A COMBINED APPROACH TO SEARCH FOR EVASION TECHNIQUES IN NETWORK INTRUSION DETECTION SYSTEM

Rutuja R. Patil[1], P. R. Devale[2]

[1]*Research Scholar, Department of Information Technology, Bharati Vidyapeeth Deemed, University College of Engineering, Pune, Maharashtra, India*
[2]*Professor, Department of Information, Technology, Bharati Vidyapeeth Deemed, Pune, Maharashtra, India*

Abstract

Network Intrusion Detection Systems (NIDS) whose base is signature, works on the signature of attacks. They must be updated quickly in order to prevent the system from new attacks. The attacker finds out new evasion techniques so that he should remain undetected. As the new evasion techniques are being developed it becomes difficult for NIDS to give accurate results and NIDS may fail. The key aspect of our paper is to develop a network intrusion detection system using C4.5 algorithm where Adaboost algorithm is used to classify the packet as normal packet or attack packet and also to further classify different types of attack. Apriori algorithm is used to find real time evasion and to generate rules to find intrusion These rules are further given as input to Snort intrusion detection system for detecting different attacks.

Keywords: *NIDS, Evasion, Apriori Algorithm, Adaboost Algorithm, Snort*

----------***----------

1. INTRODUCTION

Many established businesses have to maintain a huge important information and data. Security measures should protect this information from unauthorized access. The functioning of burglar alarm in the real world can be mapped to the working of IDS function in the digital world. The conflict between the attackers and IDS developers is never ending because the attackers keep on finding new ways to get access to the system, while system developers keep on finding new ways to restrict the attackers.

Intrusion is a technique where in an attacker tries to get unauthorised access into the system with wrong intention. Intrusion Detection systems (IDS) is a network security appliance that monitors network traffic as well as system activities to check for malicious activity. Intrusion Detection System can be categorized in two ways Network based (NIDS) and host based (HIDS) intrusion detection systems.

1.1 Network Based Intrusion Detection System

As the packets on the network are monitored in this system so it is called as Network Based IDS. Its motive is to check whether an attacker is trying to get access to the system. The analysis of the network traffic is done in order to check for various malicious actions.

These systems can be broadly classified into two major categories. These are mainly: i) Anomaly based NIDS (ii)Signature based NIDS. In this paper, we focus on Signature based NIDS.

1.2 Signature Based Intrusion Detection System

The signatures of the attacks are stored in the database A signature based IDS compares these signatures with the packets on the network. Many of the antivirus software detects malware in the similar fashion. However if a new threat is discovered it will require some time span to discover the signature of the threat [2]. This situation causes attackers to find new evasions over the signatures of these systems. The overall concept of intruder is to carry out attack in a way that the Intrusion Detection System should not be able to detect it as an attack.

Following is the simplified explanation of Evasion:
Let us consider 2 strings " malicious " and "anamalous "which represented as known malicious code. The entry to the system is prohibited when an IDS finds these strings in the request. However if " annamil " and "lousmousci" were part of a request, the system would not recognise it as malicious strings "malicious " and "anamalous " which are merged together and reconstructed in a new form and the attacker can get access to the system.

The IDS does not interfere and entry would be allowed. The effort of this project is to develop a framework that looks to find novel evasive techniques by analyzing NIDS behavior.

2. RELATED WORK

Methodology of Network Intrusion Detection Evasion system is described in several papers. In paper [2] the authors proposed the concept of evasion and concludes that the evasion will be successful if the implementation of NIDS differs from the endpoint implementation.

Fragroute is an evasion tool which intercepts, modifies, and rewrites the traffic which is routed for the specified host[Online]. It helps the attackers to bypass the signature matching on the NIDS.

In paper[5], prototype system IDSprobe is introduced which tests the accuracy of NIDS to detect and handle evasion attacks. Author of paper [7] introduces Split Detect approach where in he focuses on splitting the signature into pieces.By splitting the signature the attacker is forced to include at least one piece of information completely and then the abnormal behavior of packets can be identified.

In the article[10] Snort an open source ,cross platform, lightweight Intrusion detection system is introduced. The paper also tells about the different applications where snort can be used.

