Volume 2, Issue 5, May 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Snort Based H-IDS with KF sensor and Weka

Durgesh Kumar*, Vivek Vashishtha
Department of C.S.E.
G.C.E.T. Greater Noida
Durgesh.durge@gmail.com

***Abstract*— Intrusion Detection System (IDS) used today suffer from several shortcomings in the presence of complex and unknown attacks. Hence in this paper Snort based hybrid Intrusion Detection System with automatic signature generation is investigated. The problem of unknown attacks with IDS is solved using anomaly detection. Entropy is one of the well known detection technique used in intrusion detection. In this work, a system is designed with the help of Entropy based technique and integrated with real time system Snort (Signature based technique) so that it can have advantages of both techniques. A feature extraction system is designed which can be used for calculating the important features for which entropy can be calculated for anomaly detection. Another issue of IDS, hectic amount of alert data, has also been addressed by developing alert unification system which comprises of alert ranking and reduction system. Alert reduction system is used to efficiently unify alerts generated by hybrid IDS whereas alert ranking system is used to give ranks to those alerts according to their importance.**

***Keywords*— Snort. Entropy, anomaly detection, alert unification, ranking,**

I. INTRODUCTION

Due to rapid growth of Internet and network based services; security becomes the primary concern for organizations. There are several ways in which an attacker can attack the network of an organization. These can be accessing information for which he is not authorized, bringing down the whole network, etc. Many systems are developed to protect a network..The security of a computer is compromised when an intrusion takes place. An intrusion can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. The Internet is being used by increasing number of users day by day. A survey [1, 2] show that the number of hosts connected to the Internet has increased to almost 550 million and more than 1.5 billion users are currently using the Internet. The recent survey of Mini Watts Marketing Group [2] estimated that the total number of Internet users was 1,802,330,457 on December 31st 2009. In 2010, the Kaspersky system logged 1,311,156,130 network attacks. That number was just 220 million in 2009.

Review shows that with the increasing number of Internet users, the cyber crimes also have been increased worldwide to a great value. Fortunately, some intrusion prevention techniques as a first line of defence, such as user authentication (e.g. using passwords and biometrics), avoiding programming errors, and information protection (e.g. encryption) have been applied to protect computer systems. Intrusion prevention alone is not sufficient because as systems are becoming even more complex. As the technology advances, more security is added to the systems. But none of the system is completely secure. There remain some loop holes which make system vulnerable. For example, after it was first reported many years ago, exploitable "buffer overflow" still exist in some recent system software due to programming errors. Hence Intrusion detection system comes into picture to protect the system with these holes. Intrusion detection methods with machine intelligence started appearing in the last few years. Using intrusion detection methods, you can collect and use information from known types of attacks and find out if someone is trying to attack your network or particular hosts. The information collected this way can be used to harden your network security, as well as for legal purposes. Snort is one the most famous open NIDS. It is signature based. It uses alert based system to denote the suspicious activities. Its alert comprises of packet source and destination information along with signature id and timestamp. The main problems with Snort are vulnerability to unknown attacks, huge amount of alerts and no ways to identify the importance of alerts.

II. BACKGROUND RELETED WORK

First intrusion detection model was given by Dorothy E. Denning in 1988 [4]. This was the base model of all the intrusion detection systems. The model was independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general purpose intrusion detection expert system Apart from the known attacks, a lot of unknown types of attacks keep happening. A lot of machine intelligence Techniques have been used in intrusion detection area to reduce vulnerability to unknown attacks. If we talk about Fuzzy logic [5].

