Journal of Computer Science, 9 (4): 421-426, 2013
ISSN 1549-3636

doi:10.3844/jcssp.2013.421.426 Published Online 9 (4) 2013 (http://www.thescipub.com/jcs.toc)

Research Proposal: An Intrusion Detection System Alert Reduction and Assessment Framework Based on Data Mining

[1]Karim Al-Saedi, [1]Selvakumar Manickam, [1]Sureswaran Ramadass, [2]Wafaa Al-Salihy and [1]Ammar ALmomani

[1]National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
[2]School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia

Received 2012-06-14, Revised 2012-12-21; Accepted 2013-05-08

ABSTRACT

The Intrusion Detection System (IDS) generates huge amounts of alerts that are mostly false positives. The abundance of false positive alerts makes it difficult for the security analyst to identify successful attacks and to take remedial actions. Such alerts to have not been classified in accordance with their degree of threats. They further need to be processed to ascertain the most serious alerts and the time of the reaction response. They may take a long time and considerable space to discuss thoroughly. Each IDS generates a huge amount of alerts where most of them are real while the others are not (i.e., false alert) or are redundant alerts. The false alerts create a serious problem for intrusion detection systems. Alerts are defined based on source/destination IP and source/destination ports. However, one cannot know which of those IP/ports bring a threat to the network. The IDSs' alerts are not classified depending on their degree of the threat. It is difficult for the security analyst to identify attacks and take remedial action for this threat. So it is necessary to assist in categorizing the degree of the threat, by using data mining techniques. The proposed framework for proposal is IDS Alert Reduction and Assessment Based on Data Mining (ARADMF). The proposed framework contains three systems: Traffic data retrieval and collection mechanism system, reduction IDS alert processes system and threat score process of IDS alert system. The traffic data retrieval and collection mechanism systems develops a mechanism to save IDS alerts, extract the standard features as intrusion detection message exchange format and save them in DB file (CSV-type). It contains the Intrusion Detection Message Exchange Format (IDMEF) which works as procurement alerts and field reduction is used as data standardization to make the format of alert as standard as possible. As for Feature Extraction (FE) system, it is designed to extract the features of alert by using a gain information algorithm, which gives a rank for every feature to facilitate the selection of the feature with the highest rank. The main function of reduction IDS alert processes system is to remove duplicate IDS alerts and reduces the amount of false alerts based on a new aggregation algorithm. It consists of three phases. The first phase removes redundant alerts. The second phase reduces false alerts based on threshold time value and the last phase reduces false alerts based on rules with a threshold common vulnerabilities and exposure value. Threat score process of IDS alert system is characterized by using a proposed adaptive Apriori algorithm, which has been modified to work with multi features, i.e., items and automated classification of alerts according to their threat's scores. The expected result of his proposed will be decreasing the number of false positive alert with rate expected 90% and increasing the level of accuracy compared with other approaches. The reasons behind using ARADMF are to reduce the false IDS alerts and to assess them to examine the threat score of IDS alert, that is will be effort to increase the efficiency and accuracy of network security.

Keywords: False Positive, Reduction Alert, Association Rules, Aggregation Alert, Assessment Threat

Corresponding Author: Karim Al-Saedi, National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia11800 USM, Penang, Malaysia

1. INTRODUCTION

Recently, many institutions have been experiencing a heavy usage of networks within their systems. However, the broad technological expansion that accompanied these networks has brought along various threats to them. These threats included many kinds of malicious programmes that affect the efficiency of networks, such as the transmission of data through the network or data that can be accessible via the network. This issue has urged researchers to improve and develop new techniques to explore and contain such threats (Al-Saedi *et al*., 2011).

This gives rise to cyber security. Cyber security is a branch of computer technology known as information security. It can be applicable to computer systems and networks within the sectors of communication (email, cell phones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards) and medicine (equipment, medical records). Cyber security involves protecting the system information by effectively preventing, detecting and responding to attacks (Tjhai *et al*., 2010).

Many types of risks with various intensities can attack the computer systems and networks. As far as the serious ones are concerned, these embedded viruses can cause the following damages: delete one's entire system, allow someone to penetrate someone else's system, alter files, attack other computers from someone's computer, allows someone to steal another person's credit card information and make unauthorised purchases. Unfortunately, there is no one hundred percent guarantee that these threats will not happen even if someone is extremely cautious (Xu and Ning, 2008).