It is very difficult to find the patterns of network traffic behavior whether it is good,bad or anomalous. Data mining is the conventional solution for this. However in paper [11] author has discussed about the use of Genetic Programming for the above purpose. The author also focuses on the advantages of using Genetic Programming.

Author of the paper [13] discusses a combined approach of Decision Tree and Support Vector Machine to model IDS. The author concludes by proving that using the combined approach increases the detection accuracy and minimizes the computational complexity.

3. PROPOSED SYSTEM ARCHITECTURE

In this approach, KDD- 99 (Knowkedge Discovery and Data Mining) which is publicly available data set that contains information about network traffic is used. It is given as input to C4.5 algorithm using Weka tool to build NIDS. Weka tool is open source tool. C4.5 algorithm gives output as a Decision Tree.

Adaboost algorithm is used to classify the network traffic as normal or attack. It consists of 4 phases : data labeling, data mining, training and testing. Detection result and false alarm rate will then get displayed.

After this apriori algorithm is used to find real time evasion and will also will generate rules for detecting attacks. After creating these rules, the rules are then passed to snort. Snort is an open source IDS. Snort will check for the rules and accordingly give the output whether it Is evasion or attack detection. Figure 1 shows the block diagram of NIDS.

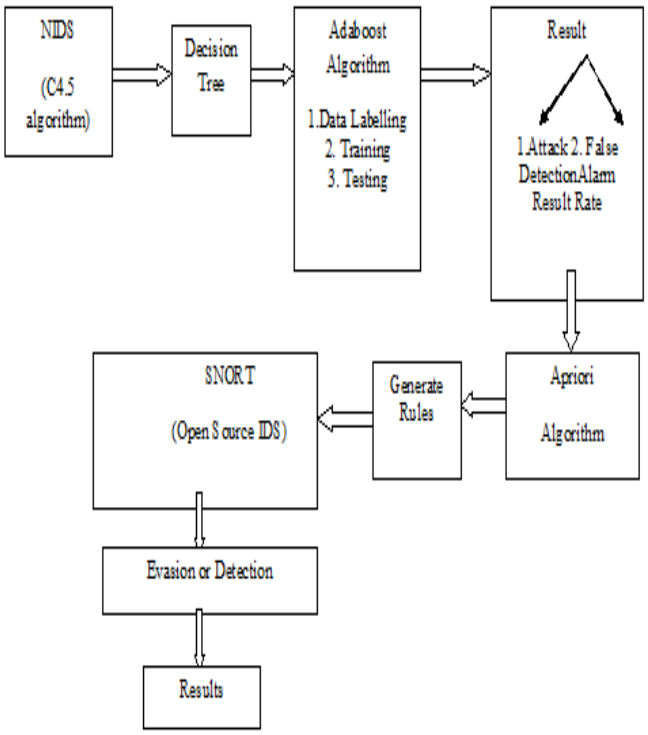

Fig 1: Architecture of NIDS System

4. PROPOSED APPROACH AND IT'S MODULES

4.1 Generation of Decision tree

In this project work, we take into consideration KDD dataset. KDD has data as network traffic sessions which is captured at different hours of a day. The traffic contains both normal and attack traffic. In the project we have taken into consideration only !0% traffic of the original KDD data set, the traffic is then processed to convert the output into binary (i.e. normal or intrusion) so that the non-numerical fields are normalised. Weka tool [15] is used to obtain the C4.5 based NIDS. C4.5[16] algorithm generates Decision tree. Some attribute is taken as base to generate the Decision Tree, this attribute is given some weight and will be used to further classify. The type of attack will be represented by leaf node of the decision tree. C4.5 algorithm uses the concept of Entropy and Information Gain to construct a Decision Tree.

To build a decision tree top-down approach is used which means root node is found out first. C4.5 uses entropy to find out samples with similar values that is to calculate homogeneity of samples.

4.2 Classification of Attacks using Adaboost Algorithm

In second module the. Adaboost algorithmis used for classification of attack packets. It has 4 phases namely Data labeling, data mining, training and lastly testing. In Data labelling phase the normal packet are labelled as +1 value and attack packet is labelled as -1 at the end which will be

the last attribute of TCP packet. Some features are extracted from data mining phase. Then the testing of the created NIDS is done to check for its accuracy. Adaboost algorithm differentiates the traffic into 4 types of attacks DOS, U2R, R2L, probe and normal packet. The output of this module is Detection rate and false alarm rate.

