IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 07-10
www.iosrjournals.org

A Study on Intrusion Detection and Protection Techniques

[1]Bini V C, [2]Aswani Shaji , [3]Prof. P Jayakumar, Nimmi M.K
[1]Dept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India, binivc@gmail.com
[2]Dept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India Aswanishaji1991@gmail.com
[3]Dept. of CSE Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India

Abstract: *Intrusion Detection Systems (IDS) plays a major role in computer security. In network environment IDS detect the activities that affect Confidentiality, Integrity and Availability on network data. There are two types of intruders External and Internal. External intruders are the outsiders from the network they are trying to attack the system with different techniques where as Internal Intruders are the authorized person to access the networks and they perform unauthorized or illegal activities. It is very difficult to detect the internal attacks. Most of the IDS and Firewalls detect the outsider attack only. Nowadays the numbers of cyber attacks and threats are increasing rapidly. Existing IDS are not efficient in detecting new threats and internal intrusions. Building efficient IDS for protecting information security system is a challenging task. The aim of this paper is to present a study on different techniques and algorithms used in IDS systems including insider attacks. The focus is on detection at System Call (SC) level using data mining and forensic techniques, genetic algorithms using the mechanism of natural selection and genetics and finally Fuzzy logic for an alert mechanism in IDS.*
Keywords : *Intrusion Detection, System Call, Genetic Algorithm, Data mining, Fuzzy logic*

I. Introduction

Intrusion Detection (ID) is the process of monitor the system activities and analyzes the attempt to compromise the confidentiality, integrity and availability on system data or network data. An IDS has different components [2] data collector responsible for collecting and providing for future reference, intrusion detector is the core component of IDS which analyze the audit pattern collected by the data collector and detect the attacks another component is the system profile used to characterize the normal and abnormal behavior last component is the response engine it controls the alert mechanisms. There are different types of attacks [3] and abuses are detectable by intrusion detection systems. They are : Password cracking and access violation, Trojan horses, interception, spoofing, scanning ports and services including ICMP scanning, remote OS fingerprinting, network packet listening, stealing information, authority abuse, unauthorized network connections, denial of service.
In this paper we perform a study on different techniques used in IDS. Detection of intrusion at system call level by using data mining and forensic techniques, Intelligent agents in IDS for detect the malicious activities intelligently, Genetic Algorithms to find out the anomalous network connections and finally Fuzzy logics for alerting when any abnormal activity detected. The remaining part of this paper is organized as follows. In Section II, we present an introduction on Intrusion Detection System. In Section III, we present a study on different Intrusion Detection Techniques. In Section IV, we give our conclusions

II. Intrusion Detection Systems

Intrusion means someone penetrate the security of the system without permission. Intrusion Detection System (IDS) [1] can detect the illegal activities performed by the Intruders and can report to the higher authorities. IDS is a set of methods and techniques to detect the illegal activities in System level and Network level. IDS can be broadly classified into two, Host Based Intrusion Detection Systems and Network Based Intrusion Detection Systems. Two phase protocol in which first handshake uses asymmetric cryptography which occurs only once and uses symmetric cryptography in the second phase.

A. Host based Intrusion Detection System

Host based Intrusion Detection System (HIDS) [4], [5] monitor the activities of a single system or host. Separate sensor or agent needed for each machine. It is one of the OS auditing mechanisms. The sensors also monitor the system log files and other logs generated by the operating system.

Advantages of HIDS are it can detect the attacks that involve the system integrity breaches and Trojan horse. It is useful for monitor the individual user behaviors. This can help to detect the attacks while they are happening or prevent the potential attacks before exploit in the system. It can be the ability to work in the encrypted environment. One of the main disadvantage of HIDS is it cannot see the network traffics [6]. Another thing is it is strongly depend on the host operating system. Its performance cost is high. Portability is an another issue.

B. Network based Intrusion Detection System (NIDS)

Network based Intrusion Detection System (NIDS) [6] collect information from the networks. They analyze the packet header of the data packets moving across the networks. If there is any misbehavior detected while analyzing the header information it inform to the authorities by using alert mechanisms. In NIDS deploy sensors having attack signature in different part of the networks. If any malicious activity is detected the sensors attached to it activated and alert to the authorities.

