I J C T A, 9(15), 2016, pp. 7613-7618

Test Case Based Analysis on Traffic as a Parameter for Intrusion Detetcion in a Library System

Saurav Mishra*, Manjusha Pandey and Gargi Srivastava*****

ABSTRACT

The network traffic analysis has increase massively over the last couple of year because of increasing use of computer by and even increases need of connecting computer for slowing of data processes and resources. The traffic may be defining as a flow of data across the internet during the usage. Traffic analysis has been the most vulnerable activity in the cyber world. Intrusion detection is a mechanism of detecting the arising of any malicious pattern in the traffic condition of the system. The IDS may also base on various parameter through traffic is are of prime parameters. In my article I have used KIIT library system on the intrusion detection system which provide security to the KIIT database. In the present article we have taken the KIIT data traffic of library system as a use case. We implement the intrusion detection system which provide security to the user in the KIIT library system database. We have defined the front end system as well as the back end system. The front end system has been describing for the detailed and the back end system are used for the support for analysis and visualization of malicious traffic generated and propagated. The back end system is responsible for the incoming and outgoing traffic in the KIIT library system.

Keywords: Intrusion Detection system, Traffic analysis, PCAPLIB

1. INTRODUCTION

The idea [1] of the intrusion detection system was proposed by Anderson in 1980. He provides the technique to examine the behavior of the user and to detect the attacker who want to access the system form unauthorized way. Intrusion detection system [2] is a system to detect unwanted activity of the system. Intrusion [9] detection system is largely implemented in the computer networks. Intrusion detection system can be used as a powerful tool to protect the organization from the different types of attacker. The network traffic plays a major role in the intrusion detection system. Intrusion detection system used to monitor the network traffic from the malicious activities. Intrusion detection system [12] monitor the system behavior and show the alert while any error occurs [3]. THz e intrusion detection system is to use all available information and data in order to passive attacker and hacker. Intrusion detection consist of following two detection technique. The firstly named as Anomaly based intrusion detection system and the secondly is named as Misuse based intrusion detection system.

1.1. Anomaly based intrusion detection system

The anomaly based intrusion detection system is used to detect the anomaly in normal pattern of the system. This abnormal traffic pattern may be like anomaly time, anomaly routing etc. The anomaly based intrusion detection system detect both network as well as the host level of the system [3]. The anomaly intrusion detection system provide defense to detect anomaly network traffic pattern and network layer that passes through a firewall or other security device to the network traffic. The misuse based intrusion detection

* line 1 KIIT UNIVERSTY, line 2: India, line 4: *Email: sauravm62@gmail.com*

** line 1 KIIT UNIVERSITY, line 2: India, line 4: *Email: manjushapandey82@gmail.com*

*** line 1 KIIT UNIVERSITY, line 2: India, line 4: *Email: Gargisri68@gmail.com*

system is used to identifies the traffic pattern of the unwanted activities like malicious routes, wrong destination etc. The misuse base intrusion detection system also called as signature based detection system. The intrusion detection system based on the type application could be of the following as 1) Network based intrusion detection system.2) Host based intrusion detection system.

1.2. Network based intrusion detection system

Network based intrusion [3] detection system is an in depend platform that identify network traffic and monitor the multiple host as the network for the traffic generation and termination pattern. Network based intrusion detection system gain the access to network by connecting to the network hub, network switch, configuration for port monitory g and the network hop. NIDS is used to monitor and analysis network traffic to protect the system from server can also scan system file and also keep watch on the unauthorized activities. The NIDS can also detect the change on the pattern in network traffic, core component of the internet traffic. The network based intrusion detection system check the pattern of the network packet in the real time. The NIDS play a vital role in the network traffic.

1.3. Host based intrusion detection system

The host based intrusion detection system is used to monitor and analysis the traffic pattern at the host level, but not including the traffic pattern widely. It provides protection to the file of the network traffic. Host based intrusion detection system is a software that project against [1][9] the buffer overflow of the memory system of the user. The main principal of the HIDS is that, it used to find that, if the intruder has successfully attack the network system or not, then it checks the appropriate region of memory which has not been modified by attacker and provide a specific tool to protect that area from the attacker.

