International Journal of Scientific Engineering and Technology ISSN : 2277-1581
Volume No. 6, Issue No. 7, PP : 216-219 1 July 2017

Classification and Analysis of Techniques Applied in Intrusion Detection Systems

Calpephore NKIKABAHIZI, Dr Wilson Cheruiyot, Dr Ann Kibe
Department of Information Technology, Jomo Kenyatta University of Agriculture and Technology (JKUAT)
Corresponding Email : traorebrahiman@yahoo.fr

Abstract- Currently, the development of most of organizations depends on technology for mining information, storing and its transactions. But these frequent use online technologies make the data to be exposed to the risk of attacks that compromise the normal activities of systems. To protect and prevent these attacks, the researchers had implemented the intrusion detection systems (IDS). Even the IDS are so many, the attacks still also increasing in different forms. This paper reviews most techniques usable in IDS, to help users and security professionals to take robust measures in identifying the strength and weakness of each technique. The result of this study shows that majority of techniques perform well at rate more than 99%.

Key words: Data mining, IDS, normalization

Introduction

All Organizations in worldwide make decision based on information in all its levels. Therefore, information management concentrates on mining knowledge useful in developing the organization and its security in all level from data layer through analytical access layer to the medium. This information is vital for organizations and comes from diverse sources, and use online channel to be shared. Due to this online profiling, the digital data over the networks have increased marginally (Bilal, 2014).

Today, the information security is one of the serious problems across a variety of industries, due to malicious activities of threats that attack the system to steal the information or causing the incidental damage. The mechanism of security is very important to detect the intrusive behavior (Sandu et al. 2011).

In order to effectively monitor malicious activities, it is very crucial to use information detection system (IDS) to monitor network traffic and its suspicious behavior against security. The IDS uses different techniques to detect and to prevent intruders. This paper makes a survey on techniques used for IDS detection and prevention.

1. Related Works

This section describes some important works related to the survey on techniques used in intrusion detection and prevention.

Beigh (2014) proposed a new classification scheme for intrusion detection system and related techniques used to prevent or detect the malicious activities .This classification helps users or security professionals to know what and how to do in their daily work of securing the developed systems.

Sundus et al. (2015) examined different machine learning techniques that have been proposed for detection intrusion by focusing on hybrid classifier algorithm, and this paper strengthens the readers, users and personnel in charge of security to be ready on hybrid techniques to find a relevant solution of different attacks.

Sandhu et al. (2011) made a survey on intrusion detection and prevention .Their work set out the advantage and disadvantages on each technique based on position of deployment of systems.

Deka et al. (2015) presented a comprehensive survey of methods and systems introduced by other researches done before to protect network resources from intrusion, and listed issues and research challenges.

Vijayarani and Sylvia (2015) provided a complete study on IDS methods, life cycle, types of attacks, different tools and techniques, research needs, challenges and the applications.

2. Classification and Techniques for Intrusion Detection

IDS are an essential parts of the security infrastructure.They are used to detect, identify, alert and stop intruders. Different authors used techniques according to the issues being solved, or prevented. According to Beigh (2014), the classification of IDS depends on anomaly based detection, misuse based IDS, composite, design based, and time aspect based IDS, monitoring, architecture based and position of deployment. Sandu et al. (2011) explained two types of IDS, anomaly detection technique that stores the systems normal behavior such as Kernel information, system log event, network packet information, software running information, operating systems, information into database. An alarm is generated when abnormal behavior occurs in a system which deviates from a system normal behavior, this results either false positive or false negative. The second technique is signature detection or misuse detection scheme that stores the sequence of pattern, signature of attacks or intrusion into the database. Once the system matches the signature of intrusion with the predefined signature that already stored in database, it generates a successive alarm.

Hoque ,Mukit and Bikas (2012) classified intrusion detection into two main categories, Host Based Intrusion Detection (HIDS) that evaluates information found on a single or multiple host systems ,including content of OS, system and application files, and Network Based Intrusion Detection (NIDS) that

evaluates information captured from network communication. They also explained the three functional components of IDS, the event generator or data source, analysis engine that takes information from data source and examines the data for symptoms of attacks or policy violation .The analysis engine use either or both misuse/signature based detection and anomaly /statistical detection.

