Network Intrusion Detection Evading Systems

N. B. Dhurpate[1], L.M.R.J. Lobo[2]
[1]*Walchand Institute of Technology, Computer Science and Engineering Department, Solapur, India*

[2]*Walchand Institute of Technology/ Information Technology Department, Solapur, India*

Abstract

Nowadays, Signature based Network Intrusion Detection Systems (NIDS), which apply a set of rules (to identify hostile traffic in network segments) are quickly updated in order to prevent systems against new attacks. The goal of an attacker is to find a new evasion technique to remain unnoticed. Unfortunately, most of the existing techniques are based on the ambiguities of network protocols. Due to this the emergence of a new evasion technique NIDS system may fail to give a correct result. The central idea of our paper is to develop a network based intrusion detection system based on modified Apriori and other approaches for attack detection and test the input thus produced, by the Apriori algorithm and others with the well known snort intrusion detection system, once candidate sets for detecting different attacks are generated. These candidates in turn will be passed as inputs to the snort intrusion detection system for detecting different attacks.

1. Introduction

Ever since the rising era of internet technology has flourished, network security has become one of the most important issues that need focus today. There is an increasing public demand to develop systems that can guard against different attacks that are attempted by hackers. One security system which falls into this category is the Intrusion Detection System (IDS). Intrusion Detection Systems are software or hardware tools that automatically scan and monitor events that take place in a computer or a network, looking for evidence of intrusion.[1] Network Intrusion Detection Systems (NIDS) just analyze network traffic captured on the network segment where they are installed. These systems can be broadly classified into two major categories depending on the analysis techniques of IDS these are mainly 1) the anomaly detection and the 2) misuse detection. In this paper work we focus on misuse detection. In these types of techniques generally attack signatures are collected and stored in a database in the same way as virus protection software does in order to detect the related attacks. Signature based NIDS are effective at detecting attacks for what they are prepared.

This situation causes attackers to focus their efforts in finding evasions over the signatures of these systems. The overall idea of an intruder is to perform some changes to cause an evasion that the NIDS does not process the entire attack packet, which remains undetected. An evasion succeeds if the processing of the packets generates a different representation of the raw data in the NIDS and in the end systems. Data contained in TCP segments can encapsulate some attacks, but if the NIDS processes those segments differently from the endpoint, it will not be able to detect those attacks.

The aim of this paper is to look for new evasive techniques by analyzing NIDS behavior. In this method first we build NIDS using C4.5 algorithm. Publicly available dataset KDD-99 is given to it. AdaBoost Algorithm for supervised learning where labeling of dataset is done as normal or attack. Modified Apriori algorithm generates rules which are checked on snort for evasion. We use other methods to compare our results.

2. Literature review

The concept of evasion was first proposed by Ptacek and Newsham [2]. He focused on ambiguities in TCP and IP layer protocol. Because of these ambiguities different systems implement it in different ways. TCP does not understand what should be done when an erroneous stream comes, whether to ignore, accept or reject those packets. An evasion succeeds when NIDS ignore packets which are going to be processed on the endpoint systems or vice versa. For example, intruders' data stream is "ATNOTCK" and IDS preprocessor accepts it as it is, including "NO" which have bad checksum field while end-point system preprocessor reject the bad checksum field and accept

only "ATTACK". So the two systems treat it in different ways and evasion can take place. Several tools are implemented to exploit this. Fragroute is a tool that intercepts, modifies, and rewrites egress traffic destined for a specified host. Prototype system like idsprobe [3] , takes as input a packet trace and from it constructs a configurable set of variant traces that introduce different forms of ambiguities that can lead to evasions. Watson et.al [4] implemented Protocol scrubbers which are transparent, interposed mechanisms for explicitly removing network scans and attacks at various protocol layers. Some systems are also proposed to normalize ambiguities in network. Varguese et al. [5] presents Split-Detect which focus on the simplest form of signature, an exact string match, and start by splitting the signature into pieces. In snort [6] network topologies and the interpretation policy of the endpoint being monitored with the help of real time alerting capability. Snort is a lightweight, freely available ID's. The idea of this paper comes from [7], where GP was used to model a simple NIDS with great accuracy, using a publicly available Lawrence Berkley National Laboratory (LBNL) dataset. Later paper [8] present new improvements, performing evasions over that NIDS and corroborating the effectiveness of modeling NIDS with GP using another publicly available set KDD-99. Adaptive IDS [9] audit data so that abnormal intrusive activities can be detected by comparing the current activities with the profile.

3. Proposed System

The main aim of this paper is to develop a network based intrusion detection system based on modified Apriori approach for attack detection and test the input thus produced by the Apriori algorithm with the well known snort intrusion detection system, once a candidate sets for detecting different attacks are generated. These candidates in turn will be passed as inputs to the snort intrusion detection system for detecting different attacks.

In figure 1 the proposed system flow is given where, the input to C4.5 algorithm using Weka tool. Weka tool is implementation of various classifying and clustering algorithm. C4.5 algorithm gives output as a tree.