First intrusion detection model was given by Dorothy E. Denning in 1988 [4]. This was the base model of all the intrusion detection systems. The model was Independent of any particular system, application environment, system

vulnerability, or type of intrusion, thereby providing a framework for a general purpose intrusion

Detection expert system. The model has six main components:

***(a) Subjects*:**
Initiators of activity on a target system, generally normal users

***(b) Objects*:**
Resources managed by the system – files, commands, devices etc.

***(c) Audit Records* Audit:**
Records are generated by the target system in response to actions performed or attempted by subjects on objects – user login, file access etc. These are the 6-tuples actions.
<Subject, Action, Object, Exception-Condition, Resource-Usage, Time-Stamp>

(d) Profiles:

Profiles are the structures that characterize the behavior of subjects with respect to objects in terms of statistical metrics and model of observed activity. Observed behavior is characterized in terms of statistical metrics and models. Metrics for example event counter, interval timer, resource measures etc. Models can be operational model, mean and standard deviation model, multivariate model, time series model etc. Structure of a profile record can be in this format
<Variable-Name, Action-Pattern, Exception-Pattern, Resource-Usage, Period, Variable-Type, Threshold, Subject-Pattern, Object-Pattern, Value>

***(e) Anomaly Records*:**
Anomaly records are generated when abnormal behavior is detected.

(f) Activity Rules:

Activity rules are actions taken when some condition is satisfied, which update profiles, detect abnormal behavior, relate anomalies to suspected intrusions, and produce reports.
Generally four types of rules are defined: Audit-record rule, Periodic-activity-update, Anomaly-record and Periodic-anomaly-analysis rule.

The model can be regarded as the rule based pattern matching system. When an audit record is generated, it is matched against the profiles. Type information in the matching profile then determines what rules to apply to update the profiles, check for abnormal behavior, and report anomalies detected.

III. SYSTEM DESIGN AND IMPLEMENTATION

There are so many data mining technique the better IDS. So all the issues discussed in research gaps, here we are proposing a framework of IDS. Framework comprises of broadly three independent systems:

· (a) Automatic signature generation system
· (b) Snort based IDS
(c) Entropy based system.

Design of this module includes major three modules. First is data collection by honeypot, second is mining the data to generate attack rules and last is the RTRA (real time rule accession) in Snort. But all these modules are incompatible. E.g. honeypot log file cannot be directly given as input to the mining algorithm. So to eliminate these problems, interfaces are designed in between these modules. Similar interface is designed for rules generated by Apriori and rules added in Snort. A log file is very large so in order to efficiently process these log files DBMS is used.

Snort based hybrid IDS deals with the problem of IDSs encountered with unknown attacks. Also it addresses the issue of better alert management along with better alert and logging system for Snort.

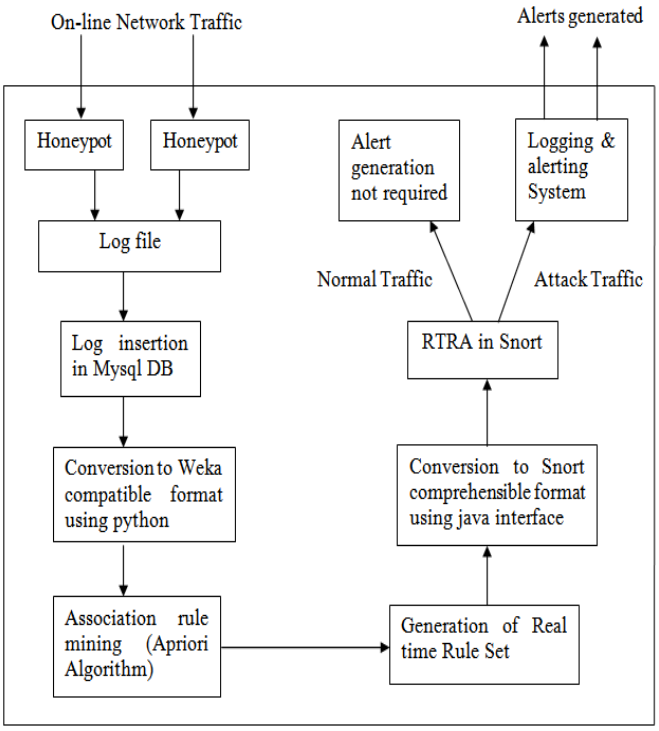


Fig. 1 System architecture

System is implemented in Ubuntu-9.04. Snort 2.8.6 is used as signature based system. Barnyard and Acid-base are used as alert and logging system. Feature selection algorithm is implemented in java. NSL-KDD data is used as off line traffic. Entropy based Anomaly detection module is implemented in Java.

