Intrusion Detection System - False Positive Alert Reduction Technique

Manish Kumar[1], Dr. M. Hanumanthappa[2], Dr. T. V. Suresh Kumar[3]
[1]Asst.Professor, Dept. of Master of Computer Applications,
M. S. Ramaiah Institute of Technology, Bangalore-560 054, INDIA
E-Mail:- manishkumarjsr@yahoo.com
[2]Dept. of Computer Science and Applications,
Jnana Bharathi Campus, Bangalore University,
Bangalore -560 056, INDIA
[3]Professor & Head, Dept. of Master of Computer Applications,
M. S. Ramaiah Institute of Technology, Bangalore-560 054,
E-mail:- hanu6572@hotmail.com, hod_mca@msrit.edu

***Abstract*- Intrusion Detection System (IDS) is the most powerful system that can handle the intrusions of the computer environments by triggering alerts to make the analysts take actions to stop this intrusion, but the IDS is triggering alerts for any suspicious activity which means thousand alerts that the analysts should take care of it. IDS generate a large number of alerts and most of them are false positive as the behavior construe for partial attack pattern or lack of environment knowledge. These Alerts has different severities and most of them don't require big attention because of the huge number of the false alerts among them. Monitoring and identifying risky alerts is a major concern to security administrator. Deleting the false alerts or reducing the amount of the alerts (false alerts or real alerts) from the entire amount alerts lead the researchers to design an operational model for minimization of false positive alarms, including recurring alarms by security administrator. In this paper we are proposing a method, which can reduce such kind of false positive alarms.**

***Index Terms* - Intrusion Detection, False Positives, Alert Reduction**

I. INTRODUCTION

Intrusion detection is the process of monitoring computers or networks for unauthorized access, activity, or data modification, so that action may be taken to prevent or repair the damage later. Anderson [1] defined an intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to (i) Access information (ii) Manipulate information, or (iii) Render system unreliable or unusable. There are two basic types of intrusion detection system: Host-based and Network-based. Each has a distinct approach for monitoring, securing data and systems. Host-based IDS examine data on individual computers that serve as hosts, while network-based IDS examine data exchanged between computers. William Stallings [12] classified IDSs based on various parameters, Rule-based Detections and Statistical Anomaly Detection. Statistical anomaly detection systems are grouped into Profile based detections and threshold detection. Stefano Zanero [11] classified IDS based on concept of processing misuse detection or anomaly detection. IDS based on Anomaly detection create behavior model for the monitored infrastructure including its users. Any deviation from normal behavior, beyond defined threshold, marks the action as suspicious. Alternately, a set of signatures stored in a knowledgebase will be used by misuse detection IDS to identify intrusion attempts. Since IDSs (Intrusion Detection System) collect activities from the protected network and analyze them to generate alerts if there is an intrusion. These alerts will be usually saved in the log file based on the network packets stream.

A. IDS Alert Modes

The IDS triggers an alert if it is capturing an infected packet. SNORT which is an open source network intrusion prevention and detection system the alert can be written in two mode; either a fast mode alert or a full mode alert. The fast mode contains simple components which are time stamp, alert message, source IP address, destination IP address, source port and destination port. The full mode alert contains the fast mode components plus extra components such as length of the IP header and length of IP packet. The main difference between the two modes is printing the alert message and the packet header as in the full mode alert while the fast mode alert prints only the alert message

II. FALSE POSITIVES IN IDS

A. False Positive

False positive problem is mystery term that describes the situation where the IDS trigger alerts when there is a malicious activity in simple words (IDS makes a mistake) [5,6]. Organizing and dealing with the recorded logs and generated alerts by the security sensors such as the IDS, firewalls, packet filtering and servers are not easy job. Most of the organizations consider these alerts as a major problem. Since these sensors are independent so they will generate alerts and send it to the analyst party to analyze these alerts for understanding the nature of the intrusion using the provided tools, methods and techniques leading to reduce the false alerts rate and increase the attack detection rate. Even though, there are still weaknesses in these processes because of the quality of the input data, huge number of alerts with a plenty of false alerts will be the way of how any sensor works even when a harmless event accrued.

DOI: 01.IJNS.02.03.104

B. False Negative

The act of not detecting an intrusion when the observed event is illegal is defined as false negatives. False negative can also be defined as an action of IDS system that does not detect actual anomaly/misuse action and allows passing. Subject's normal behavior is the basis for the Anomaly detection, "any action that significantly deviates from the normal behavior is considered as intrusive". Therefore the normal behavior in IDS shall be defined explicitly. Stefano Zanero [11] proposed models for the evaluation of the IDS. More false positives are reported in anomaly detection systems while signature based systems report very low, but produce false negatives. J Snyder [4] states that "the target-based architectures will reduce false positives". False negatives also create a nuisance and issue of importance. Large number of new attacks will generate false negatives in misuse based systems, since there may not be any similar signature.