1.3.1. Network traffic as a parameter for Intrusion detection system

The network traffic mostly encapsulated in network packet which provide information to the network. The network traffic is the main [5][6] component for the traffic analysis. In the case of intrusion detection system network traffic plays a major role for detecting anything of network attack on the traffic flow. The network traffic is increase massively last couple of year [11]. This has been results of the increase in network access on speed, leading toward network based intrusion. Hence the network traffic plays an important role as a parameter to detect and correct the network intrusion.

1.3.2. The KIIT Library System and the PCAPLib system

The KIIT library system is the test case system consider for which provide the traffic was monitored to make the system intrusion free [7][8]. The problem definition lies with how to identifies and detect the KIIT library system. In this the particular case we consider fake traffic for intrusion detection in network traffic The analysis was done while maintaining the network quality for the network user. The network traffic consists of record of the data of the user in the network traffic. This is monitored by the user the (PCAP) lib [10]. The real of the articherture is to trace and identify the malicious activity and file traffic provide by the user in the KIIT library system. We consist two mechanisms as front end system and back end system. The front end system not only extract data and characterize valuable packet from the real world traffic but also protect the data and the sensitive information of KIIT library system. The front end system consists of component, the first component is named as preprocess and second component is names as Core processes.

3. PRE-PROCESSES

In the pre-processing is dependent on the following component based on functioning of the KIIT library system are:

ALERT SERVER – The alert server is used to trace the different type of malicious activity and harmful data provided by the user while submitting on information input the KIIT library network

MULTIPLE DUT (device under trace) – To detect the abnormal behavior of various user. We use DUTs in the use of abnormal activity that will trigger an alert, while any unwanted occurrence occurs.

RESTART TOOL – The restart tool is used to restart the system, if any case of inaccuracy in or input given to the system. The restart tool also checks all unwanted activities the while the time of restart.

PCAPLIB SYSTEM – The PCAPLIB system stand for packet capture (PCAP) library system. It is used to store the different type of packet or data of the library system

3.1. Core Processes

In the core-processing is dependent on the following component based on functioning of the KIIT library system are;

EXTRACTION MODULE – In the case of extraction module is used to extract or separate the data which is provided by PCAP KIIT library system. It used to separate unwanted, malicious activity and authenticated data of the user.

SORTING MODULE – In the case of allocation module, it used to organize the data of the KIIT library system It is used to arrange, while input information in the library network.

