International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 12, December 2015 **ISSN 2319 - 4847**

A Technique of Classification of Data Using NIDS And Response System

Prajakta G Sawant[1], Mrs. Asha M.Pawar[2]

[1]Student, Dept. of Computer Engineering, ZES's ZCOER, Pune, Maharashtra, India

2Assist.Proff., Dept. of Computer Engineering, ZES's ZCOER, Pune, Maharashtra, India

ABSTRACT

With the growth of network-based services and sensitive information on networks, network security is becoming more important. Intrusion detection techniques is defenses against computer attacks behind firewalls, secure network architecture design and personal screening. The number of network attacks has risen leading to the essentials of network intrusion detection systems to secure the network. Intrusion Detection Systems (IDSs) plays an important role in network security. IDSs can monitor events at the endpoints or on the network, with huge traffic volumes and heterogeneous accesses, several pattern identification techniques have been brought into the research community. The security of a computer system is compromised when an intrusion is took place. An intrusion can be defined as any set of actions that attempt to compromise of confidentiality, availability or integrity of a resource. Data mining or KDD is a process of the process of identifying valid, useful and understandable patterns in data.

Keywords: Classification; Data Mining; Intrusion Detection

1. Introduction

With the growth of internet, internet attack cases are increasing, and the methods of attack differs each day, thus information safety problem has became a significant issue all over the world. So, it is an urgent need to detect and identify such attacks effectively [2]. With rapid growth of network-based services and sensitive information on networks, the security of network is getting more and more importance than ever. A wide range of security technologies such as access control information encryption and intrusion prevention can be deployed to protect network based systems, there are always many undetected intrusions. For example, firewalls cannot prevent internal attacks. Thus, Intrusion Detection Systems (IDSs) play a important role in network security. To evolve the cyber attack and to overcome this problem this is faced by researchers and industry as a whole, the security of the network is very essential.

2. Data mining and IDS

2.1 DATA MINING

Data mining technology will be applied to Network Intrusion Detection System (NIDS), it may discover the pattern from the massive network data, to reduce the workload of the manual compilation normal behavior patterns and intrusion behavior patterns [3].Data Mining means extracting or mining the knowledge from large amount of data, it means processing data so as to gain the implied, prior unknown, potential and useful knowledge, which can be expressed as patterns. Data mining is the latest introduced technology of intrusion detection. It is attempt to use data mining in achieving network security, data mining itself is a general knowledge discovering technique. There are number of methods to strengthen the network security at the moment such as VPN, encryption, firewall, etc., but all of these are not dynamic to give an effective protection. However, intrusion detection is a dynamic one, which can gives dynamic protection to the network security in attack , monitoring and counter-attack .Intrusion Detection is the problem of identifying unauthorized use of computer systems by both system insiders and external intruders.

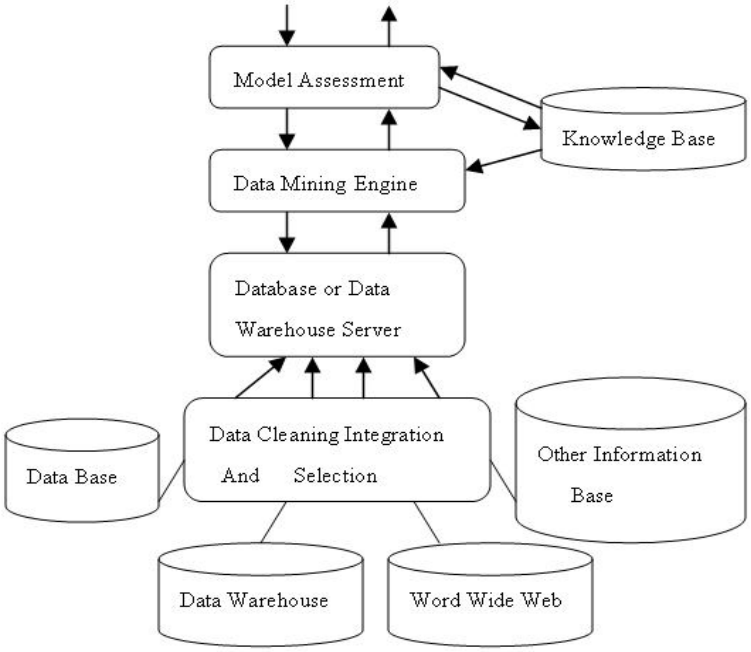

Fig1: Data mining system structure

2.2 INTRUSION DETECTION TECHNOLOGY:

DS defined as a system which identifies and deals with the malicious use of computer and network resources. IDS is the powerful system which can handle the intrusions of the computer environments by triggering alerts to make analysts which take actions to stop the intrusion.[6] Intrusion Detection is the problem of identifying misuse, and abuse of computer systems. According to the differences of data analysis methods, are two types of IDS. Data mining is a technology which IDS uses for attack recognition scheme. Using Intrusion Detection System various techniques, policies, methodologies introduced. Intrusion Detection Systems (IDS) have become a standard component in network security infrastructures and is an mechanism to protect computer systems from attacks. The conventional intrusion prevention techniques such as firewalls, encryption have failed to protect networks from increasingly complicated attacks and malwares. An Intrusion Detection System can be defined as a combination of software and hardware components which monitors computer systems and it makes an alarm as intrusion occurs.