III. FALSE ALERTS REDUCTION

There is two different ways to study the false Alerts reduction either study the false alert reduction at the sensor level or after the detection on the log alert file.

A. False Alerts Reduction at the Sensor Level

False Positive alert was addressed by many studies using different techniques and methods like Mahmoud when he proposed solution to reduce the false alert rate by using fuzzy cognitive maps (FCM) which is a soft computing modeling techniques generated from the compensation of fuzzy logic and neural network. In this proposed solution he measures (availability, similarity, occurrence, relevancy, independent and correlation factors) then he assign an effect value for each one of the factors to estimate the total degree of abnormality per packet. Depending on the factor value the packet will be dropped or ignored. That if the packet is below malicious and if not it will be considered as real alert in the (FCM). The last step is to measure the (effect/influence) value and there is a degree from 0 to 1, while 0 means normal relation and 1 means high relation. This study shows that improving the detection deficiency will be by reducing the false alerts and increasing the detection accuracy at the sensor level [7]. Cheung used agents and data mining technology to give more accuracy when capturing the actual behavior of network traffic. There are three types of agents for the three data mining techniques, which are: (clustering, association rules and sequential association rules). The number of agents will be different in both training and detection process, the clustering-base agents extracts properties from traffic in terms of frames and tries to make the normal traffic in the training stage. If the unknown traffic is far from the normal cluster it is classified as an attack. The association rule-based agent finds out the relationship between features selected and traffic property in the training phase. The agents will capture the rule of selected features and in the detection phase, the agents count the rules of each connection to be matched, when the frequency is less than the threshold it classified as an attack. The sequential association rule-based agents (in the training phase) capture the sequential patterns in network traffic dialog to assist the association mining process. In the detection phase the agents tests the abnormal connections matched within the (packet/time) frame. If it is larger than the threshold, it will be declared as an attack. In the decision maker stage they check if the alert is generated from both clustering based and rule based to declare an attack, else it will be a false alert from one side which will be eliminated by the other side [3]. Pi-Cheng made an optimization of the rule selection and the attack identification in attack analysis, by proposing a scenario-based approach to correlate malicious packets and to select intrusion-detection rules in intelligent way. The scenario-based approach is based on how to choose rules to be tested according to the threats detected and attack scenarios identified at the moment of the attack. Instead of being tested simply according to some predetermined order, depending on a dependency graph which is a direct acyclic graph, the main idea of this approach is to classify rules in the rule database in terms of threats and thus associate the rules with a dependency graph [9].

B. False Alerts Reduction after the Detection Level

Abdulrahman reduced the false alerts rate by classifying the alerts sequences into two patterns classes, continuous and discontinuous. While the continuous patterns represent the real alerts the discontinuous patterns reflect the sequences mixed with noisy data. According to this study the alerts sequences may contain a several continuous sub-sequences. Ignoring such patterns will lead to miss significant patterns. Reducing the false alerts here will be after denoting all alerts in one sequence Xi by the length m, Xithen will be expanded to a number of sequential patterns. These patterns generated by extracting all possible combinations [2]. Njawa proposed (IAQF) intrusion alert quality framework to reduce false alerts by measuring five quality criteria scores of the alerts (correctness, accuracy, reliability and sensitivity). In there study they calculated a weight for each quality criteria score and depending on the total score they use the five threshold that they implement to classify the alert as a real alert or false alert, where these five thresholds can be modified according to the environment. IAC intrusion alert correlation was classified in this study into two levels, the low-level alert preparation and the high-level alert operation. The low-level alert preparation is based on Intrusion Alert Quality Framework (IAQF), alert collection, Host / Network information gathering, alert quality criteria scores measurement and normalize alert into (IDMEF) format [8]. The high level was based on Gorton proposed solution in which he divided generic intrusion alert correlation procedure into 4 generic tasks (Correlation, Filtering, Analysis and Attack Scenario Building). Other approaches of reducing false alerts are based on data mining methods which provide automatic intrusion detection capabilities by mining knowledge from audit data to characterize normal and abnormal user behavior. Wenke propose a data mining framework for constructing intrusion detection models to mine system audit data to be consistency and useful patterns and to use the set of relevant system features presented in the patterns to compute the

DOI: 01.IJNS.02.03. 104

learned classifiers to recognize anomalies and known intrusions in order to make the classifiers effective for the intrusion detection models. Another approach based on using data mining methods to build automatic intrusion detection systems based on anomaly detection by applying mining algorithms to audit data so that abnormal intrusive activities can be detected by comparing the current activities with the characterized normal system activities profile [7].