Intrusion Detection Systems (IDSs) are commonly recognised elements within the field of internet security arsenal. penetration and threats are usually made by hackers to get into the desired network or computer system or to attack, hit or control the victim either by sending a virus, or DDoS, worms, Bot (Elshoush and Osman, 2011; Tjhai *et al*., 2010).

It is an integral component of an in-depth architecture that provides a complete computer network security defence. It monitors packets to recognize their intrusive behaviors. An alarm is raised once an intrusive event is detected, giving the security analyst the opportunity to react promptly against any such threat. Most of the outputs of these systems are alerts. These alerts contain a high proportion of unsuccessful alarms, known as false alerts, which require careful assessment to identify and reduce the unsuccessful ones (Porres and Fernandez, 2008; Njogu and Jiawei, 2010). Intrusion Detection System assists taking decisions that determine which security resources can be used in the network. It also helps one know about the external and internal threats facing the network. The intrusion detection system is unable to prevent threats; however, it collects information when threats are encountered. The collected information can be used to correct mistakes and fill gaps in the security system (Maggi *et al*., 2009; Xu and Ning, 2008).

Intrusion Detection System comes in the form of software or hardware. In both cases, it is used to monitor network traffic. In network traffic, traffic information within the network does not through the IDS device; instead, the latter monitors traffic through a network interface. When Intrusion Detection System detects a suspicious activity within the network, it sends an alert to the network administration about the potential threat that might be an intrusion attempt (Elshoush and Osman, 2011) Consider **Fig. 1**.

1.1. Related Works

Intrusion detection system is used to generate alerts, those alerts can be classified into false positives and true negatives. Kruegel and Robertson (2004) developed a plug-in to add an alert processing pipeline to IDS Snort. Root-cause analysis was proposed by (Julisch and Dacier, 2002) to identify the root causes that trigger false positives and remove the alert generated. However, this method cannot be controlled. Fixing a problem is also very expensive, thus its impracticality. Pietraszek (2004) adopted a system that worked faster and an effective rule learner, requiring no human feedback and background knowledge. The disadvantage of this system is that it requires infinite growth size to train the system during its lifetime; thus, the system is inefficient. To perform alert verification using the Nessus vulnerability scanner. A statistical causality analysis correlation approach was proposed by (Lee and Qin, 2005). This approach was based on statistical analysis and time series to develop attack scenarios. The authors proposed a clustering technique to aggregate the alerts to be represented as one hyper alert in each cluster based on time intervals. The objective of their approach was to reduce the amount of alerts and obtain alert prioritization to identify the important alerts. The drawback of this approach is also its incapacity to remove redundant alerts and its inflexibility to choose the alert features. A robust alert cluster mechanism to reduce false alerts was proposed by (Njogu and Jiawei, 2010). This mechanism calculates the similarities of verified alerts using distance among the new alert features.

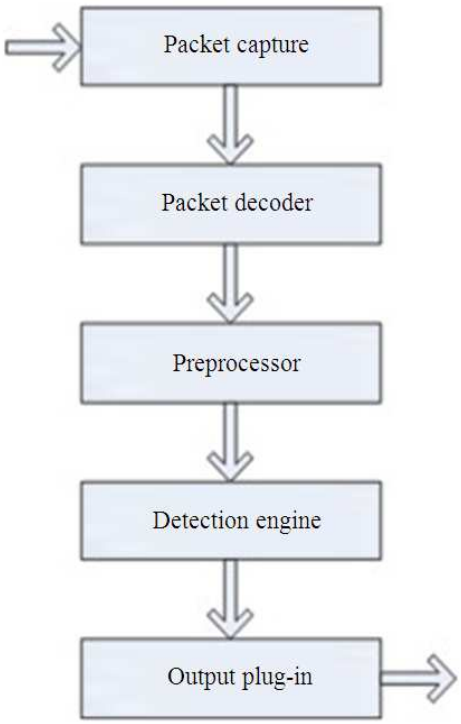

Fig. 1. Intrusion Detection System (IDS) (Deng and Purvis, 2011)

The present research proposed a new framework called IDS Alert Reduction and Assessment Based on Data Mining (ARADMF), which depends on the IDS alert database obtained from the network by leveraging IDS Snort. This framework is based on three systems: Traffic Data Retrieval and Collection Mechanism System, Reduction IDS Alert Processes System and Threat Score Process of IDS Alert System. The first system operates mainly develops a mechanism to save IDS alerts, extract the standard features as intrusion detection message exchange format and save them in DB file (CSV-type) and extracts the features.