4.3 To find Real Time Evasion using Apriori Algorithm

For real time evasion NIDS is created using Apriori algorithm. Different sessions of attacks are given as input to Apriori algorithm. According to support and confidence value ,rules are generated by apriori algorithm. These rules are given to snort which is open source NIDS. When attack is generated for which signature is stored in snort, it generate alarm. After that we show evasion over NIDS by changing some fields of it. If NIDS failed to generate alarm means evasion is successful. So we found out different types of evasion.

4.4 Comparison of Results:

Comparing Multilayer Perceptron (MLP) algorithm results with Adaboost algorithm results MLP gives more accurate results and minimum false rate compared to same.

5. EXPERIMENTAL RESULTS

5.1 Weka Explorer

KDD-99 cup data set which contain attack and normal packet attack in .arff format is given as input to C4.5 algorithm through weka tool.

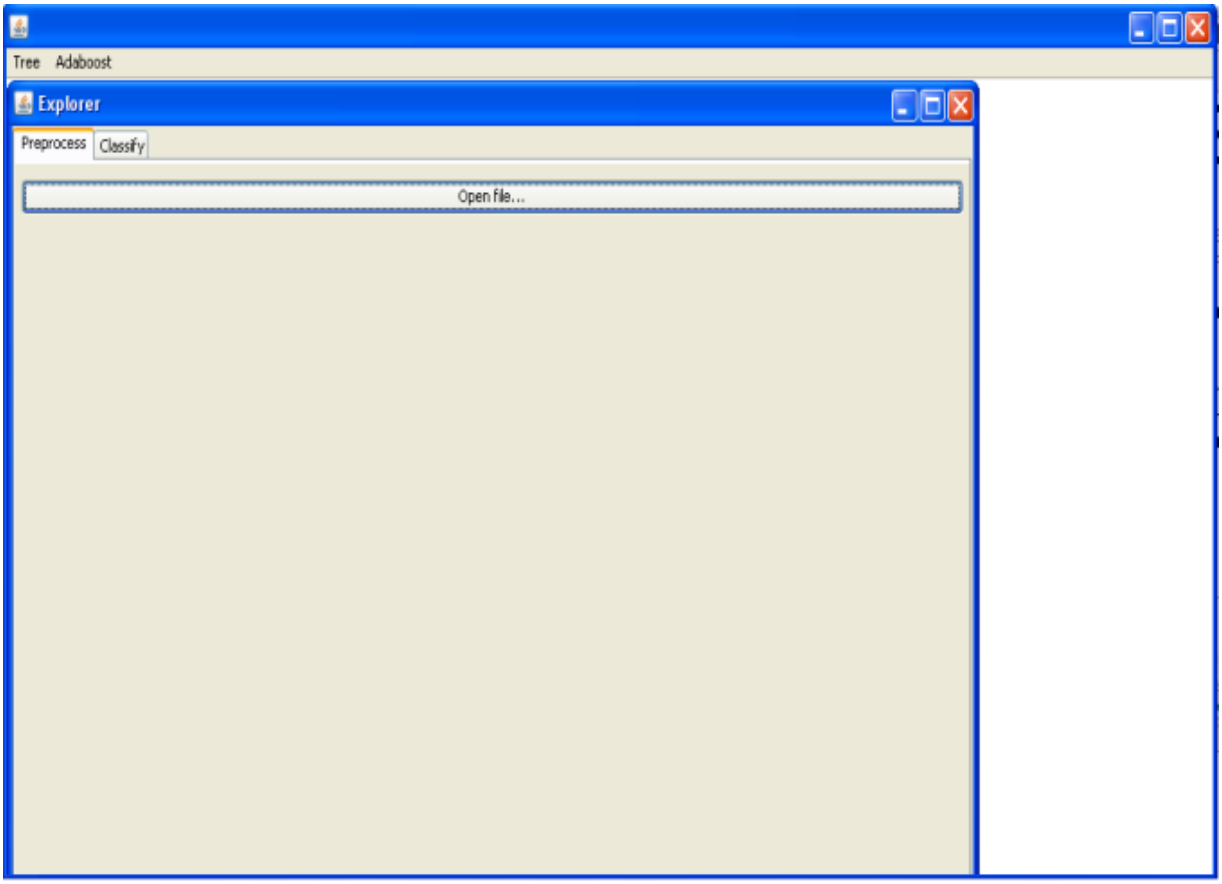

Fig 2: Weka explore to open dataset file

From Weka explorer we can select the algorithm. Here C4.5 or J48 algorithm is selected.From that selected algorithm the attacks are classified and accordingly a decision tree is generated. Division of attacks are done according to some value. Nodes are attribute by which classification is done and leaf nodes are attack names.