The main advantages of NIDS are they are independent of operating systems because of this they are portable. Another advantage of its low performance cost. The monitoring will be transparent to system users [7] this is also an advantage of NIDS.

The major disadvantage of this NIDS is its sensor have attack signature that are written based on the known and previous attacks. Another serious issue is its scalability in heavy traffic networks.

III. Different Type Intrusion Detection

1. Signature based Intrusion Detection[20]

Signature based detection involves searching network traffic for a series of malicious packet sequences and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detect malware. The main advantage of this technique is that signatures are easy to develop and understand if we know what the network behavior we are trying to identify. Signature engines also have their disadvantages. They only detect known attack, a signature must be created for every attack, and novel attacks cannot be detected. They are also prone to false positives since they are commonly based on string matching and regular expression.

2. Anomaly based Intrusion Detection[21]

The anomaly detection technique centers on the concept of a baseline for network behavior. The baseline is a description of accepted network behavior, which is specified by the network administrators. Events in an anomaly detection engine are caused by any behaviors that fall outside the accepted model of behavior. Anomaly based intrusion detection system have two major advantages .They have the ability to detect unknown attacks as well as zero day attacks. And the second advantage is that it is very difficult to an attacker to know the normal customized activities. A disadvantage of anomaly-detection engines is the difficulty of defining rules. Each protocol being analyzed must be defined and tested for accuracy.

III. Different Intrusion Detection Techniques

A. Intrusion Detection at System Call level using data mining and forensic techniques

System Call (SC) is a program signal for services from the Kernel of an operating system [8]. By analyzing SC we can categorize the normal and abnormal activities of a user. Therefore SCs widely used in IDS [8], [9], [10]. By using SCs we can generate normal user's computer using habits and also produce attacker's habits and produce user's behavior pattern and attacker's behavior patterns[12] , comparing user's behavior pattern with attackers pattern we can identify the internal attacks in a co-operate environments. Data mining is used to retrieve the information from the repositories for analyzing users and attackers' computer usage behaviors [12].

In many situations it is difficult to identify the anonymous system call from the normal one [8]. In such situation set a threshold value for the attacker pattern and user pattern.

B. Intelligent Agent and Data mining for Intrusion Detection

The characteristics of Intelligent Agents are reactivity, interactivity, autonomy and intelligent [13]. Agents are performing their activities intelligently. Agents can build knowledge from its past experience [14], [15]. The signature of attacks is changing every day. Intelligent Agent must learn new signature to detect new attacks in such situation data from agents are saved in data repositories and using data mining technique to categorize the normal and malicious activities in the network and reduces the false positive and false negative parameters [13].

C. Genetic Algorithm for Intrusion Detection

Genetic Algorithms (GA) are the heuristic search method based on natural selection and genetics [16], [17]. The algorithm begins with a population (set of individual) and each individual in the population known as chromosome. Random search used to solve optimization problem. GA is a machine learning techniques used for feature selection [17]. GA helps to learning itself from large amount of data. Embedded, filter and wrapper are three methods used in feature selection [16]. In feature selection repeated and irrelevant features are discarded and building efficient classification system. Reduces the feature subset increases the accuracy of classifier [18]. In network traffics GA uses pre classified data set for analyzing the normal and anomalous network connections [19].

D. Fuzzy-logic Based Alert Optimization Engine for IDS [22],[23]

Intrusion detection systems are designed to monitor a network environment and generate alerts whenever abnormal activities are detected. Fuzzy logic based features an alert rescoring technique that leads to a further reduction in the number of alerts.A fuzzy logic based analysis engine gives an overall threat level of an intrusion detection sensor, prioritizing alerts that are the most threatening. It is based on a set of membership functions that define certain matrices from an alert dataset and set of rules that determines a threat level based on the defined matrices.

IV Conclusion

Intrusion Detection Systems plays an important role in secure information security systems. Cyber crimes are increasing day by day. There are still many challenges to overcome for improving the efficiency of IDS. In this paper we perform a study on different techniques used in the IDS. All these techniques have some merits and demerits. The combination of these in IDS will give better result.

