Hybrid Intrusion Detection System Using ANN and Snort

K.Gayathri[1], Srikanth Yadav.M[2], K.Prem Sai Reddy[3], A.Venkata Mani Teja[4]

[1]Assistant Professor, Dept. of. CSE, Tirumala Engineering College, Jonnalagadda, NRT, AP, India
[2]Associate Professor, Dept. of. CSE, Tirumala Engineering College, Jonnalagadda, NRT, AP, India
[3, 4]U.G.Students, Dept. of. CSE, Tirumala Engineering College, Jonnalagadda, NRT, AP, India

Abstract—

In this paper, we discussed a methodology of applying artificial intelligence into intrusion detection using snort system. Intrusions detection systems (IDSs) are systems that try to detect attacks as they occur or after the attacks took place. Hybrid Snort system is proposed for network security. A brief overview of Intrusion Detection System (IDS), snort, artificial intelligence and related detection techniques are discussed. The purpose of this paper is to describe some new ideas in intrusion detection system.

Keywords— *IDS, Snort, Neural Network, Data mining*

I. INTRODUCTION

It Look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent. An intrusion detection system (IDS) is a system that is designed to capture intrusion attempts so that measures can be taken to limit damage and prevent future attacks. This is typically accomplished by sending alerts anytime the IDS detect an attack. IDSs can be broken down by where they gather their data and how they check for attacks. Intrusion Detection System (IDS) is an authorized way of identifying illegitimate users, attacks and vulnerabilities that could affect the proper functioning of computer systems. IDSs detect some set of intrusions and execute some predetermined actions when an intrusion is detected. The main benefits of snort are:

(i) Detecting attacks and other security violations
(ii) Recognize damage and affected systems
(iii) It doesn't compensate for bad security
(iv)Acting as quality control for security design and implementation
(v) Preventing problem-behaviors by increasing the perceived risk of discovery
(vi) Forensic analysis
(vii) Presenting traces of intrusions, allowing improved diagnosis, recovery and corrective measures after an attack
(viii) Documenting the existing threat from inside and outside a system, permitting security management to realistically assess risk and adapt its security strategy in response.

Characteristics of Intrusion Detection Systems: In order to satisfy its functions, the ideal intrusion detection system should have the following characteristics:

Timeliness: It should detect intrusions either while they are happening or shortly afterwards. High probability of detection: It should recognize all or most intrusions.
Low false-alarm rate: It should have a low number of false intrusion alarms.
Specificity: In identifying attacks, it should give sufficient characterization data to support an effective response. Scalability: It should be applicable to large (infinite) networks. Low a priori information: It should require a minimum of a priori information about potential attackers and their methods.

Snort is a free and open source Network Intrusion Prevention System (NIPS) and Network Intrusion Detection System (NIDS) capable of performing packet logging and real time traffic analysis on IP networks. Snort performs protocol analysis and content searching/ matching, it is commonly used to actively block or passively detect a variety of attacks and probes, such as buffer overflows, stealth port scans, web applications attacks, SMB Probes, and OS fingerprinting attempts amongst other features. The software is mostly used for intrusion prevention purposes by dropping attacks as they are taking place.

- Natural Choke Points: Areas where the network topology creates a single traffic path
- Artificial Choke Points: Exist due to logical topology of the network
- Intranet Trust/Un-trust Zone Boundaries: Similar to Natural Choke Points but are intra-network

Snort Rules

The license applied to the rules depends on who wrote or maintains them; there are several sources of rules on Snort:

- Official Snort Rules: Rules maintained by the Vulnerability Research Team (VRT). Certified Rules are distributed under the VRT Certified Rules License Agreement [68]. It enables registered end-users to freely download and use rules that have been certified by the Sourcefire VRT while restricting commercial redistribution.
- Community Rules: SourceFire is committed with keeping Snort as an open platform. They host rules submitted by the community, previously performing some basic tests to make sure they will not break Snort. These rules are distributed under the GPL and are freely available to all Snort users.

- Other Sources: Rules found on other sources might be under any license; freely available or not. It is up to its owner to decide which license applies.