Many techniques have been used to prevent or detect the anomalies, others for misuses. For anomalies detection, we use biological inspired methods: Evolution (Mbikayi, 2012) and artificial immune system (Hosseinpour et al., 2014). Data mining techniques includes K-nearest neighbor (Patel & Panchal, 2015), decision tree (Shikha & Simmi, 2016), neural networks (Vinchurkar & Reshamwala, 2012), support vector machine (Tesfahu & Bhaskari, 2015), and hybrid technique (Somani & Dubey 2014).Machine learning techniques such as Bayesian network (Vinchurkar & Reshamwala,2012),Generic algorithm (Hoque , Mukit and Bikas ,2012); (Parati & Potteti ,2015), Fuzzy logic(Sawant & Itkar, 2016), artificial neural networks (Panigrahi & Patra,2015), and layered approach (Tesfahu & Bhaskari, 2015); hybrid techniques (Sundus et al.,2015); (Solanki & Dhamdhere, 2014), and cognition based techniques (Sunilkumar et al., 2012). These techniques are more used in self learning systems (Beigh, 2014).

In programmed system, the more used techniques are statistical based techniques: Markov process (Sundarraj, 2014); (Brindascri & Saravanan, 2014), multivariate (Balapure & Shedge, 2015), and time series modeling (Abdullah et al., 2014). Other techniques are state series modeling, simple rule (Bansal & Singh, 2015), and default deny according to the system legal and threshold technique that consists on counting the number of frequency of a specific event type over an interval time (Beigh, 2014).

Misuse/signature based detection use state modeling techniques, expert systems , string matching techniques (Patel,2014), and simple rule based technique (Bansal & Singh,2015) and checksum methods.

3. Methodology And Materials

The data has been treated using computer Dell, intercore i5,RAM. The weka tool ,version 3.8.0 has been used to analyze the results. In this paper , the researcher also used data acquired from KDD 99 dataset which has network features of 4,9 millions of connection records include 22 classes of attacks grouped into four main classes of attacks ,Deny of Services (DOS), Probe, User to Root (U2R) and Remote to local (R2L).

No	Classes	Total records
1	Normal	972,780
2	DOS	3,883,370
3	probe	41,102
4	U2R	52
5	R2L	1,126

Table 1: Population

The goal of this paper is evaluate the performance of classification techniques used in IDS, and Pre- processing stage consisted of two steps: The first step involved the mapping symbolic - valued attributes to numeric - valued, scaling, attributes and the implemented non-zero numerical features, or size reduction and second step was normalization of features using Minimum maximum normalization,

$$n_v = f_2(v) = \frac{v - \min(v)}{\max(v) - \min(v)}$$

After normalization ,the research removed duplicate data, and then generated 5 labeled dataset (5 labels (normal , probe, dos, u2r, r2l,), and a Sample Size (S.S) of sample 57,279 has been selected and instances with 41 condition attributes and one class attribute has been taken in consideration .

To evaluate the performance of each technique, the metrics for analysis was used such as the accuracy and Receiver Operating Characteristic (ROC) curve. The comparison consists on their true positive rate