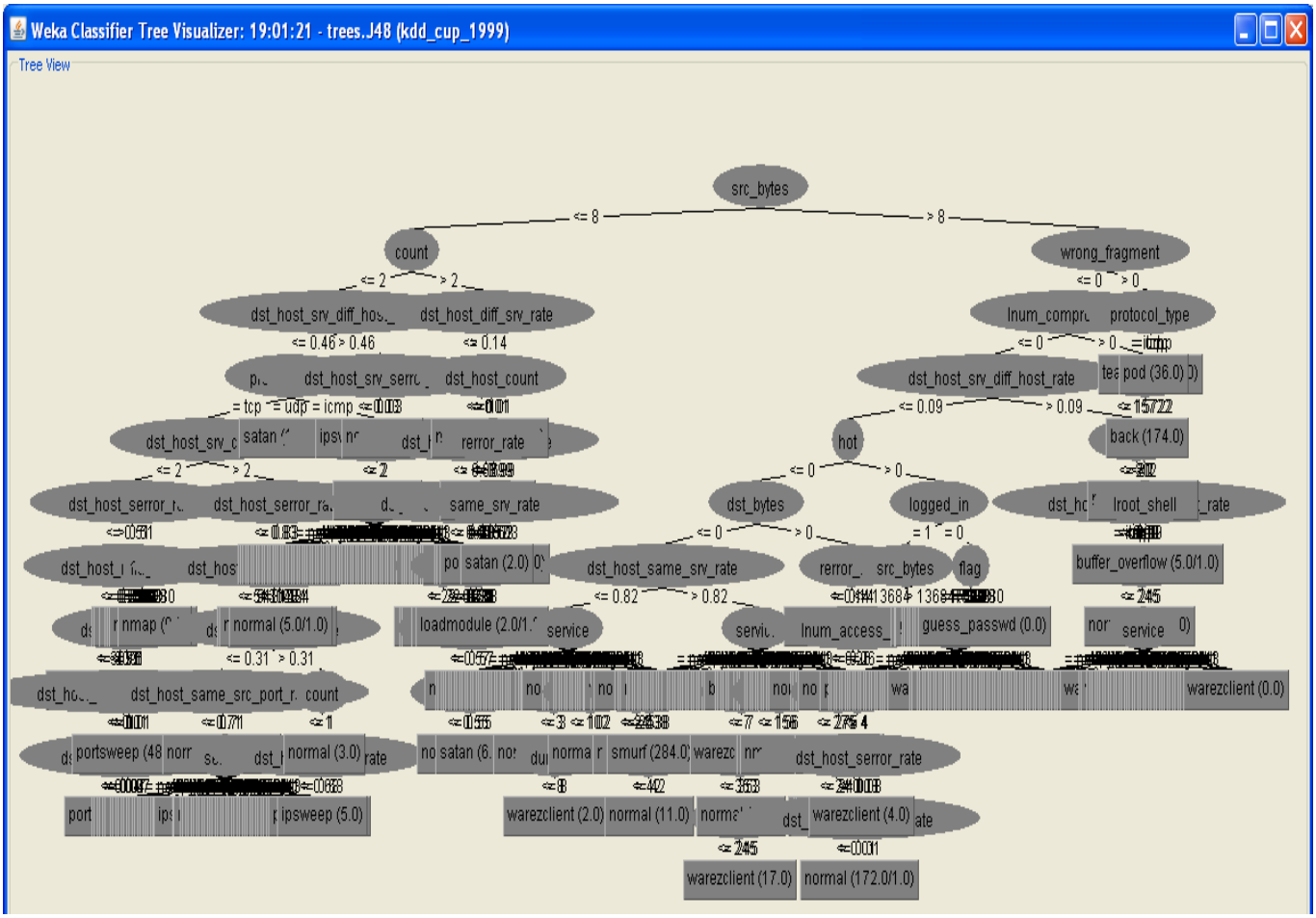

Fig 3: Visualization of C4.5 algorithm output in tree manner

5.2 Adaboost Algorithm

It is a classification algorithm. This algorithm works along with other algorithms for generating superior results. Here attacks are classified into 5 types DoS, Probe, R2L, U2R, normal Adaboost algorithm has 4 states labelling, data mining, training, testing. After testing with other datasets accuracy is calculated by input and output count. Input count is number of total attacks of that type and output count is number of attacks that are classified correctly by NIDS.