IV. EXPERIMENTAL RESULTS

In parallel to this another instance of Snort is run on the same interface. Here Snort is run in NIDS mode. So that we can detect those attacks and validate our system. All snort alerts generated our stored in two files "alert.txt" and also into mysql database through Barnyard utility.

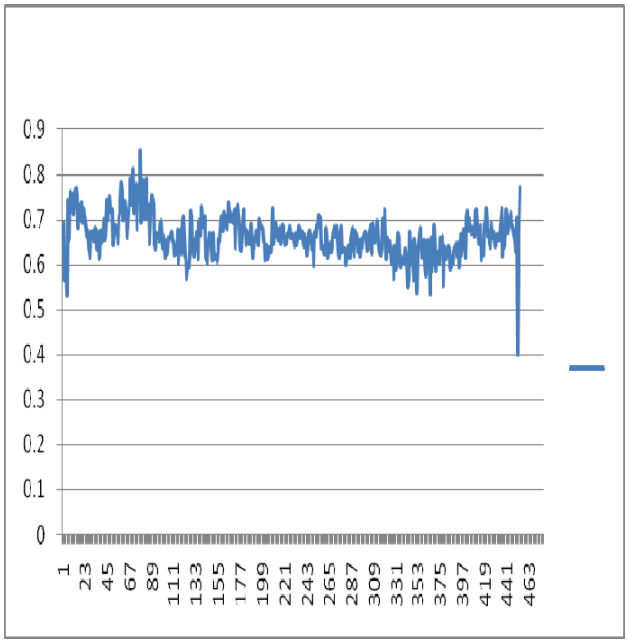
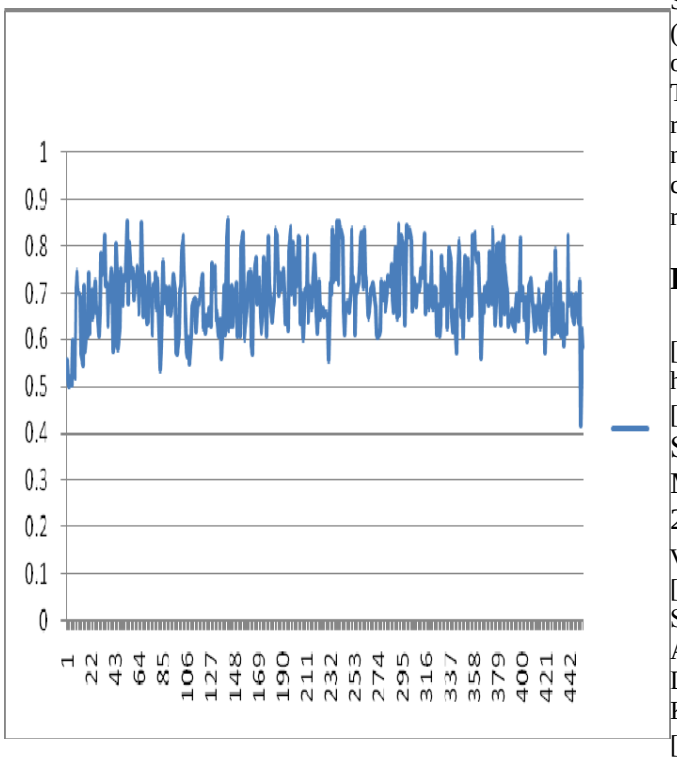


Fig. 2 Graphs representing relation between entropy (Vertical Axis) and time stamp (horizontal axis) for different features. (I) Source IP,



(II)

Fig. 2 Graphs representing relation between entropy (Vertical Axis) and time stamp (horizontal axis) for different features. (II) Source Port

First we have to prove the validity of entropy based module. For this network traffic of Institute Hostel is used. Institute is also used as the historical data. The entropy change in different features of the network traffic of a particular day .