Table 2: Selected Sample Size

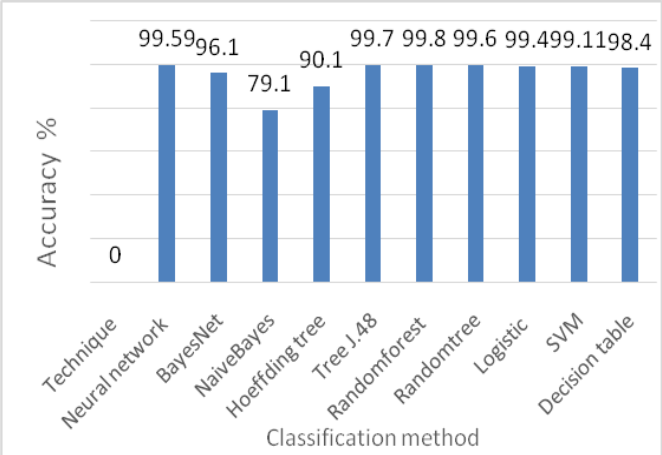
Class(C)	Subclass (S)	Number of S.S.S	Number of S.S.C
Normal	Normal	9,728	9,728
DOS	Smurf	28,079	42,266
	Neptune	10,720	
	Back	2,203	
	Teardrop	979	
	Pod	264	
	Land	21	
Probe	Satan	1,589	4,107
	Ipsweep	1,247	
	Portsweep	1,040	
	Nmap	231	
U2R	Warezclient	1,020	1,126
	Guess_passwd	53	
	Warezmaster	20	
	Imap	12	
	Ftp_write	8	
	Multihop	7	
	Spy	2	
	Phf	4	
R2L	Buffer_overflow	30	52
	Rootkit	10	
	Loadmodule	9	
	Perl	3	

ISSN : 2277-1581
1 July 2017

The result of table 2 are obtained using purposive sampling of instances with respect to 22 attacks, and the researcher selected a minimum sample size that expected to give the same convergence as the entire population.

4. Results And Discussion

Graph 1: Classification Performance



This section evaluates the performance of individual method applied on the selected dataset. This study divides the data into 10 portions. Nine portions are retrieved as training, and the other one is used for testing data. This partition overcomes issues of either under-fitting or over-fitting of model. The majority of techniques perform well at the follow rate , Randomforest 99.8%, Tree J.48 99.7%, rules part 99.7%, Neural network at rate 99.6 % , Randomtree 99.6%, logistic 99.4%, SVM 99.1%, BayesNet 96.1% , decision table 98.4%, Hoeffding tree 90.1%, and NaiveBayes 79.1% .

5. CONCLUSION

This paper reviews a series of studies on IDS techniques that is based on its class. Both anomaly and misuse detection techniques have been discussed. Biological, data mining, cognition based, machine learning, state series modeling, simple rule, threshold, default deny and statistical, and their hybrid approach have been mentioned. Particularly we reassess paper published between the year 2010 and 2016.There is no one technique that is the best among the others, except under certain working condition. The result in this paper emphasizes that the system accuracy depend on dataset used during data training. We conclude that many IDS techniques have been used, and further improvement is needed using the hybridation of techniques to strongly protect the hackers whose purpose is always attempt to compromise the system.

REFERENCE

i. Balapure, S.A. & Shedge, K.N. (2015). Identification of DOS attack and DDOS attack using multivariate analysis techniques. *International Journal of Informative & Futuristic Research 3(4), 1303-1308.*

ii. Bansal, B. & Singh, K. (2015). Rule based intrusion detection system to identify attacking behavior and severity of attacks. *International journal of advanced research in computer science and software engineering 5(1), 718-724.*

iii. Beigh, *M.B. (2014).* A new Classification scheme for intrusion detection systems. *International Journal of Computer Network and Information security 8, 56-70.*

iv. Brindascri, S. & Saravanan, K. (2014).Evaluation of network intrusion detection using Markov Chain. *International Journal on cybernetics and informatics, 3 (2), 11-20.*

v. Deka, R. K., Kalita, K. P., Bhattacharya, B. K., & Kalita, J. K. (2015). Network Defense: Approaches, Methods and Techniques: *Journal of network and computer application, 1-18.*

vi. Hosseinpour, F., Amoli, P. V., Farahnakian, F. Plosila, J. & Timo, H. (2014). Artificial immune system based intrusion detection: Innata immunity using an unsupervised learning approach. *International journal of digital content technology and its application 8(5), 1-12.*

vii. Hoque, M.S., Mukit, M. A. & Bikas, A.N. (2012).An implementation of intrusion detection system using Genetic algorithm. *International journal of network security and its application 4(2), 109-120.*

