Performance Analysis of Snort-based Intrusion Detection System

Akash Garg
Department of Computer Science and Engineering,
Ajay Kumar Garg Engineering College,
Ghaziabad, India
garg.theakash92@gmail.com

Prachi Maheshwari
Department of Computer Science and Engineering,
Ajay Kumar Garg Engineering College,
Ghaziabad, India
prashi0110@gmail.com

***Abstract* - The most important purpose of intrusion detection system is to identify attacks against information systems. It is a security method attempting to identify various attacks. Snort is mostly used signature based IDS because it is an open source software. It is used world widely in intrusion detection and prevention domain. In this paper, we used IDEVAL data set we detect attacks using Snort on this dataset.**

Keywords - Intrusion Detection System; Misuse; Snort; Network.

I. INTRODUCTION

Now a days, it is the main problem to maintain the network security. As computer network is growing day by day, security is the most powerful mechanism for a computer network. Firewalls are not much capable to secure network from attacks because firewall can only detect the attacks which come from outside of the network [1]. With the rapid use of computers and ease of access to internet in the world, the ways to attack and deceive a system has also rapidly increased. Intrusion, in other words, is an illegal process of entering or taking possession of another's assets.

This paper focal points on identifying the irregular relationship that has been noticed by our IDS via Snort when we flow the IDEVAL Data Set over the network. Intrusion Detection System mechanisms as a set of connections or network package beak or sniffer, which based on analogy of data small package inside with recognized disease signatures summarize as strategy, can begin act and evidence actions and information associated to them in a record file and/or database. Snort is a well-liked Network based intrusion detection system that is used to audit network packets and compare those packets with the information of glorious attack signature and Snorts attack signature information database may also be rationalized time by time [5].

As the set of connections surroundings turn into multifaceted and huge level, and intrusion events be converted into miscellaneous. It suggests far above the ground strains to the intrusion detection technologies, demanding intrusion detection system to bring together information set from dissimilar set of connections and host and moderator the job of the whole set of connections, appropriate cautioning intrusion detection and reply consequently [2].

What is intrusion detection?

Intrusion detection is the method of figuring out the actions happening in a computer system as well as justifying them for the symbol of intrusion.

II. INTRUSION DETECTION SYSTEM

Intrusion detection is a technique in computer network which play an important role in detecting different type of attacks. It is the procedure of observing the actions which passes in a computer system. Intrusion detection provides three main security phenomenons such as monitoring, detecting, and responding. The motive of Intrusion Detection System is to identify inner as well as outer attacks. In common we can say that, an IDS's consist of hardware component. To run hardware component compatible software is also proceeding with the system [2].

Working of Intrusion Detection System is like the security guard. The two assumptions in the field of intrusion detection are 1) user and program events are monitored by computer systems and 2) traditional and intrusion activities can have totally different behavior [3].

The main benefits can be summarized as:-

1. Detecting attacks and various security violations.
2. Identifying the harm and affected systems.
3. It doesn't suffer with the harmful security.
4. For security model and implementation, works as quality control.
5. Saving problem-behaviors by increasing the obtained risk of discovery.
6. Presenting elements of intrusions, granting corrected identification, recovery and corrective measures.
7. Listing the present malware from among and outdoors a system [4].
8. Observing and analyzing computer and/or network system activity.

[978-1-4673-9206-8/16/$31.00 ©2016 IEEE]

9. Checking the system configurations and vulnerabilities.
10. Evaluating the integrity of vital system and information files.
11. Estimating irregular activities.

Ideal IDS should possess the following features:-

1. Timeliness: The property guarantees that any abnormal behavior can be detected within stipulated time or just after that time.
2. High probability of detection: It guarantees to identify most of the abnormal behavior in the network.
3. Low false-alarm rate: This property allows a few numbers of false alarms.
4. Specificity: once attack is identified sufficient detailed information must be available so to get a better response.
5. Scalability: Scalability can be applied to big and small networks.
6. Low a priori information: This property needs a least of priori information concerning potential assailants and their strategies [4].