The main function of second system is to remove duplicate IDS alerts and reduce the amount of false alerts based on a new aggregation algorithm. The last system is responsible for extracting the threat score of the alert features, generating the rules and threat score of alert as well.

1.2. Statement of the Problem

The IDS generates huge amounts of alerts that are mostly false positives. The abundance of false positive alerts makes it difficult for the security analyst to identify successful attacks and to take remedial actions. Such alerts have not been classified in accordance with their degree of threats. They further need to be processed to ascertain the most serious alerts and the time of the reaction response. They may take a long time and big space to discuss thoroughly; therefore, the statement of the problem can be summarized by the following points:

Each intrusion detection system generates a huge amount of alerts where most of them are real while the others are not (i.e., false alert) or are redundant alerts. The false alerts create a serious problem to intrusion detection systems. Alerts are defined based on source/destination IP and source/destination Ports. However, one cannot know which of those IP/ports bring a threat to the network. The IDSs' alert are not classified depending on their degree of threat. It is difficult for the security analyst to identify attacks and take remedial action for this threat. So it is necessary to assist in categorizing the degree of threat, by using data mining techniques.

1.3. Research Objective

The objective of this proposal is to present a framework that reduces IDS alerts and assesses its threat. To achieve the above objectives, the following procedures will be taken into account:

- Leveraging information gain ratio algorithm to extract the best features of IDS alerts for the purpose of assessing the alerts
- Building a new aggregation IDS alert algorithm to reduce the amount of false positive alerts and to get rid of the alert redundancy
- Developing a multi features based on apriori algorithm to find the threat degree of multi features and to assess the threat scores of IDS alert
- Building a visualization engine that involves discovered-based knowledge to assist network engineers in making an appropriate decision

1.4. Research Motivations

- The increase in interest over the implementation of Intrusion Detection System (IDS) in computer networks security
- The huge amounts of alerts which are mostly false alerts generated by IDS, contributing negatively in system complexity and consequently increase the ambiguity of assessment decision maker for alerts

- More investigation on implementing the data mining for IDS especially to deal with the huge data for such systems

1.5. Expected Contribution

The lack of distinction between false alerts and real alerts has resulted in the need to conduct an operation process to remove the false alerts. Furthermore, the real alerts need to be classified in accordance with their degrees of threat. Consequently, the current proposal will be dedicated to present fourth main contributions, as illustrated below:

- The information gain ratio algorithm, which is leveraging to extract some of the best features in alerts assessment
- A new algorithm, which is developed to reduce false alerts and their redundancy
- An adaptive apriori algorithm to assess the threat scores of IDS alert which comprises of

Involves mining the frequent itemsets of the IDS alert features. The adaptive apriori algorithm scans the database only once. It loads the frequent items, i.e., 1-itemsets and their tidlists and then generates all frequent itemsets from these 1- itemsets without re-scanning the database.

Generate association rules for features selected and calculate the seriousness score for those features based on these rules (Output of A). Each implication will be associated with a degree of correlation between the right hand side feature set and the left hand side feature set according to users' predefined threshold.

Automated IDS alerts based on calculations of the threat score of each alert by leveraging new formula.

The analysis outcome is intuitively visualized to provide the administrator with a better decision support mechanism.

1.6. Research Methodology

The following are the three main phases of the present research framework:

1.7. Traffic Data Retrieval and Collection Mechanism Systems

This phase deals with alerts data base by using two modules. The first module is a Detection Message Exchange Format (IDMEF) which is responsible for receiving IDS alerts from IDS and save them in a text file and extracts features from IDS alert file and saves them to a DB file (CSV-type). This module has two main components: Procurement of IDS Alerts and Field Reduction and Data Standardization.

The second module is called Feature Extraction (FE). It is designed to extract the best features of alert by using a gain information algorithm, which gives a rank for every feature to facilitate selecting the feature with the highest rank.

1.8. Reduction IDS Alert Processes System

This phase will be built over a proposed new aggregation alert algorithm and it will be done in three stages. The first stage removes any redundant alert based on the similarity of the alert features. The second stage also removes the redundant alert based on similarity of the alert features with threshold value which gives more accuracy result. The final stage of algorithm proposes to remove the false alert based on rules prepared for this purpose.