After that, adaboost algorithm is applied on output of C4.5. Adaboost algorithm contains steps like data labeling, training and testing. Data labeling will contain identification normal and attack packets. +1 means attack packet and -1 means normal packet. Training phase will contain initialization of parameters. Testing phase will contain real identification attack packets and classifying each detected attack under its category (Such as Dos attack, probe attack, U2R attack, R2Lattack). After that detection result and false alarm rate will get displayed.

After this step modified apriori algorithm is used, which contain process of creation of rules for detecting attacks. After creating rules they are passed to snort. Snort is an open source IDS. Now this method will detect the packets in the network. It evades the packets by changing the rules. Detection output will get stored in text files. The workflow is depicted in the following block diagram.

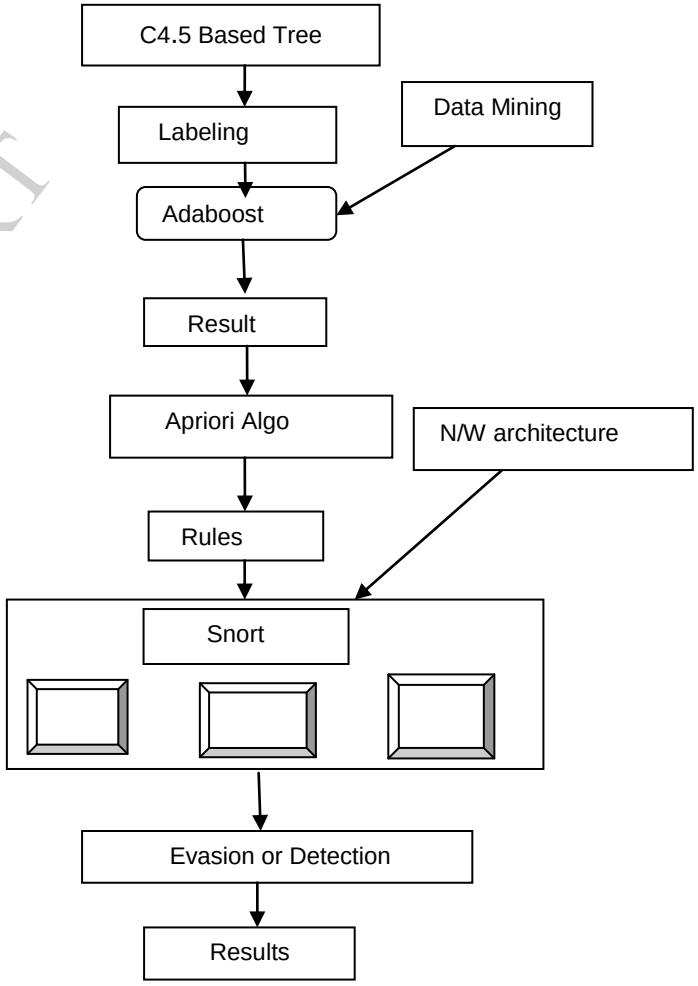

Figure 1: Flow of System

4. Conclusion

This paper present a new methodology that improved the task of looking for new forms of evasion, thus allowing systems administrators to be warned before the attackers could exploit them. A network based intrusion detection system based on modified Apriori approach and other methods for attack detection was developed and tests were performed on the input thus produced by the Apriori algorithm with the well known snort intrusion detection system.

.

5. References

[1] L.W.Stolfo, K.W.Mok,, "A Data Mining Framework For Building Intrusion Detection Model", *IEEE Symposium on Security and Privacy*,1999. pp.153 157.

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

[3] 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: *5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Paris, France*, 2008, pp. 267-278.

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

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

[6] S. Pastrana, A. Orfila, and A. Ribagorda, "Modeling NIDS evasion with Genetic Programming", *International Conference on Security and Management, SAM 2010, Las Vegas, Nevada,USA*, July 11-15, 2010

[7] S. Pastrana, A. Orfila, and A. Ribagorda, " A Functional Framework to Evade Network IDS", *IEEE* 2011.

[8] M.Hossian and S.Bridges, "A framework for an adaptive intrusion Detection system with data mining," *13thAnnu.CITSS Jun*.2001.

[9] F. Bodon. "A Fast Apriori Implementation". *IEEE ICDM Workshop on Frequent Itemset Mining Implementations*, 2003.

Ms. Neelam B Dhurpate received B.E degree in Information Technology in 2009 from PUNE University, Maharashtra, India and pursuing the M. E. degree in Computer Science and Engineering in Walchand Institute of Technology, Solapur, India. She is doing her dissertation work under the guidance of Mr. Lobo L.M.R.J, Associate Professor & Head, Department of IT, Walchand Institute of Technology, Solapur, Maharashtra, India.

Mr. Lobo L.M.R.J received the B.E degree in Computer Engineering in 1989 from Shivaji University, Kolhapur, India and M. Tech degree in Computer and Information Technology in 1997 from IIT, Kharagpur, India. He is registered for Ph.D in Computer Science and Engineering at SGGS, Nanded of Sant Ramanand Teerth Marathawada University, Nanded, India. Under the guidance of Dr. R.S. Bichkar. He is presently working as an Associate Professor & Head, Department of IT Walchand Institute of Technology, Solapur, Maharashtra, India. His research interests include Evolutionary Computation, Genetic Algorithms and Data Mining.