III. LITERATURE SURVEY

Mahoney described the two models for anomaly detection system for checking doubtful traffic. First of all for passing simply the data packets of the majority requirement, e.g. first some packets of inward server requests, the traffic were filtered. Second, at the packet byte stage to flag events that have not been found for a long span of time, the most common usable network protocols (IP, TCP, telnet, FTP, SMTP, HTTP) were designed [9].

Mahoney and Chan characterize an empirical PHAD that determines the ordinary range of values for 33 fields of the Ethernet, IP, TCP, UDP, and ICMP protocols. On the IDEVAL data set, PHAD identify 72 of 201 objects of attacks, together with all but 3 types that accomplishment the network protocols tested, at a speed of 10 false alarms per day performing the training on 7 days of attack less internal network traffic. PHAD studied in various ways, and the better outcomes were finding by exploring network packets and fields separately, and by using uncomplicated nonstationary structures [14].

Mahoney and Chan introduced a set of instruction called learning algorithm which structures design of usual nature from anomalies free network traffic. Nature that bifurcates from the known normal design signals possible novel attacks. Their intrusion detection system is special in two aspects. In first, the nonstationary model is presented in which the designing chances based on the span of time from the time when the occurrence of last event instead of the rate. Now in the second, the intrusion detection system monitors the protocol collection in order to identify the unknown attacks that try to harm design faults in poorly monitored characteristics of the target software. On the 1999 DARPA intrusion detection system evaluation information set, they identified 70 of 180 attacks, and portioned among user behavioural anomalies and protocol anomalies. As their ways are alternative, there is a symbolic non-overlap of their intrusion detection system with the genuine DARPA members, which symbolise that they can be taken overall to enhance the coverage [10].

Mahoney and Chan introduced a set of instruction called LERAD that operates principles for identifying few occurrences in normal time series information with long order reliance. They used LERAD to identifying anomalies in network traffic packets and TCP sessions to identify novel intrusions. LERAD results the actual participants in the DARPA dataset, and identified almost all attacks that arise a firewall. LERAD is well-organized for three causes. First, only a small part of the traffic has been tested. Second, the principles using only a little sample of the training information has been generated. Third, for building a small collection of principles that mostly covers the information, a coverage test has been used [11].

Aydin et al proposed a hybrid intrusion detection system which is the combination of misuse and anomaly based intrusion detection. In this paper they took snort as misuse based with PHAD and NETAD as anomaly based intrusion detection. PHAD and NETAD are the anomaly based statistical method. Firstly, snort is tasted on IDEVAL dataset then it detects 27 attacks out of 201 attacks, secondly PHAD is added to the snort as a preprocessor (Snort + PHAD) is tested on same dataset then the number of attacks detected is increases up to 51 out of 201 attacks, finally NETAD is added to the snort and PHAD as a preprocessor (Snort + PHAD + NETAD) is tested on same dataset then the number of attacks detected is increases up to 146 out of 201 attacks [1].

Nandiammai and Hemalatha proposed a method named as hybrid intrusion detection in which first they used the statistical based anomaly methods such as ALAD, LERAD and PHAD then combine these methods with snort which is misuse based. Firstly snort is tested on KDD Cup 99 dataset then it detects 77 attacks out of 180 attacks after that PHAD is added to the snort as a preprocessor (Snort + PHAD) is tested on the same dataset then the number of detected attacks raises to 105 out of 180 attacks after that ALAD is added to the snort and PHAD as a preprocessor (Snort + PHAD + ALAD) is tested on the same KDD Cup 99 dataset then the number of attacks detected increases to 124 out of 180 attacks after that LERAD and ALAD is added to the snort as a preprocessor (Snort + LERAD + ALAD) is tested on the same KDD Cup 99 dataset then the number of attacks detected increases up to 149 out of 180 attacks. Secondly, the advantage of both supervised and

unsupervised methods has been used to develop a semi-supervised method. Semi supervised approach requires less amount of labeled data with heavy amount of unlabeled data. For semi supervised approach 5000 dataset are taken, in that 2500 taken as training phase and least is taken as testing phase. Training phase includes both the labeled and unlabeled data together. The result of semi supervised approach shows 98.88 % detection rate and 0.5529 % false alarm rate [12].