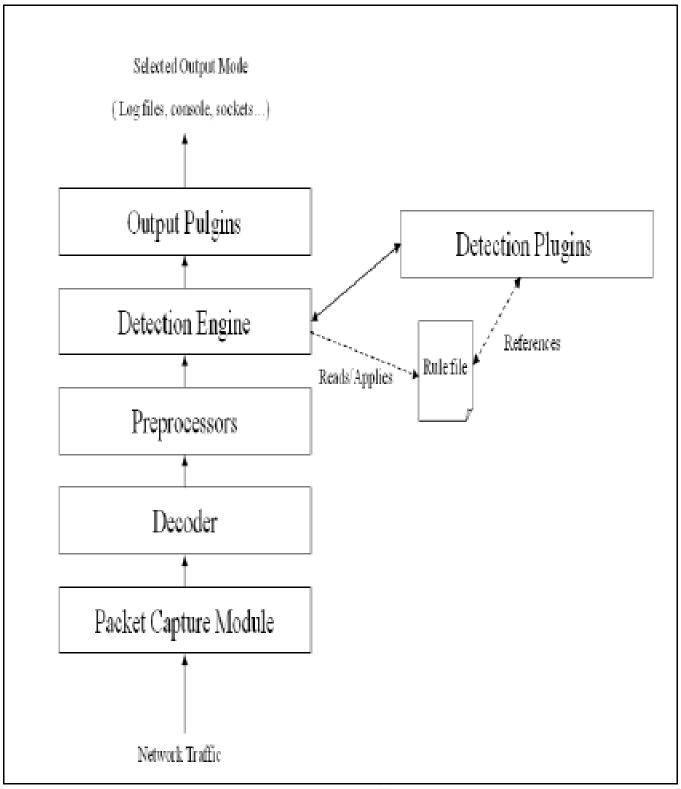

Figure1: Snort Architecture

Internal Structure It illustrates the modules in which Snort is divided:

Packet Capture Module is based on the popular packet programming library libpcap; can be optimized for MMAPed pcap in case of looking for performance. It provides a high-level interface to packet capture.

Decoder fits the captured packets into data structures and identifies link level protocols. Then, it takes the next level, decodes IP, and then TCP or UDP in order to get useful information like ports and addresses. Snort will alert if it finds malformed headers.

Preprocessors could be seen like some kind of filter, which identifies things that should be checked later such as suspicious connection attempts to some TCP/UDP ports or too many TCP SYN packets sent in a short period of time . Preprocessors function is to take packets potentially dangerous for the detection engine to try to find known patterns, as we explained before they will be in charged of doing the Stateful Protocol Analysis.

Rules Files are plain text files which contain a list of rules with a known syntax. This syntax includes protocols, addresses, output plug-ins associated and some other things. Those rules files can be updated.

Detection Plug-ins are modules referenced from its definition in the rules files. They are used to identify patterns whenever a rule is evaluated.

Detection Engine Making use of the detection plug-ins, it matches packets against rules loaded into memory during Snort initialization.

Output Plug-ins are the modules which allow formating the notifications (alerts, logs) for the user to access them in many ways (console, extern files etc).

II. RELATED DATA

A. Host based IDS

The host operating system or the application logs in the audit information. These audit information includes events like the use of identification and authentication mechanisms, file opens and program executions, admin activities etc. This audit is then analyzed to detect trails of intrusion. Host-based IDS monitors network traffic of a particular host and some system events on the host itself. One may be installed on each host or simply on some chosen critical ones within a network.

B. Network based IDS

This IDS looks for attack signatures in network traffic via a promiscuous interface. A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic. Intrusion detection is a security technology that attempts to identify intrusions against a computer network. An intrusion is an unauthorized usage of or misuse of a computer system. In order to discover these intrusions a network administrator can employ an intrusion detection system (IDS).

C. Hybrid IDS

The management and alerting from both network and host based intrusion detection devices, and provide the logical complement to NID and HID - central intrusion detection management.

III. CLASSIFICATION OF IDS

A. Misuse Detection-based IDS

Misuse detection technique is the most widespread approach used in the commercial world of IDSs. The basic idea is to use the knowledge of known attack patterns and apply this knowledge to identify attacks in various sources of data being monitored.

B. Signature based approach

Signature based approach of misuse detection works just similar to the existing anti-virus software. In this approach the semantic characteristics of an attack is analyzed and details is used to form attack signatures. The attack signatures are formed in such a way that they can be searched using information in audit data logs produced by computer systems.

C. Anomaly-Based Detection

Anomaly detection identifies abnormal behavior. It requires the prior construction of profiles for normal behavior of users, hosts or networks; therefore, historical data are collected over a period of normal operation. IDSs monitor current event data and use a variety of measures to distinguish between abnormal and normal activities.

IV. PROPOSED SYSTEM

There are several different soft computing techniques and algorithms that can be successfully used to detect intrusions. These techniques include:

- Fuzzy logic
- Probabilistic reasoning
- Neural networks
- Genetic algorithms

Using neural network classifier which efficiently and rapidly classifies observed network packets with respect to attack patterns which it has been trained to recognize. This is a feed forward network which uses supervised training, and which:

- can be trained rapidly,
- can be trained incrementally,
- once trained, can perform fast and accurate classification of its input.

The idea here is to train the neural network to predict a user's next action or command, given the window of „n" previous actions or commands. The network is trained on a set of representative user commands. After the training period, the network tries to match actual commands with the actual user profile already present in the net. Neural networks are basically sets of individual cells that have weighted connections to other connected cells. The training process of a neural network consists of setting weights for each connection and comparing the output with the desired output.