IV. PROPOSED MODEL FOR FALSE POSITIVE ALARM MINIMIZATION

The best way to secure the infrastructure and to get rid of the false positives is to review the configurations and update the security patches, update the behavior signatures [10]. Complete elimination of false positives can be achieved only when all possible threats to be listed and signature/ behavior prepared and deployed in IDS. However, it is not practically possible to list all feasible threats; therefore alternate methods are necessary to address false negatives or false positives. The present work is done using a campus network spread in multiple buildings. Snort IDS is used for the evaluation. Definitions proposed in the model are:

1 Let S_a be the set of total alarms generated by snort.

2 Let T_a be the set of total alarms by partially or exactly matching the signatures in the current environment.

3 Let C_a be the set of alarms that are exactly matched signatures. Based on the signature definitions in snort IDS, hence

$$C_a \subset T_a$$

4 Let X_a be the set of alarm, which was generated for the suspected intrusion and whose source IP address was spoofed.

$$X_a \subset T_a$$

(Note: - In most of the Intrusion case, the source IP address is spoofed IP address. Hence if the alarm is generated for certain suspected intrusion whose source IP address is found spoofed, can be considered as a true positive alarm.)

5 The partially matched alarms (Fig:-1) are

$$P_a = T_a - C_a$$

6 Let F_p be the set of probable false positives in current environment.

7 The possible false positives shall be in partially matched signature alarms only. The exactly matched alarms C_a and X_a are true positives.

8 The set of possible false positives (Fig:-1) are

$$F_p \leq (P_a - X_a)$$

9 Minimization of false positives can be achieved if the partially matched alarms are reduced to zero, i.e.

$$F_p = P_a = 0$$

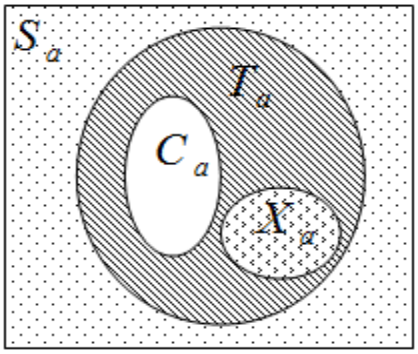

Figure 1:- False Positive Alarm ($P_a = T_a - C_a - X_a$)

CONCLUSIONS

This paper tries to review what the researchers had been done in the false alert reduction in IDS area. IDS generate a large number of alerts (false positives). Most of these alerts demand manual intervention from Administrator. Continuous monitoring of alerts and there by evolving a judgment for improving security is the major concern. The research presents approaches for minimizing the false positives. The proposed technique also consider the attack which is generated using a spoofed IP address . The false positive reduction can be in the sensor level or after the detection level, while at the sensor level can be considered as enhancing the detection method. So we believe that standardization is needed to clarify false positive reduction term. Finally, the IDS researchers still keep digging to find the most suitable method to reduce the false positive alert and response of attacks so they can be able to stop and prevent these attacks to reach the final stage.

REFERENCES

[1] Anderson, J P, Computer Security threat Monitoring and surveillance (Technical Report). Fort Washington,PA: James P Anderson Company, 1980.

[2] A. Alharby, H. Imai, IDS false alert reduction using continuous and discontinuous patterns, Computer Science, Springerlink 3531 (2005) 192-205.

[3] H. Debar, D. Curry, B. Feinstein, Intrusion detection exchange format, Internet draft, available online at: http://www.ietf.org/rfc/rfc4765.txt, 2009.

[4] J Snyder, Taking Aim: "Target–Based IDS Squelch Network Noise to pinpoint the alert you really care about". Information security Magazine, January 2004.

[5] K. Timm, Strategies to reduce false positives and false negatives in NIDS, Security Focus Article, available online at: http://www.securityfocus.com/infocus/1463, 2009.

[6] M.J. Ranum, False Positives: A User's Guide to Making Sense of IDS Alerts, ICSA Labs IDSC, 2003.

[7] M. Jazzar, A.B. Jantan, Using fuzzy cognitive maps to reduce false alerts in som-based intrusion detection sensors, in: Proceeding of the Second Asia International Conference on Modelling & Simulation, 2008.

[8] N. A. Bakar, B. Belaton, Towards implementing intrusion alert quality framework, in: Proc. First International Conference on Distributed Frameworks for Multimedia Applications (DFMA4'05), IEEE Computer Society, Washington, DC, USA, 2005, pp. 198-205.

DOI: 01.IJNS.02.03.104

[9] P.C. Hsiu; C.F. Kuo, T.W. Kuo, E.Y.T Juan, Scenario based threat detection and attack analysis, International Carnahan Conference on Security Technology, 2005, pp. 279-282.
[10] "Stephen Northcutt & Judy Novak", (2003) Network Intrusion Detection (3rd .ed), Indianapolis: New Riders Publishing. P79, P401-404
[11] Stefano Zanero (2007), "Flaws and Frauds in the Evaluation of IDS.IPS Technologies", first accessed on 21.09.07, http:// www.first.org/conference /2007/papers/zanero-stefano-paper.pdf, 2007.
[12] William Stallings, "Cryptography & Network Security Principles & Practices", Intrusion Detection (pp. 571), 2003, 3rd Edition.

DOI: 01.IJNS.02.03.104