ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

Survey on Network Intrusion Detection System (NIDS)

Sagar Dhende [1], Dr. R.B. Ingle [2]

P.G. Student, Department of Computer Engineering, PICT Pune, SPPU, Pune, India[1]

Professor, Department of Computer Engineering, PICT Pune, SPPU, Pune, India[2]

ABSTRACT: Intrusion detection system (IDS) is software application which monitors system or network to detect the suspicious activities and abnormal behaviors of users in that network. IDS is classifying in two categories host based intrusion detection system(HIDS) and network based intrusion detection system (NIDS). NIDS monitor the network traffic in the system to detect the various kinds of attacks. NIDS contain two analysis strategy, one is rule based or misuse detection analysis strategy and other is anomaly based intrusion detection analysis strategy. Rule based detection technique unable to detect novel attack because of rules are encoded manually as per the experts knowledge so that if the rule are not encoded for particular attack then the attack can not be detect. In network security anomaly detection analysis strategy is used to detect novels attacks. The machine learning technique will be increase the attacks detection accuracy. This paper present survey of NIDS by applying supervised and unsupervised machine learning methods to find out the anomaly in network

KEYWORDS: System security, Machine learning, User behavior, Intrusion detection

I. INTRODUCTION

In network security the major goal of network intrusion detection system is identify the various kinds of attacts in real time by both system external and insiders penetrators. The network system should be contain data confidentiality and communication intigrity against the denial of service, probing, root to local and user to root attacks.The high growth of internet use in today's life also raise the concern to safe network from various kind of attacks. The network security become a very important than the traditional system. The many security technologies is introduced but the there are various undetected threats are present in the network that disrupt the privacy.

Intrusion Detection System(IDS) :
Intrusion detection system (IDS) is software application which monitors system or network to detect the suspicious activities and abnormal behaviors of users in that network. IDS is classifying in two categories host based intrusion detection system(HIDS) and network based intrusion detection system (NIDS).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

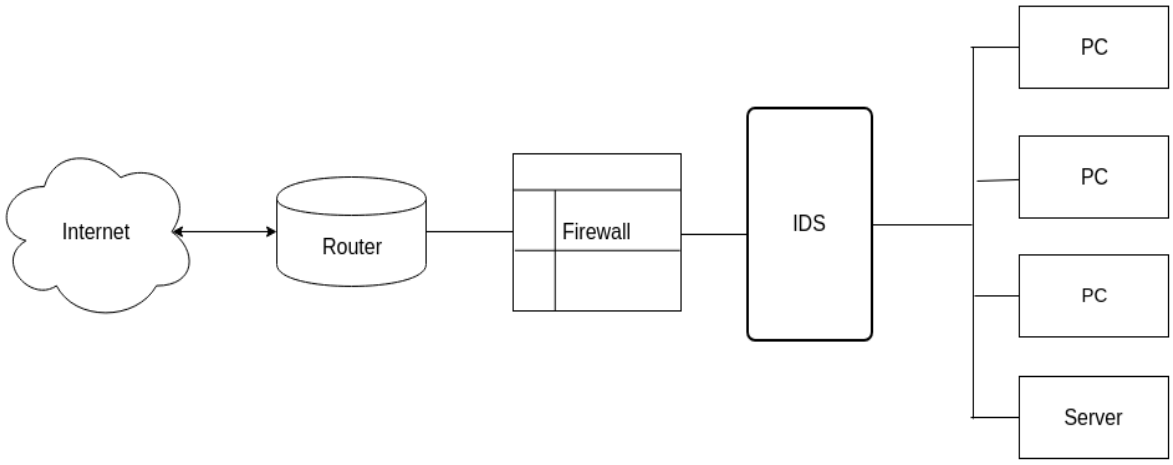

Fig: Intrusion Detection system

The above figure shows the simple overview of intrusion detection system.

1. Host Based Intrusion Detection (HIDS):
Host Based Intrusion Detection System (HIDS) is capable to analyzing and monitoring computer system or network packet on network. It work similar to the network based intrusion detection system but difference in HIDS and NIDS is the HIDS is only install on certain intersection point such as routers , servers while NIDS is install on every host machine.

2. Network Based Intrusion Detection system (NIDS):
Intrusion detection system is monitor the network traffic in the system to detect the various kinds of attacks in network. Network based intrusion detection system contain two techniques one is rule based detection technique and other is anomaly based detection technique.