Nandiammai and Hemalatha proposed an intrusion detection system which is the combination of four approaches such as classification of data named as EDADT (combination of hybrid PSO with C4.5), snort based processing named as hybrid IDS (combination of snort which is misuse based IDS with ALAD and LERAD which are anomaly based statistical algorithm), semi-supervised approach, migrating DDoS attacks named as Varying HOPERAA. Firstly EDADT algorithm gives result as 92.51% sensitivity, 88.39% specificity, 95.37% accuracy, 0.72% false alarm rate. Secondly hybrid IDS gives result as discussed above and Third semi supervised gives result as also discussed above. Finally in HOPERAA algorithm a variable clock drift method is proposed to avoid the client waiting time for server and at the same time message loss is avoided greatly. Thus HOPERAA can minimize the message transfer delay as well as execution time [13].

IV. IDS TYPES

There are two ways of IDS's. These are misuse-based IDS and anomaly-based IDS. Misuse approach detects the better known attacks that are predefined however fails to identify the unknown attacks. The major advantage of using misuse approach is to produce less false alarms. In anomaly approach, it detects the unknown attacks with high false alarms. Once an anomaly based attack is detected it becomes a signature based or misuse based attack.

1. Misuse-based or Signature Based IDS

Misuse based IDS is used to detect the known attacks which are predefined. Each of the known attacks are predetermined in the form of signature and are saved, incoming data is matched with their signature to determine the attacks [5].

Working of Misuse-based or Signature Based IDS:-

Misuse-based or Signature Based IDS works when a person sends data to the network. Firstly all data depart to the server and server verify them, if any harmful data is found then server discards the packet else sends it to the network. When the data arrives to server, server uses comparing tool to verify that network packet from the database of signature stored in the server and if server identify the packet that is matched to the database then it discards the network packet else sends the data to the network [5].

Advantages

1. Alarm is raised when the signature is matched.
2. Signatures are developed based on predefined rules in the tool and depending on the network behavior.
3. Generate low false positive alarm rate.

Disadvantages

1. They can only detect the attacks which are previously stored in the database.
2. They cannot detect the live attacks which are created by human.
3. The information about attack depend on operating system we are using, application we are running.

1.1 Snort

Snort is a well liked open source NIDS (available at http://www.snort.org/assets/125/snort_manual-_8_5_1.pdf). It can examine concurrent transfer communication analysis and data flow in system. It is clever to make sure procedure psychoanalysis and can identify dissimilar kind of bother. In NIDS snort essentially make sure packet alongside rule written by user. Snort rules may be written in any language, its models is in addition under stable and it can be easily read and rules can be modified. In buffer overflow attack, snort can noticed the anomalies by identical the preceding prototype of anomalies and then will take suitable act to avoid from these anomalies. In signature based IDS system, if pattern competition then anomalies can be with no trouble found but when a new anomaly move toward then system fails but snort conquer this restraint by examining the real-time transfer communication. At any time any small package gets nearer into system then snort make sure the performance of network. If performance of system humiliates then snort discontinue the dispensation of packet, rejects the packet and stores its detail information in the signature database [5].

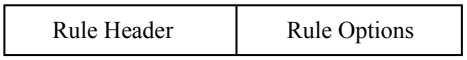

Fig. 1. Snort IDS rule structure [6]

Figure 1, shows the basic structure of the Snort-IDS rules which are portioned into two parts: first, rule header and second, rule option.

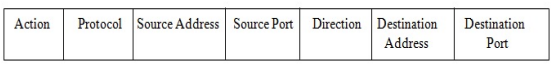

Fig. 2. Snort IDS rules header structure [6]

Figure 2, shows each field in the rule header of the Snort-IDS rules.