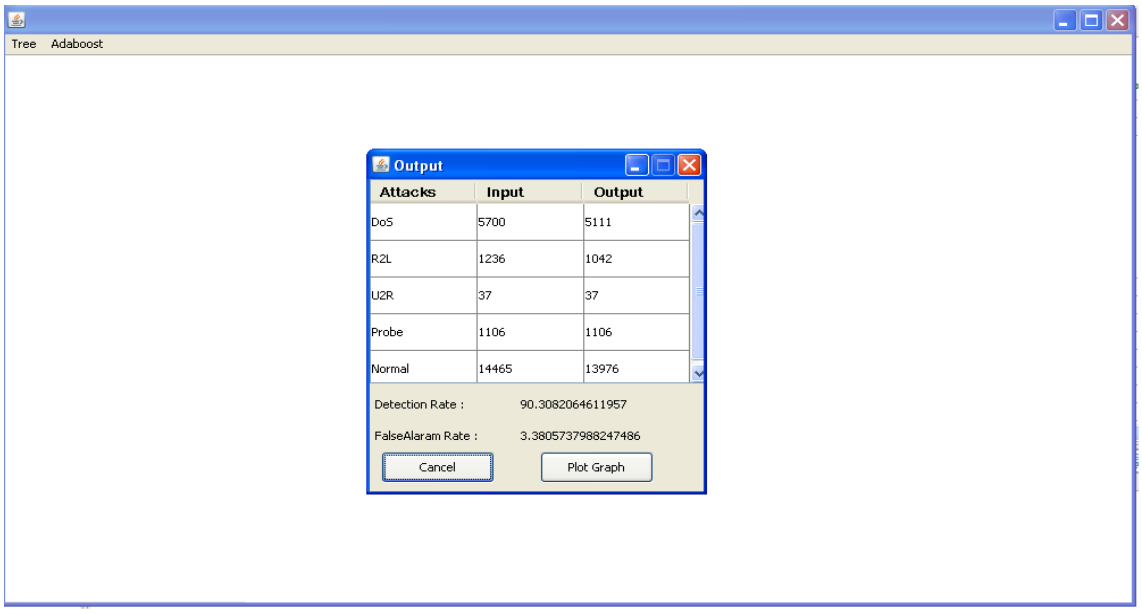

Fig 4: Adaboost output -classification of attacks, detection rate and false alarm rate

5.3 Apriori Algorithm

A real time evasion can be shown by apriori algorithm. We can select the file which contains attack sessions as input to apriori algorithm. From the GUI we can select support and confidence values. Rules are generated by apriori algorithm by trying different combination of attacks. Their support and confidence values are checked.