There are two types of classification methods for intrusion detection system:

1. According to different data sources, intrusion detection system includes network-based IDS and host-based IDS.
2. According to different analysis methods, intrusion detection system includes Anomaly Detection and Misuse Detection [2]

The components in the architectural framework are:

- Data Gathering Device: it is responsible for collecting the data from different monitored system.
- Response Component: it initiates response (active or inactive) when intrusion is detected.
- Detector – ID Engine: processes the data collected from sensors to identify intrusive behavior and send an alarm signal to response component if there is an intrusion.
- Knowledge Base: it contains pre-processed information which is provided by network experts and collected by sensors.
- Configuration Device: it provides information about the current state of IDS. [7]

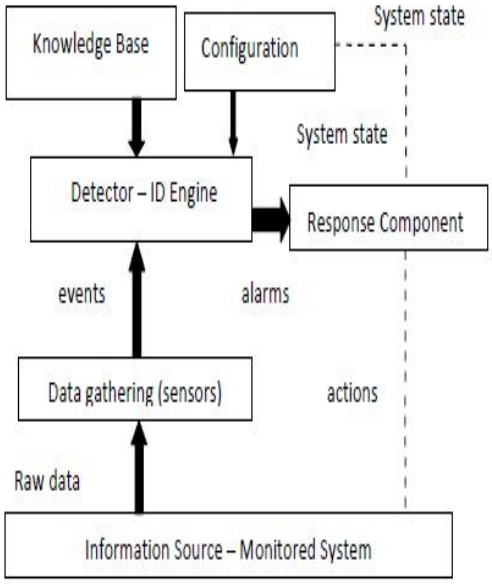

Fig2: Basic Architecture of IDS

An IDS can be categorized as misuse detection and anomaly detection. The misuse detection detects intrusions which is having low false alarm rate, but it fails to detect new attacks.IDS analyze the information it gathers and matches with the large databases of intrusive behavior or attack signatures. It is also called as signature-based detection. Anomaly detection has a capabalitiy which detects new types of attacks by defining whether the attack is static or dynamic. It determines whether or not deviation from the established normal usage patterns and is declared as intrusions.[7]

3. Literature review

Firstly the J. Parkkriri and K. Wiriyaphan in 2007 are performed the classification process on KDD using Decision Tree (DT),Ripper Rule (RR), and Neural Networks (NN) using weka tools which gives outstanding performance of decision tree. After one year in 2008 classification performance is measured of four main attack ie DoS, PROBE,U2R, R2L on KDD CUP by H.A. Nguyen and D. Choi. In 2010 P. Sararak and S. Prakarncharen measured the classification accuracy on KDD using *k*–Nearest Neighbour and NN on Weka tools.[1]

4. Related Study

For evaluate the performance of classification techniques, the methodology consist following four steps, which are, dataset preparation, data pre–processing, attribute selection, and classification.

4.1 DATASET PREPARATION :

To evolve the cyber attack and to overcome this problem this is faced by researchers that the security of the network is very essential and important. KDD CUP 1999 selected for classification evaluation process for standardizing the datset. The KDD CUP 1999 is based on the intrusion detection simulation of U.S. Air force local area networks using tcpdump. In general, KDD CUP has of four main attacks; they are DoS (Denial of Service), , U2R (User to Root), and R2L (Remote to User) , PROBE excluding BOTNET attacks, where each of which generates its individual attack.[1]

4.2 DATA PRE–PROCESSING:

KDD CUP 1999 is required totransform into a suitable format, before performing data mining classification.for making evaluation parameters fairly affected by un–equivalent numbers of records, a random record selection was performed given an equal proportional number of evaluated classes.[1]

4.3 ATTRIBUTE SELECTION:

As there many un–relevant attributes probably leading to low classification precision and high computational complexity the selection stage is used to figure out the suitable attributes[1]

4.4 CLASSIFICATION

There are sixn classification models embedded into the recent Weka tools; they are, Decision Tree, Naïve Bayes, Neural Networks, Ripper Rule, *k*–Nearest–Neighbour, and Support Vector Machine.[1]

5. Conclusion

There are different classification models are used in data mining techniques they are, Decision tree, Nural Networks , Naïve Bayes .Which are studied and evaluated in this research on network intrusion detection dataset in both KDD CUP 1999 and BOTNET (Zeus) trace using Weka tools.The classification methodology which includes different attribute and dataset selection criteria with different evaluation patterns which performed in details to illustrate the relationship among classes such as normal vs. attack, types of attack, and each individual attack.

References

[1] Chakchai So–In, Member, IEEE, Nutakarn Mongkonchai, Phet Aimtongkham, Kasidit Wijitsopon and Kanokmon Rujirakul," An Evaluation of Data Mining Classification Models for Network Intrusion Detection",2014
[2] S.Y. Wu and E. Yen, "Data mining–based intrusion detectors,"Expert System with Applications, vol. 36, no. 3, pp. 5605–5612,2009
[3] Ming Xue, Changjun Zhu," Applied Research on Data Mining Algorithm in Network Intrusion Detection", DOI 10.1109/JCAI.2009
[4] R. G. M. Helali, "Data Mining Based Network Intrusion Detection System: A Survey," Novel Algorithms and Techniques in Telecommunication and Network, pp. 501–505, 2010.
[5] H.J. Liao, C.H.R. Lin, Y.C. Lin, and K.Y. Tung, "Intrusion detection system: A comprehensive review," Journal of Network and Computer Application, vol. 36, no. 1, pp. 16–24, 2013.
[6] Manish Kumar, Dr. M. Hanumanthappa, Dr. T. V. Suresh Kumar," Intrusion Detection System Using Decision Tree Algorithm", 978-1-4673-2101-3, 2012
[7] P.Amudha, S.Karthik, S.Sivakumari," Classification Techniques for Intrusion Detection – An Overview",ijca Volume 76– No.16, August 2013

AUTHOR

Prajakta G. Sawant. Student at ZES's ZCOER, Department of Computer Engg. Pune, Maharashtra, India. Completed B.E. in Information Technology

Mrs.A.M.Pawar. Assist.Proff at ZES's ZCOER,Department of Computer Engg. Received M.Tech (CSE) from Belgaon .