2.1. Rule Based:
Rule based technique is used to discovers known attacks and it unable to detect unknown attacks in network. In the rule based technique traffic of network is very huge so that the process of the manually encoded rules is very slow and expensive. Cyber security professionals and experts are needed to change or modify the rules manually by using the rule driven languages

2.2 Anomaly Based:
Anomaly detection technique is used to detect the known and unknown attacks while to overcome limitations of rule based technique, anomaly based detection technique is used. Anomaly based detection technique play very important role to detct unknown attacks. The anomaly detection accuracy can be increses by using the machine learning technique.

Machine Learning:
Machine learning is a subtype of artificial intelligence in the computer science area that are used statistical technique to assign computers ability to learn with data. Machine learning classified into two broad categories,
1. Supervised learning
2. Unsupervised learning

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

II. SUPERVISED LEARNING FOR INTRUSION DETECTION

Supervised learning method is also called classification method which required the dataset that contain the labeled data containing the both normal and intrusion samples to construct the NIDS predictive model. Basically the supervised learning method gives the better detection accuracy than the semi supervised learning method and unsupervised method. There are various kind of supervised algorithm can be use to detect attacks in networks such as support vector machine(SVM), supervised neural network, bayesian networks, k-Nearest neighbors, and decision tree.

1. **Support Vector Machine(SVM):**
Support vector machine is the supervised learning that can analyze or perform pattern recognition and regression analysis task. Support vector machine is widely used for multi class classification by finding hyper-plane of training data set. The multi class support vector machine can be construct the multiple classes at the training time.

2. **Supervised Neural Network(NN):**
The neural network can predict the users abnormal behavior in the system. Neural network with proper implementation have the ability to address various problems which are encountered by the misuse or rule based technique. NNs have the ability to conclude the solution from the dataset without having the prior knowledge of that dataset. The NNs approach can be apply to intrusion detection, the dataset contain the normal and attacks data NNs is used to automatically introduced attacks during the training phase.

3. **Bayesian Network (BN):**
In Bayesian network two type of learning possible one is parameter learning and other is structure learning. The structure learning constructing the structure of the graph which can be gives the dependencies between variables. The parameter learning required an previously already defined structure of the graph. Parameter learning can be find only accurate parameters of the conditional and prior probabilities. Parameter learning is useful if the data is insufficient, it allows to change or modify already presented parameters values.

4**. K-Nearest Neighbor (k-NN):**
K-Nearest neighbors algorithm is supervised learning algorithm can be used for the classification which is mainly based on k-nearest neighbor category. The k-NN calculate the approximately distance between input vectors and gives the unlabeled data point to class of the k-NN. In the use of k-NN classifier let ‘k’ is the very important parameter. For example if the ‘k’ is huge then the neighbors which are used for prediction will be require large classification time and it will also affect the accuracy of prediction.

5. Decision Tree:
Decision tree is the supervised learning classification technique which is basically used for classification and prediction of attacks in network intrusion detection system. The decision tree is nothing but the tree which is contained three important components such as nodes, arcs and leaves. The each node in the decision tree labeled with feature attributes, each arc is labeled with features value. And each leaf is labeled with class or category. The decision tree is starting classification from the root and moving toward until leaf node is reached. C4.5 and ID3 are the implementation of the decision tree.

III. UNSUPERVISED LEARNING FOR INTRUSION DETECTION

Unsupervised intrusion detection technique do not neet of training data. Basically they are based on the two rules or assumptions. First one , they assume most of connections in network are normal traffic and very small amount of traffic is malicious or abnormal. And other assumption is they anticipate that abnormal traffic is statistically different from normal traffic. According to this rule data group of similar instances which seen frquently are supposed to be normal traffic. While infrequently instances assumed maliciou. There are various unsupervised learning algorithms such as K-Means, clustering technique, one-class support vector machine, C-means, unsupervised niche clustering.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

1. **K-Means**:
K-means algorithm is the unsupervised learning algorithm which is traditionally clustering algorithm. K-means algorithm devides the data into k cluster and also keep attention that the data in the cluster has the similar properties. K-means technique firstly select 'K' data random in initial cluster and after that remaining data add to that cluster with similarity according to its distance toward the center of cluster. The K-means algorithm is play very important role in the intrusion detection. K-mean reduce the noise in dthe dataset by dividing clusters.