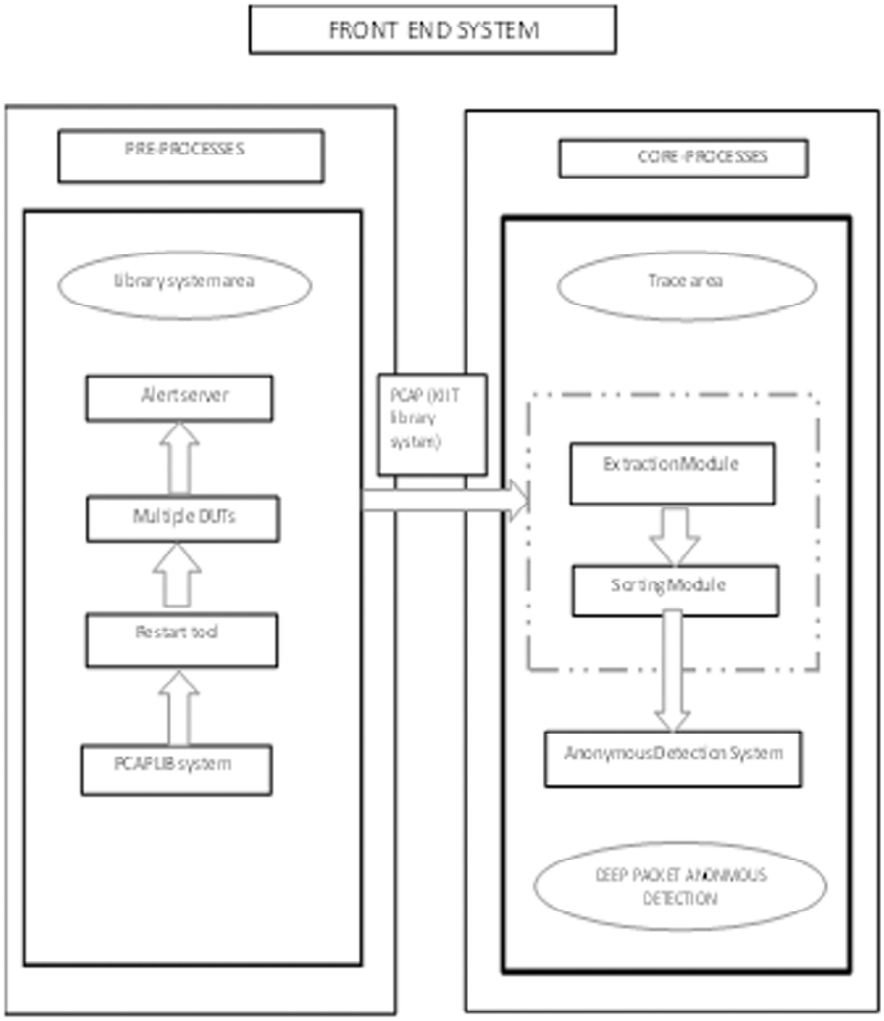

Figure 1: (a) front end system block diagram

ABNORMAL DETECTION MODULE – This is a module used to detect the unwanted, malicious activity occur in the network of the of KIIT library system

The other side we have "BACK END SYSTEM "which have database of the KIIT library system. The database consists of an APPLICATION, WEBSITE, LOGIN BLOCK. Are describe as follow;

APPLICATION – It is a tool which show all the information of the back end system to the user. These application tool produces vital information the user and enabling the user to perform his task

WEBSITE – The website consists the address of the "BACK END SYSTEM ". The website is homepage of the back end system of the KIIT library system.

LOGIN BOX – It is a processes by which authorized individual can access the website to use it

FAKE TRAFFIC DETECT TOOL – The fake traffic detect tool is a tool that has been used to detect the flow of fake traffic in the KIIT library system. With the help of traffic tool, we can identify the fake flow of traffic information which are generated by the attacker. It identifies the fake traffic based on the data flow from the website by the other authorized user when they open during their website.

RESTART BOTTOM: The restart bottom is used to restart if the user enters error password. By these it will reduce time and increase the accuracy.

CHECK BOTTOM – The check bottom is used to check the unwanted activity in the flow of data while the user login into the website of the KIIT library system.

LIST – The list contains the detail of the address as well as the information about the user through which we can access the traffic flow and detect the malicious behavior.