References

[1] J. Jabez and B. Muthukumar" Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach" *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015)*

[2] Rajni Tewatia, Asha Mishra " Introduction To Intrusion Detection System: Review "*INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 4, ISSUE 05, MAY 2015.*

[3] Sapna S. Kaushik, Dr. Prof.P.R.Deshmukh" Detection of Attacks in an Intrusion Detection System" *Sapna S Kaushik et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (3) , 2011, 982-986.*

[4] Lin Ying,Zhang Yan,Ou Yang-jia "The Design and implementation of Host-Based Intrusion Detection System" *IEEE Conference Publications on Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium,pages Pages: 595 – 598,*

[5] https://www.giac.org/.../host-vs-network-based-intrusion-detection.../102...

[6] Bace,Rebecca "An Introduction to Intrusion Detection &Assessment" *Infidel Inc., prepared for ICSA Inc. Copyright 1998.*

[7] Dr. S.Sasidhar Babu, " Secured SMS- A protocol for SMS security", International Journal of Computer Engineering & Technology, Volume 5, Issue 12, December (2014), pp. 37-41

[8] Zhenghua Xu , Xinghuo Yu , Yong Feng , Jiankun Hu , Zahir Tari , Fengling Han "A Multi-Module Anomaly Detection Scheme based on System Call Prediction*" 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA).*

[9] J. Hu, X. Yu, D. Qiu, and H.-H. Chen, "A simple and efficient hidden markov model scheme for host-based anomaly intrusion detection,"*Network Magazine of Global Internetworking*, vol. 23, pp. 42–47, 2009.

[10] L. Khan, M. Awad, and B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering," *The VLDB Journal*, vol. 16, no. 4, pp. 507–521, 2007.

[11] C. Warrender, S. Forrest, and B. Pearlmutter, "Detecting intrusions using system calls: Alternative data models," in *IEEE Symposium on Security and Privacy (S&P)*, 1999, pp. 133–145.

[12] Fang-Yie Leu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao-Tung Yang "An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques" *IEEE SYSTEMS JOURNAL*

[13] Irina Ioniţă, Liviu Ioniţă "An Agent-Based Approach for Building an Intrusion Detection System" *Networking in Education and Research, 2013 RoEduNet International Conference 12th Edition , pages 1-6, 26-28 Sept. 2013* ,

[14] I. M. Hegazy, T. Al-Arif, Z.T. Fayed, and H. M. Faheem, "A framework for multiagent-based system for intrusion detection", *in Proceedings of the 3rd International Conference on Intelligent Systems Design and Applications (ISDA'03), August 2003*

[15] I. M. Hegazy, H. M. Faheem, T. Al-Arif, and T. Ahmed, "Performance evaluation of agent-based IDS", *in Proceedings of the 2nd International Conference on Intelligent Computing and Information Systems (ICICIS 2005), p. 314 - 319, March 2005.*

[16] Mr. Ketan Sanjay Desale, Ms. Roshani Ade "Genetic Algorithm based Feature Selection Approach for Effective Intrusion Detection System" *2015 International Conference on Computer Communication and Informatics (ICCCI -2015), Jan. 08 – 10, 2015.*

[17] Wei Li, "Using Genetic Algorithm for Network Intrusion Detection", *Proceedings of the United States Department of Energy Cyber Security Grou, Training Conference, 2004, Vol. 8, pp. 24-27.*

[18] Mouaad KEZIH, Mahmoud TAIBI, "Evaluation Effectiveness of Intrusion Detection System with Reduced Dimension Using Data Mining Classification Tools", *2nd International Conference on Systems and Computer Science (ICSCS) , August 26-27, 2013.*

[19] Wei Li "Using Genetic Algorithm for Network Intrusion Detection".

[20] V.Jyothsna,V.V.RamaPrasad" A Review of Anomaly based IntrusionDetectionSystems".

[21] J.L.Rana,R.N.Yadav" Taxonomy of Anomaly Based Intrusion DetectionSystem:AReview" *International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012 1 ISSN 2250-3153 www.ijsrp.org.*
[22] Gray, Jeremy D., "ARF : an Automated Real-Time Fuzzy Logic Threat Evaluation System." (2006). Electronic Theses and Dissertations. Paper 526. http://dx.doi.org/10.18297/etd/526
[23] BIJIT - BVICAM's International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)