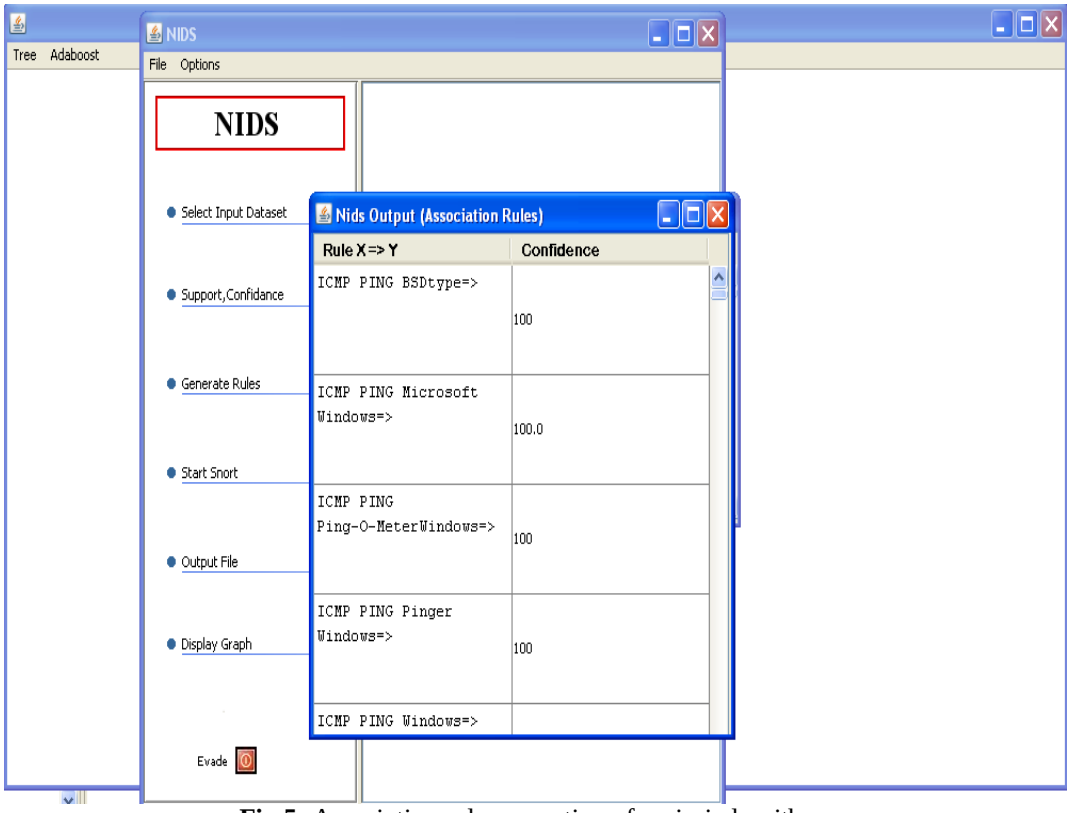

Fig 5: Association rule generation of apriori algorithm

4. Snort Output

The rules are given to snort. If the intruder generates the same attack for that a signature is stored in snort, snort generates alert messages.