2. **Clustering Techniques**:
Basically clustering technique work in group of data into clusters, according to similarity there are two approaches of clustering based on the intrusion detection. First approach contained the intrusion detction model trained by using unlabeled data that consist of attack traffic and normal traffic. Second approach contained intrusion detection model trained by using only normal data.

IV. CONCLUSION

Machine learning have become considerable attention in network based intrusion detection to overcome rule based detection technique. The main motive of this survey is increasing the attacks detection accuracy by reducing the false positive rate. This paper proposes a overview of network based intrusion detection system using the various machine learning techniques.

REFERENCES

1. Mohammed a. Ambusaidi, Member, Priyadarsi Nanda and Zhiyun Tan, "Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm", IEEE transactions on computers, vol. 65,no. 10,october 2016.
2. Salima Omar, Asri Ngadi, and Hamid H. Jebur, "Machine Learning techniques for Anomaly detection: An Overview", International Journal of Computer Applications (0975 – 8887) Volume 79 – No.2, October 2013
3. Jiong Zhang, Mohammad Zulkemine, and Anwar Haque, "Random-Forest-Based Network Intrusion Detection System", IEEE Transactions In Systems, Man, and Cybernetics, Part C (Applications and Reviews) (Volume: 38, Issue: 5, Sept. 2008).
4. Fang-Yie Leu, Kun-Lin Tsai, Member, IEEE, Yi-Ting Hsiao, and Chao-Tung Yang, "An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques" , IEEE systems journal, vol. 11, no. 2, june 2017.
5. Kriangkrai Limthong and Thidarat Tawsook, "Network Traffic Anomaly Dtetection using Machine Learning Approach" , IEEE conference nov 2012.
6. Sujata Yeldi, Sweta Gupta, Tanmay Ganacharya, Shirish Doshi, Dhanashree Bahirat, Prof, Rajesh Ingle, Anandamoy Roychowdhary, PICT, "Enhancing Network Intrusion Detection System with Honeypot", TENCON 2003. Conference on Convergent Technologies for the Asia-Pacific Region.
7. Juliette Dromard, Gilles Roudière, and Philippe Owezarski, "Online and Scalable Unsupervised Network Anomaly Detection Method", IEEE transactions on net work and service management, vol. 14, no. 1, march 2017.
8. Shuai Zhao, Mayanka Chandrashekhar, Yugyung Lee, Deep Medhi, "Real-Time Network Anomaly detection System using Machine Learning", IEEE International Conference june 2015.
9. Nguyen Thanh Van,Tran Ngoc Thinh, Le Thanh Sach, "An anomaly-based Network Intrusion Detection System using Deep learning", IEEE International Conference 2017.
10. Nabila Farnaaz and M.A.Jabbar, "Random Forest Modeling for Network Intrusion Detection System", Nabila Farnaaz and M.A. Jabbar / Procedia Computer Science 89 (2016) 213 – 217.
11. Ramana Rao Kompella, Student Member, IEEE, Sumeet Singh, and George Varghese, Member, IEEE, "On Scalable Attack Detection in the Network", IEEE/acm transactions feb 2007.
12. Chee-Wooi Ten, Member, IEEE, Junho Hong, Student Member, IEEE, and Chen-Ching Liu, Fellow, IEEE, "Anomaly Detection for Cybersecurity of the Substations", ieee transactions on smart grid, vol. 2, no. 4, december 2011.
13. Praneeth NSKH, Naveen Varma M, Roshan Ramakrishna Naik, "Principle Component Analysis based Intrusion Detection System Using Support Vector Machine", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.
14. Sumaiya Thaseen and Ch.Aswani Kumar, "Intrusion Detection Model Using fusion of PCA and optimized SVM" 2014 International Conference on Contemporary Computing and Informatics (IC3I), 978-1-4799-6629-5/14
15. Sara Pourfallah, Amir H. Jafari et.al, "an intrusion detection algorithm for ami systems based on svm and pca", International Journal on Cybernetics & Informatics (IJCI)},Vol. 3, No. 4, August 2014.
16. Soukaena Hassan Hashem, "efficiency of svm and pca to enhance intrusion detection system." in \textit{Journal of Asian Scientific Research,} 2013, 3(4):381-395.
17. Gabriel Y. Keung, Member, IEEE, Bo Li, Fellow, IEEE, and Qian Zhang, Fellow, IEEE, "The Intrusion Detection in Mobile Sensor Network",IEEE/ACM transactions on networking, vol. 20, no. 4, august 2012.