sing NBTree", In Proc. of the International Conference on Data Mining and Knowledge Engineering (ICDMKE 2010) page 186- 190,April 2010.

[10] Dewan Md. Farid, Nouria Harbi, and Mohammad Zahidur Rahman "Combining Naive Bayes And Decision Tree For Adaptive Intrusion Detection" International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010.

[11] Dewan Md. Farid, Mohammad Zahidur Rahman, Chowdhury Mofizur Rahman "Adaptive Intrusion Detection based on Boosting and Naïve Bayesian Classifier" International Journal of Computer Applications (0975 – 8887) Volume 24– No.3, June 2011

[12] Pragati H. Chandankhede, Sonali U. Nimbhorkar "Autonomous Network Security using Unsupervised Detection of Network Attacks" Pragati H. Chandankhede et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (1) , 2012, 2992 – 2995

[13] FaseeUllah1, Waqas Tariq, Dr. Muhammad Arshad, Muhammad Saqib, Noor Gul "Analysis of Security Techniques for Detecting Suspicious Activities and Intrusion Detection in Network Traffic" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012, ISSN (Online): 1694-0814

[14] P. Natesan, P. Balasubramanie , G. Gowrison "Improving Attack Detection Rate in Network Intrusion Detection Using Adaboost Algorithm with Multiple Weak Classifiers" Journal of Information & Computational Science 9: 8 (2012) 2239–2251

[15] Prof.S.S.Manivannan, Dr.E.Sathiyamoorthy "Detection System to detect the Network Attack Groups using the Layer wise Individual Feature Set" International Journal of Engineering and Technology (IJET), Vol 5 No 4 Aug-Sep 2013

[16] Kriangkrai Limthong "Real-Time Computer Network Anomaly Detection Using Machine Learning Techniques" Journal of Advances in Computer Networks, Vol. 1, No. 1, March 2013.

[17] P.Sreenivasul, K.RameshReddy " A Scalable Classifier for Intrusion Detection in Adhoc Networks" International Journal of Advanced Engineering and Global Technology Vol-2, Issue-4, April 2014

[18] Miss. M. R. Yadav, Prof. P. B. Kumbharkar " Intrusion Detection System with Supervised Learning Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014

[19] Amit D. Sagale, 2 Swati G. Kale "Combining Naive Bayesian and Support Vector Machine for Intrusion Detection System" IJCAT International Journal of Computing and Technology, Volume 1, Issue 3, April 2014

[20] Sunil Kumar, Surjeet Dalal "Optimizing Intrusion Detection System using Genetic Algorithm" International Journal of Research Aspects of Engineering and Management ISSN: 2348-6627, Vol. 1, Issue 1, FEB 2014, pp. 42-45

[21] Roshani Gaidhane, Student, Prof. C. Vaidya, Dr. M. Raghuwanshi "Survey: Learning Techniques for Intrusion Detection System (IDS)" International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 2, Feb 2014. ISSN 2348 - 4853