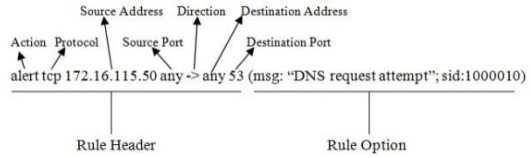

Fig. 3. The snort IDS rules example [6]

Figure 3, shows an example of the Snort-IDS rule. This Snort-IDS rule will generate the alert, when a tcp packet with source IP address number 172.16.115.50 is sent from any port to any destination IP address with destination port number is 53 (DNS). In addition, it also shows the message "DNS request attempt" and the number of the rule is sid:1000010 [6].

An illustration of Snort's packet processing is given in figure 4,

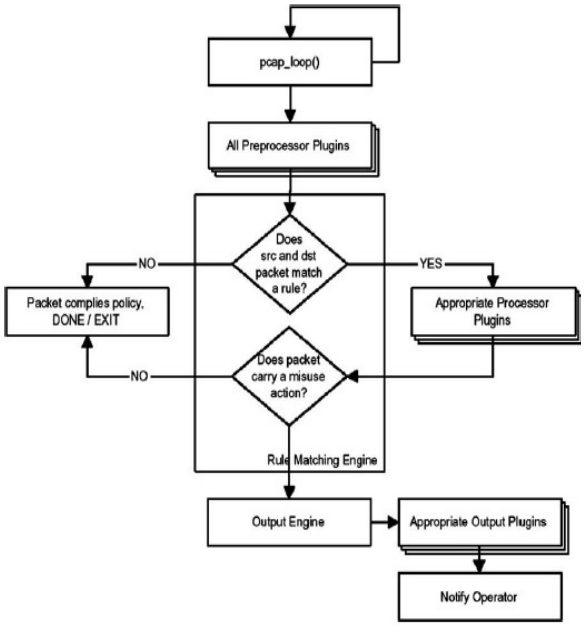

Fig. 4. Packet flow through Snort [1]

Component of Snort

Snort is the combination of various components which is shown in figure 5,

1. Packet Decoder
2. Preprocessor
3. Detection Engine
4. Logging and Alerting System
5. Output Modules

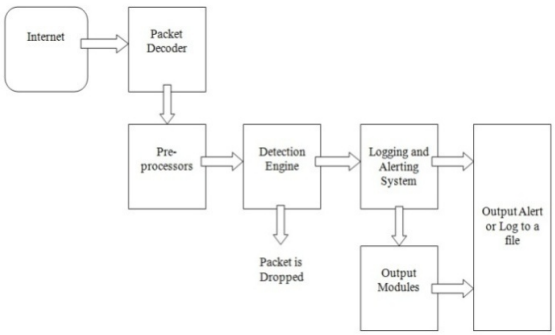

Fig. 5. Component of Snort [5]

1. Packet Decoder

It extracts packet from network in form of tcpdump-formated file and forward packet to preprocessor [5].

2. Preprocessor

If the packet is corrupted, it is used to modify them using some operation & then resends them to the detection engine. It generates alert if any attack is found in the packet [5].

3. Detection Engine

This component is mainly used to detect intrusion activity which exists in the packet by using snort rules. If the intrusion is found then it applies appropriate signature and action otherwise drops the packet. The time taken is proportional to number of rules (signature) defined [5].

4. Logging and Alerting System

This component is used to generate the alarm or log activity of intrusion that is detected by detection engine [5].

5. Output Modules

It is used to save the output generated by logging and alerting system [5].

2. Anomaly Based IDS

Anomaly based IDS is used to detect the unknown attacks. It identifies the abnormal behavior. Anomaly detection characterizes the forecasted performance of the network. Any notable variations from such outline forecasted performance are reported as possible attacks [7]. It is an effort to recognize malevolent network traffic based on aberrations from reputable usual network traffic patterns [8].

Advantages

1. They can be utilized to acquire the signature information used by misuse-based IDS.
2. They identify attacks still when complete information of the attack does not be present.
3. No rules needed to be written [9].

Disadvantages

1. They generate high false alarms rate.
2. Defining rule set is difficult.
3. They do not define the nature of attack [9].
4. Low detection rate [7].