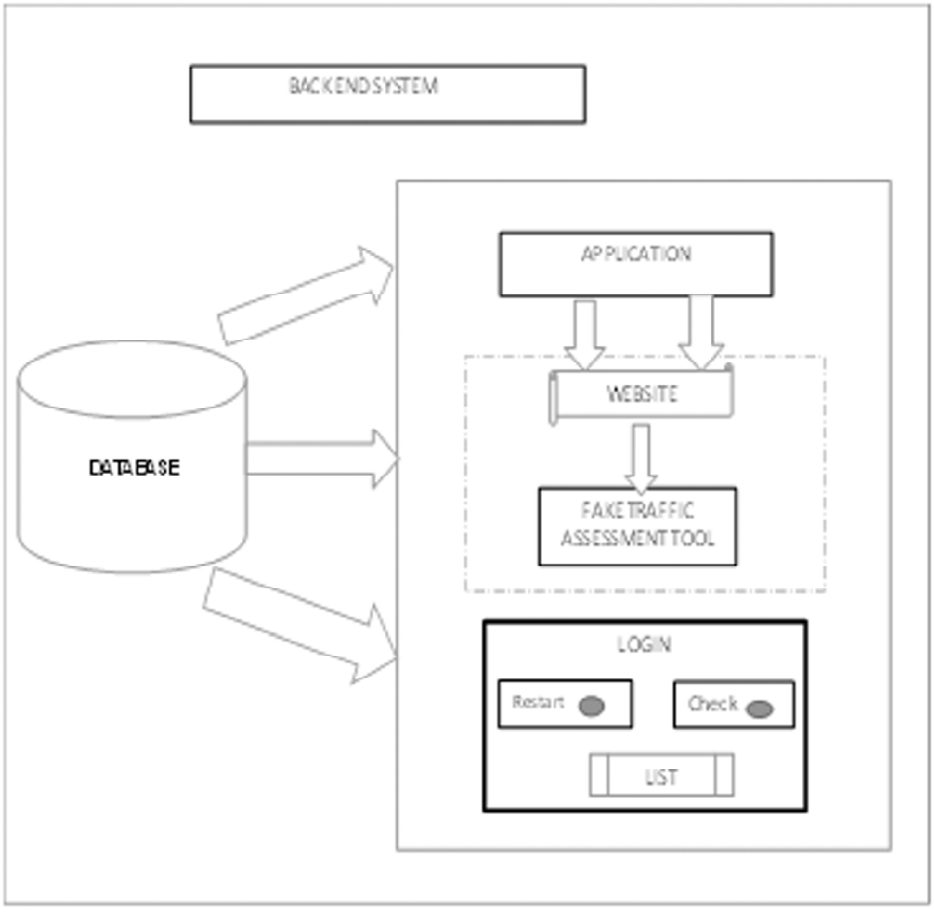

Figure 1: (b) back end system block diagram

4. DISCUSSION

In our presented article we have implemented a front end system and back end system for the KIIT library system using intrusion detection system [18] [19] [20] based network traffic. The front end system generates the structural overview for the user as an interface to store their information in the KIIT library system. The front end system consists of two set of processes, first set is named as Pre Process and second set is named as Core Processes. The front end system is use to authorizes the vital information of the user like Id, password, so that error reduction can be done. Many components of the front end system help us to identifies the malicious activities by the monitoring traffic flows that based on the flow data into the KIIT library system. These component based on their inbuilt mechanisms for provide efficiency, accuracy to the KIIT library system. The PCAPLIB [5][6] system play a vital role in these preprocesses structure. The PCAPLIB is also known as "packet capture alert processor" for library system. PCAP help to capture or collect the packet or data of the user and other client while they produce it during the use of library. The PCAP is used to transmit the data or packet to the restart tool. The restart tool identifies information of the user based on the data store in it memory. The processes are tranced the information using data to multiple DUTs. The DUTs is also known as "data under trace".is used to trace the data and information of the user, if any error or vulnerability find and show alert warning to Alert server. Then the pre processer collect and send verified data of the user through the PCAP to the Core-processes that take the session of the front end system [8]. The core-processes consist of some vital components as trace area, anonymous detection module, deep packet anonymous detection. The trace area is divided into subarea as Extraction module and sorting module [7]. The extraction module is used to separate the data and packet send through the traffic flow to KIIT library system. The sorting module used to sort the data or arrange then in organized manner. Anonymous module is used detect the abnormal behavior of the data and also trace their time when the data has been insert in the database of the library system. The deep packet anonymous detection system is detecting and trace unauthorized, unwanted data of the student while insert the data. The deep packet anonymous detection also detects deeply users account, id, password. The back end system of the KIIT library system [10] all data that are store in the database. The back end system contains of components like application, website, logic block. [14] The back end system provides the hypertext link through which the user can access comfortable The back end system provides secure IP address [13] for the user in network cyber world. In this paper we have taken a KIIT library system as a test case for our traffic based intrusion detection system. We have considered the front end system and back end system which help to reduce error and detect malicious activity [17] in KIIT library system. We have used different component of the front end and back systems to reduce the error and increase efficiency, accuracy. We aim that this article will help student to understand how traffic analysis could be used as parameter for intrusion detection system. In our article we have presented a structural overview how to detect the network traffic and use it to design and evolve our intrusion detection system

5. ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R. B. G.) thanks . . ." Instead, try "R. B. G. thanks". Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

[1] Callao, Arthur, et al. "A survey on internet traffic identification. "*Communications Surveys & Tutorials, IEEE* 11.3 (2009): 37-52.