viii. Sundus, J., Muda, Z., Mohamed, M.A. & Yassin, W. (2015). Machine learning techniques for intrusion detection system: A review. *Journal of theoretical and applied information technology 72(3), 422-429.*

ix. Malleh. Y. & Ezzati, A. (2015).Lightweight intrusion detection scheme for wireless sensor networks. *International journal of computer science 42(4).*

x. Maleh.Y. & Ezzati, A. (2013). A review of security attacks and intrusion detection schemes wireless sensor networks. *International journal of wireless & mobile networks 41(3), 79-90.*

xi. Mbikayi, H. K. (2012).An evolution strategy approach toward rule set generation for network intrusion detection systems. *International journal of soft computing and engineering, 2(5), 1-5.*

xii. Mudgal, A. & Munjal, R. (2015).Using support vector machine and naïve Bayes classification for intrusion detection. *International Journal for innovation research and technology, 1(9), 224-227.*

xiii. Panigrahi, A. & Patra, M. R. (2015). An artificial neural network for network intrusion detection using entropy based feature selection. *International network security and its application 7(3), 15-29.*

xiv. Parati, N. & Potteti, S. (2015). Intelligent intrusion detection system using SVM and Genetic algorithm. *International journal of science and information technology 4(2), 1-5.*

xv. Patel, B. (2014).Efficient string matching algorithm for intrusion detection. *International journal of computer engineering and science, 1-9.*

xvi. Patel, P. & Panchal, K. (2015).Effective intrusion system using Data mining Technique. *Journal of emerging technologies and innovation research 2(6), 1869-1878.*

xvii. Paliwal, S., Singh, R. S. & Mandoria, H. (2015). Analytical study on detection and prevention system .*International journal trends and technology in computer science 4(6), 177-182.*

xviii. Rizvi, R. S. H. & Keole, R. R. (2015). A Review on intrusion detection system .*International Journal of advance research in computer science and management studies,3(3),22-28.*

xix. Sawant,T. S. & Itkar, S. A. (2016).Intrusion detection system using adaboost based approach and fuzzy genetic algorithm. *International*

journal of innovative research in computer and communication engineering, 4(2), 2751-2758.

xx. Sandu, U.A., Haider,S., Naseer, S. & Ateeb, U. O. (2011). A Survey of intrusion detection and prevention techniques. *International on information communication and management 16, 66-71.*

xxi. Sharifi, A. A., Noorollah, B.A., & Farokhmanesh, F. (2014). Intrusion Detection and Prevention Systems and Security Issues. *International Journal Computer Network and Information security 14(11), 80-84.*

xxii. Shikha, S. & Simmi, J. (2016). A comparative analysis of decision tree based intrusion system. *International journal of modern trends in engineering and research 115-119.*

xxiii. Somani, M. & Dubey,R. (2014). Hybrid detection model based on clustering and association. *International journal of advanced research electrical, electronics and instrumentation engineering 3(3), 8152-8160.*

xxiv. Sunilkumar, G., Thriveni, J. ,Venugupal, K. R. & Patnail, L.M. (2012).Cognitive approach based user node activity monitoring for intrusion detection in wireless networks .*International journal of computer science issues 2(3),301-308.*

xxv. Sundarraj, B.(2014). Authentication Using Biometric Technique and Authorization for High Security Manets. *Middle-East of Scientific Research 19(6),775-779.*

xxvi. Solanki,M. M. & Dhamdhere,V.(2014).Intrusion detection system by using K-Means clustering, C4.5,FNN,SVM Classifier. *International Journal of emerging trends and technology in computer science 3(6),19-23.*

xxvii. Tesfahun, A. & Bhaskari, D. L. (2015).Effective hybrid intrusion detection system: A layered approach. *I.J Computer Network and Information security 3, 35-41.*

xxviii. Vijayarani, S. & Sylvia, M. S. (2015). Intrusion detection system. *International journal of security privacy and trust management 4(1), 31-44.*

xxix. Vinchurkar,D.P. & Reshamwala, A. (2012). A review of intrusion detection system using neural network and machine learning. *International journal of engineering and innovation technology 1(2), 54-63.*