V. EXPERIMENT RESULTS

- Alert identified by Snort:

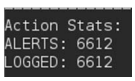

Fig.6. Alert detected by Snort

- Attack detected by Snort:

Fig.7. Attack and False Alarms detected by Snort

- Graph showing relation between attacks and false alarms detected by Snort,

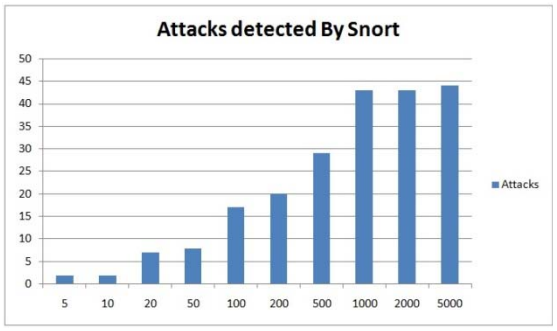

Fig.8. Graph shows Alert and False Alarms detected by Snort

VI. CONCLUSION

Intrusion Detection System detects attacks using signatures that carry malicious and harmful attacks. Signature-based IDS can be used to detect known attacks; on the other hand unknown attacks are detected trough Anomaly based IDS. Anomaly based IDS enables attack detection that has signatures which are not in the database of already available attack patterns.

Snort is open-source IDS solution which is not only used for detecting attacks but can be used for preventive actions too, for instance, as soon as attacks are detected connection can be blocked immediately to stop entering of any malicious and attacks to the network system. As a result Snort should be updated frequently because it has to be made familiar with new attacks and threats. Snort can be used for protection of network systems from any potential attacks or threats before they create any damage to network system.

VII. REFERENCES

[1] M. Ali. Aydin, A. Halim Zaim and K. Gokhan Celyan, "A hybrid intrusion detection system design for computer network security", Computer and Electrical Engineering 35(2009) 517-526.

[2] Qingqing Zhang, Hongbian Yang, kai Li and Qian Zhang, "Research on the intrusion detection technology with hybrid model", 2nd Conference on environmental science and information application technology, IEEE, 2010.

[3] Sumaiya Thaseen and Aswani Kumar, "Intrusion detection model using fusion of PCA and optimized SVM", IEEE, 2014.

[4] Divya and Surendra Lakra, "HSNORT: A Hybrid intrusion detection system using artificial intelligence with snort", International journal computer technology & application, Vol 4(3), 466-470, 2013.

[5] Vinod Kumar and Dr. Om Prakash Sangwan, "Signature based intrusion detection system using SNORT", International Journal of computer application & information technology, 2012.

[6] Natttawat Khamphakdee, Nunnapus Benjamas and Saiyan Saiyod, "Improving intrusion detection system based on snort rules for network probe attack detection", International conference on information and communication technology, IEEE, 2014.

[7] Kapil Wankhade, Sadia Patka and Ravinndra Thool, "An efficient approach for intrusion detection using data mining methods", IEEE, 2013.

[8] Mohammadreza Ektefa, Sara Memar, Fatimah Sidi and Lilly Suriani Affendey, "Intrusion detection using data mining techniques", IEEE, 2010.

[9] Matthew V. Mahoney, "Network traffic anomaly detection based on packet bytes", ACM, 2003.

[10] Matthew V. Mahoney and Philip K. Chan, "Learning nonstationary models of normal network traffic for detecting novel attacks", ACM, 2002.

[11] Matthew V. Mahoney and Philip K. Chan, "Learning Rules for Anomaly Detection of Hostile Network Traffic", Florida Institute of Technology, Melbourne, FL 32901.

[12] G. V. Nadiammai and M. Hemalatha, "Handling intrusion detection system using snort based statistical algorithm and semi-supervised approach", Research Journal of Applied Sciences, Engineering and Technology 6(16): 2914-2922, 2013.

[13] G. V. Nadiammai and M. Hemalatha, "Effective approach toward intrusion detection system using data mining techniques", Egyptian Informatics Journal (2014) 15, 37–50.

[14] Matthew V. Mahoney and Philip K. Chan, "PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic, Florida Institute of Technology", Melbourne, FL 32901.