[2] www.wileyindia.com /Network security by Bible

[3] Rowland, Craig H. "Intrusion detection system." U.S. Patent No. 6,405,318. 11 Jun. 2002.

[4] Rowland, Craig H. “Intrusion detection system.” U.S. Patent 6,405,318, issued June 11, 2002.

[5] Lin, Ying-Dar, et al. “Pcaplib: A system of extracting, classifying, and anonymizing real packet traces.” (2014).

[6] Ho, Cheng-Yuan, et al. “False positives and negatives from real traffic with intrusion detection/prevention sys-tems.” International Journal of Future Computer and Communication 1.2 (2012): 87.

[7] Ho, Cheng-Yuan, et al. “Statistical analysis of false posi-tives and false negatives from real traffic with intrusion de-tection/prevention systems. “Communications Magazine, IEEE 50.3 (2012): 146-154.

[8] Rani, S. Jamuna, and J. Preethi. “ANALYSE THE IN-TRUSION FROM NETWORK PACKETS USING IDS.”

[9] Hu, Zhi Yu, and Li Li. “Detecting Computer Network Anomaly with Data Mining Technology.” 2015 Interna-tional Conference on Intelligent Systems Research and Mechatronics Engineering. Atlantis Press, 2015.

[10] Lin, Ying-Dar, et al. “On campus beta site: architecture designs, operational experience, and top product de-fects.” Communications Magazine, IEEE48. 12 (2010): 83-91.

[11] Mukherjee, Biswanath, L. Todd Heberlein, and Karl N. Levitt. “Network intrusion detection.” Network, IEEE 8.3 (1994): 26-41.

[12] Abu Hmed, Tamer, Abedelaziz Mohaisen, and Dae Hun Nyang. “A survey on deep packet inspection for intrusion detection systems.” arXiv preprint arXiv:0803.0037 (2008).

[13] Arndt, Manfred Ruediger, and Frank John Actis. “Method of configuring a valid IP address and detecting duplicate IP addresses in a local area network.” U.S. Patent No. 5, 724, 510. 3 Mar. 1998.

[14] Huang, Zazen. “Method and system for protecting computer system from malicious software operation.” U.S. Patent Application No. 10/792, 506.

[15] Zhengbing, Hu, Li Zhitang, and Wu Junqi. “A novel network intrusion detection system (nids) based on signa-tures search of data mining.”Knowledge Discovery and Da-ta Mining, 2008. WKDD 2008. First International Work-shop on. IEEE, 2008.

[16] Krügel, Christopher, Thomas Toth, and Engin Kirda. “Service specific anomaly detection for network intru-sion detection.” Proceedings of the 2002 ACM sympo-sium on Applied computing.

[17] Pérez, Manuel Gil, et al. “RepCIDN: A reputa-tion-based collaborative intrusion detection network to lessen the impact of malicious alarms.”Journal of Net-work and Systems Management 21.1 (2013): 128-167.

[18] Debar, Hervé, Marc Dacier, and Andreas Wespi. “Towards a taxonomy of intrusion-detection sys-tems.” Computer Networks 31.8 (1999): 805-822.

[19] Back, Adam, Ulf Möller, and Anton Stiglic. “Traffic analysis attacks and trade-offs in anonymity providing systems.” Information Hiding. Springer Berlin Heidel-berg, 2001.

[20] Vaidya, Vimal. “Dynamic signature inspec-tion-based network intrusion detection.” U.S. Patent No. 6,279,113. 21 Aug. 2001.