1.9. Threat Score Process of IDS Alert System

It has two main components: the generating featuresets and the generate rules featuresets and auto threat score. The generating featuresets is characterized by using a proposed algorithm; Adaptive Apriori Algorithm (AA). AA has been modified to its ability work with multi features, i.e., items. The advantage of this algorithm is being accurate when the confidence degree of association rule is extracted. This feature has been exploited to find the correlations between Alert Features, get the threat score of features and to extract the rules needed in forecasting. The generate rules featuresets and auto threat score based on using Adaptive Rule Generation Algorithm (ARG). ARG it has been developed and enhanced to its ability to automate calculate the threat score of features after generate rule and automated classification of alerts.

1.10. Proposed Framework

The proposal framework explained in this chapter contains three systems: Traffic data retrieval and collection mechanism system, reduction IDS alert processes system and threat score and automated classification of IDS alert system. **Figure 2** depicts the ARADMF methodology.

The traffic data retrieval and collection mechanism systems contain Intrusion Detection Message Exchange Format (IDMEF), they work as procurement Alerts, field reduction as data standardization to make the format of alert as standard as possible. As for Feature Extraction (FE) system it is designed to extract the features of alert by using a gain information algorithm, which gives a rank for every feature to facilitate selecting the feature with the highest rank.

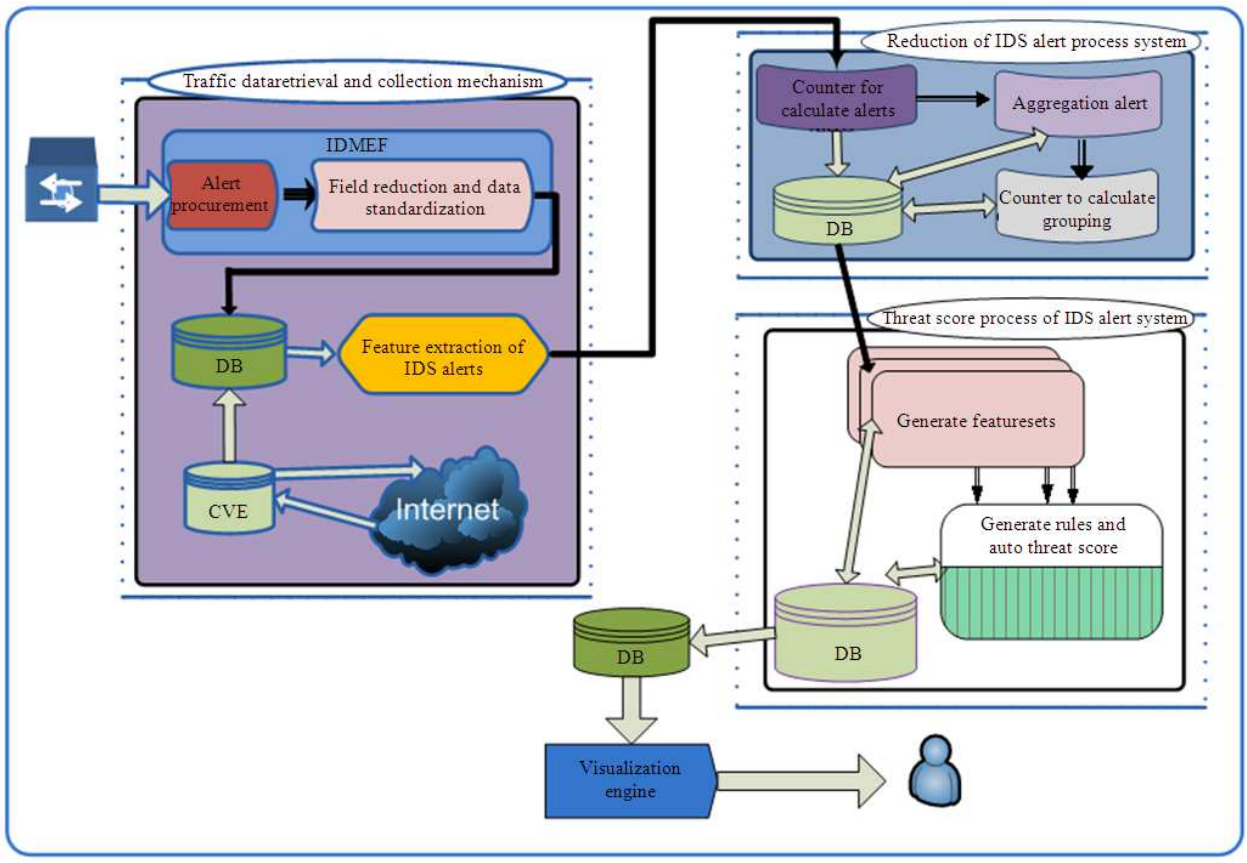

Fig. 2. An IDS Alert Reduction and Assessment Framework Based on Data Mining (ARADMF)

The main function of reduction IDS alert processes system is to Reduce False Alert (RDRFA). This algorithm aims to remove all redundant alerts and reduce them as well.