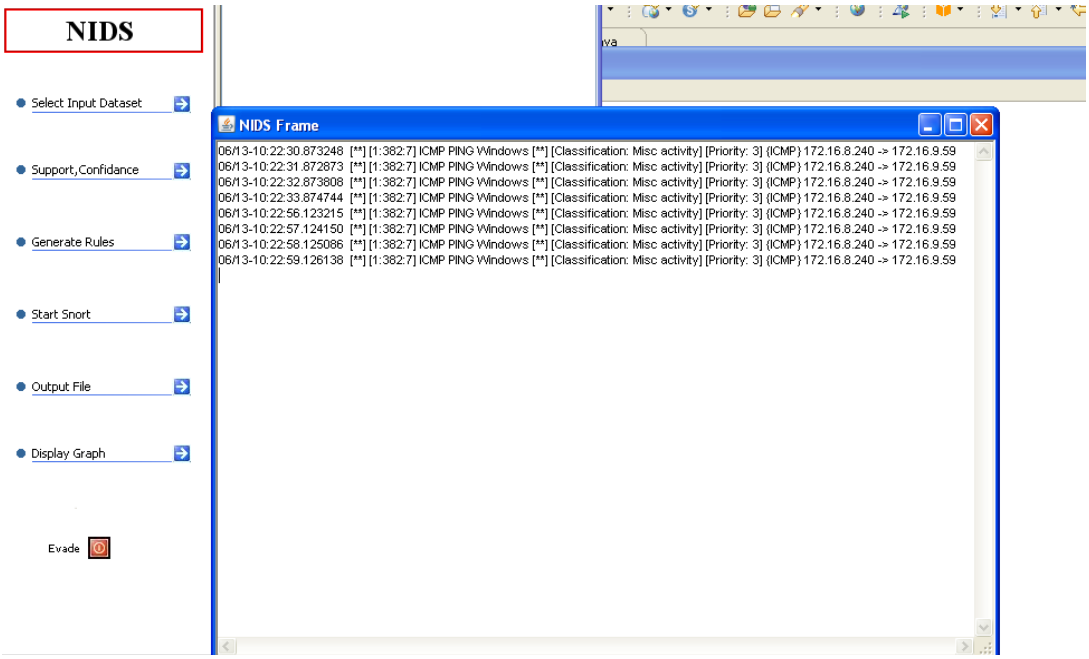

Fig 6: Alert message generated by snort on intrusion

6. CONCLUSION

Currently, NIDS are prepared to detect a huge variety of attacks. If we consider Snort it takes into account the possibility of being evaded with the techniques. However, they are not prepared to find new evasive forms that can appear. Here in this work we present a proof of concept showing how to perform detection and evasion in NIDS using publicly available datasets KDD-99.

In this dissertation we put forward a structure to search for evasions over a given NIDS. This model shows how the network data is classified by NIDS. We have shown the effectiveness and detection rate increases when using NIDS based on Adaboost algorithm. A real time evasion and detection is shown by NIDS based on Apriori algorithm which generates rules. Once this model is obtained, some fields of the packets can be changed and we can look for evading the NIDS detection. By this we can analyse different pattern of evading systems. Thus an environment to check the evasion of necessary attacks is successfully created..

REFERENCES

[1]. R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems", 800-31, 2001

[2]. T. H. Ptacek and T. N. Newsham, "Insertion, evasion and denial of service: Eluding network intrusion detection," Technical report, 1998.

[3]. S. Pastrana, A. Orfila, A. Ribagorda, “A Functional Framework to Evade Network IDS”,IEEE xplore, System Sciences (HICSS), 2011 44th Hawaii International Conference.

[4]. D. Son. (2002) Fragroute. [Online] http://www monkey.org/~dugsong/fragroute/

[5]. L. Juan, C. Kreibich, C.-H. Lin, and V. Paxson, "A Tool for Offline and Live Testing of Evasion Resilience in Network Intrusion Detection Systems," in DIMVA '08: Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Paris, France, 2008, pp. 267-278.

[6]. D. Watson, M. Smart, R. G. Malan, and F. Jahanian, "Protocol scrubbing: network security through transparent flow modification," IEEE/ACM Transactions on Networking, vol. 12, pp. 261--273, 2004.

[7]. G. Varghese, J. A. Fingerhut, and F. Bonomi, "Detecting evasion attacks at high speeds without reassembly," in SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, Pisa, Italy, 2006, pp. 327--338.

[8]. U. Shankar and V. Paxson, "Active Mapping: Resisting NIDS Evasion without Altering Traffic," in SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy, Washington, DC, USA, 2003, p. 44.

[9]. D. Mutz, C. Kruegel, W. Robertson, G. Vigna, and R. A. Kemmerer "Reverse Engineering of Network Signatures", in Proceedings of the AusCERT Asia Pacific Information Technology Security Conference, Gold, 2005

[10]. M. Roesch, "Snort - Lightweight Intrusion Detection for Networks," in LISA '99: Proceedings of the 13th USENIX conference on System administration, Seattle, Washington, 1999, pp. 229--238.

[11]. A. Orfila, A. Ribagorda, “Evolving High-Speed, Easy-to-Understand Network Intrusion Detection Rules with Genetic Programming”, Springer-Verlag Berlin Heidelberg, 2009.

[12]. S. Mukkamala, A. Sung, and A. Abrham, "Modeling intrusion detection systems using linear genetic programming approach," in IEA/AIE'2004: Proceedings of the 17th international conference on Innovations in applied artificial intelligence, Ottawa, 2004, pp. 633--642.

[13]. S. Peddabachigaria, A. Abraham, “Modeling intrusion detection system using hybrid intelligent systems”, Journal of Network and Computer Applications.

[14]. Ferenc Bodon, “A fast APRIORI implementation”, Informatics Laboratory, Computer and Automation Research Institute.

[15]. M. Hall, E. Frank, G. Holmes, B. Pfahringer, P.Reutemann, I. H. Witten, "The WEKA Data Mining Software: An Update", in SIGKDD Explorations, Volume 11, Issue 1,2009.