Feature	**No. of Anomalous Point Detected when t =2**	**No.of Anomalous Point Detected when t=3**
Src_ip	95	8
Dst_ip	93	1
Source Port	95	5
Destination Port	71	6

Table shows the drastic impact for threshold value values used for anomalies detection. Number of anomalous points drastically increases when it is decreased to 2 from 3. This causes a lot of points to be declared as anomalous points.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we have designed and implemented real time Intrusion detection system with the help of integration of Snort (Signature based system) and Entropy based (Anomaly based) system. Also we improve the efficiency of that IDS by developing automatic signature system. This system is developed using honeypots and association rule mining techniques which detected attack traffic in the network timely and effectively. The honeypot was used to create a virtual network topology with virtual systems running various services.

REFERENCES

[1] Wikipedia Article of IDS. Available online at http://en.wikipedia.org/ids.html.

[2] Internet System Consortium, "ISC Domain Survey: Number of Internet Hosts." [Last accessed: May, 2010].[Online]Available:http://ftp.isc.org/www/survey/ reports/2010/04/...

[3] E. Eskin, A. Arnold, M. Preau, L.Portnoy, and S. Stolfo, "AGeometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data " Applications of DataMining in Computer Society, Kluwer Academic Publishers, 2002.

[4] Denning, D.E.; "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, vol.SE-13, no.2, pp. 222- 232, Feb. 1987

[5] W. Yunwu, "Using Fuzzy Expert System Based on Genetic Algorithms for Intrusion Detection System", Information Technology and Applications, IFITA, pages 221-224, 2009.

[6] W. Lee; S. J. Stolf; K. W. Mok, "A Data Mining Framework for Building Intrusion Detection Model", Security and Privacy, Proceedings of the 1999 IEEE Symposium, pages 120-132, 1999.

[7] W. Lee; S. J Stolfo, “Data mining approaches for intrusion
detection”. Proc. Of Seventh USENIX Security Symposium. San Antonio, TX, 1998
[8] D. Barbara; J. Couto; S. Jajodia; N. Wu , “Adam: Dtecting
Intrusions by Data Mining” Proc. Of 2nd Annual IEEE Information Assurance Workshop. West Point, NY, 2001
[9] T. Abraham; “IDDM: Intrusion Detection Using Data Mining Techniques.” Technical report DSTO-GD-0286, DSTO Electronics and Surveillance Research Laboratory, 2001 [10] A. Valde; K. Skinner , “Adaptive, model based monitoring for cyber attack detection”, Recent advances on Intrusion Detection, France, Springer Verlag, pp 80-93, 2000
[11] L. Eetoz; E. Eilertson; A. Lazarevic; P. Tan; P. Dokes; V. Kumar; J. Srivastava, “Detection of Novel Attacks using Data Mining”. Proc. IEEE Workshop on Data Mining and Computer Security, 2003
[12] D. E. Denning, “An Intrusion-Detection Model” , IEEE Transaction on Software Engineering, Vol. SE-13 No.2, 1987.
[13] G. Nychis, V. Sekar, D.G. Andersenm, H. Kim and H. Zhang, “An empirical evaluation of entropy-based traffic anomaly detection”, Proceedings of 8th ACM SIGCOMM conference on Internet Measurement, pp 151-156, 2008.
[14] M. Celenk; T. Colony; J. Willies; J. Graham; , "Predictive Network Anomaly Detection and Visualization," *Information Forensics and Security, IEEE Transactions on* , vol.5, no.2, pp.288-299, June 2010.
[15] T. Zang; X. Yun; Y. Zhang; , "A Survey of Alert Fusion Techniques for Security Incident," *Web-Age Information Management, 2008. WAIM '08. The Ninth International Conference on* , vol., no., pp.475-481, 20-22 July 2008