The third system, the seriousness IDS alert process system, is characterized by using the adaptive Apriori algorithm, which has been modified to increase the speed factor, work multi items and automated classification. The advantage of this algorithm is being accurate when the confidence degree of association rule is extracted.

This feature has been exploited to find the correlations between alert features, get the values of features seriousness and to extract the rules needed in forecasting. The final stage is the automated IDS alert classification. This stage has been designed to classify the IDS Alerts, based on a new Formula dedicated for this purpose. The formula embeds calculating the degree of the seriousness of threats and the value of this degree within the range (1-10). This formula is based on the outcomes of the Seriousness items stage and on the value of CVE.

2. CONCLUSION

This proposal proposes a new framework called An Ids Alert Reduction and Assessment Framework Based on Data Mining (ARADMF). Our framework expect to reduce the false positive alerts and to get rid of the alert redundancy, also to find the threat score of features to assessment the threat score of IDS alerts. This to increase the efficiency of network security and to increase it is accuracy level.

3. REFERENCES

Al-Saedi, K.H., H. Al-Khafaji, A. ALmomani, S. Manickam and S. Ramadass, 2011. An approach to assessment of network worm detection using threatening-database mining. Aus. J. Basic Applied Sci., 5: 2676-2683.

Deng, J.D. and M.K. Purvis, 2011. Multi-core application performance optimization using a constrained tandem queueing model. J. Netw. Comput. Appli., 34: 1990-1996. DOI: 10.1016/j.jnca.2011.07.004

Elshoush, H.T. and I.M. Osman, 2011. Alert correlation in collaborative intelligent intrusion detection systems-A survey. Applied Soft Comput. J., 11: 4349-4365. DOI: 10.1016/j.asoc.2010.12.004

Julisch, K. and M. Dacier, 2002. Mining intrusion detection alarms for actionable knowledge. Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Jul. 23-26, ACM Press, New York, USA., pp: 366-375. DOI: 10.1145/775047.775101

Kruegel, C. and W. Robertson, 2004. Alert verification: Determining the success of intrusion attempts. Proceedings of the 1st Workshop the Detection of Intrusions and Malware and Vulnerability Assessment, (DIMVA' 04), pp: 1-14.

Lee, W. and X. Qin, 2005. Statistical causality analysis of infosec alert data. Massive Comput., 5: 101-127. DOI: 10.1007/0-387-24230-9_4

Maggi, F., M. Matteucci and S. Zanero, 2009. Reducing false positives in anomaly detectors through fuzzy alert aggregation. Inform. Fusion, 10: 300-311. DOI: 10.1016/j.inffus.2009.01.004

Njogu, H.M. and L. Jiawei, 2010. Using alert cluster to reduce IDS alerts. Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology, Jul. 9-11, IEEE Xplore Press, Chengdu, pp: 467-471. DOI: 10.1109/ICCSIT.2010.5563925

Pietraszek, T., 2004. Using adaptive alert classification to reduce false positives in intrusion detection. Rec. Adv. Intrusion Detection, 3224: 102-124. DOI: 10.1007/978-3-540-30143-1_6

Porres, I. and M.D.M. Fernandez, 2008. An Evaluation of current IDS. M.Sc Thesis, Department of Electrical Engineering, at Linkoping Institute of Technology, Sweden.

Tjhai, G.C., S.M. Furnell, M. Papadaki and N.L. Clarke, 2010. A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm. J. Comput. Securty, 29: 712-723. DOI: 10.1016/j.cose.2010.02.001

Xu, D. and P. Ning, 2008. Correlation Analysis of Intrusion Alerts. In: Intrusion Detection Systems (Advances in Information Security), Pietro, R.D. and L.V. Mancini (Eds.), ISBN: 0387772650, pp: 65-92.