Hybrid model is the combination of snort system, neural network and involving data mining technique. This improves the current security of the system.

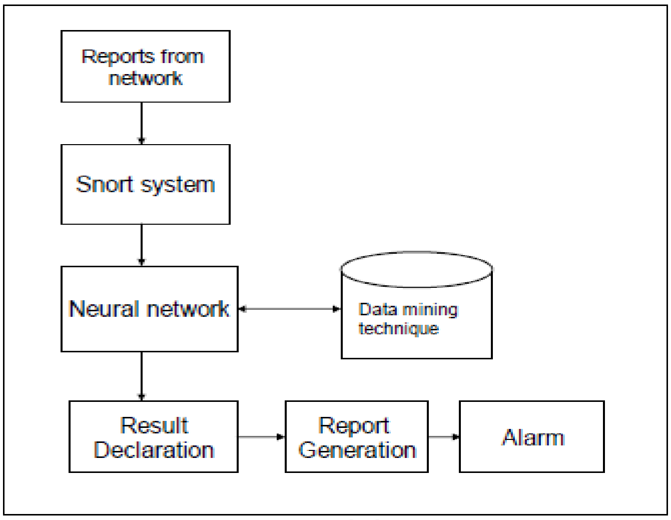

Figure2: Proposed Alert System

A. *Steps involved: Reports from network*:

It collects the network traffic of the leaf level sensor when it receives reports from lower layer. These are deployed in a network or on a device to collect data. They take input from various sources, including network packets, log files, and system call traces. Input is collected, organized and then forwarded to one or more analyzers.

B. *Snort system:*

It detects intrusions by first parsing network traffic to extract is application-level semantics and then executing event oriented analyzers that compare the activity with patterns deemed troublesome.

C. *Neural network and data mining:*

Using neural network classifier with combination of misuse technique which efficiently and rapidly classifies observed network packets with respect to attack patterns which it has been trained to recognize. This is a feed forward network which uses supervised training, and which: _ can be trained rapidly, _ can be trained incrementally, _ once trained, can perform fast and accurate classification of its input. It is used and trained to fetch information using data mining technique from the previously stored data.

D. *Result Declaration:*

In this step the result in concluded and the result is further passed to the next level for storing results for later use.

E. *Report generation:*

Report is generated giving the information about attacks. These reports are then send to the security manger.

F. *Alarm:* -

If it detects an intrusion then it raises the alarm. It beeps the alarm when it finds the intrusion in a system.

V. CONCLUSION

A hybrid intrusion detection system is a part of the defensive operations that complements the defenses such as firewalls. Intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. Snort has a team dedicated to the creation, test, maintenance, and documentation of its official rules to ensure their quality. Snort is oriented to high speed links. These are a highly flexible security tool that can be used in a variety of different deployments. These are tools to acquire knowledge. The education they provide is their most important contribution. They also require substantial resources to operate correctly. It can provide a fantastic learning tool in computer security. These are a cheap and simple way to add protection to a network and help developing new ways for countering them.

VI. REFERENCES

[1] Bridges, Susan, and Rayford B. Vaughn. 2000, "Intrusion Detection Via Fuzzy Data Mining" in Proceedings 12th Annual Canadian information Tech. securitySymposium,pp.109-122.Ottawa, canada

[2] Bezroukov, Nikolai. 19 July 2003. "Intrusion Detection. Softpanorama: Open Source Softwarec ducational Society. Nikolai Bezroukov.

[3] Divya and Amit Chugh, "GHIDS: A Hybrid Honeypot Using Genetic Algorithm", published in IJCTA, vol 3. Jan 2012

[4] Miguel A. Calvo Moya, analysis and evaluation of The snort and bro network intrusion detection system September 2008.

[5] A. F. Arboleda and C. E. Bedon, Snort diagrams for developers, Universidad del Cauca Colombia, 2005

http://afrodita.unicauca.edu.co/cbedon/snort/snortdevdiagra ms.htm

[6] Divya and Amit Chugh, "Wsnort: A Hybrid Snort System For Intrusion Detection Using Genetic Algorithm In Wireless Environment ", published in Proc. of NationalConference on Data Mining & Warehousing 2012 2012

[7] Network-based Hybrid Intrusion Detection and Honeysystems as Active Reaction Schemes Pedro García-Teodoro in 2007.

[8] Cliff, A. Password Crackers - Ensuring the Security of Your Password. Unknown: SecurityFocus.com, 2001, accessed 12 October 2004

[9] New Methods of Intrusion Detection using Control- Loop Measurement May 16, 1996

[10] Moradi and M. Zulkernine. A neural network based system for intrusion detection and Classification of attacks. In 2004 IEEE International Conference on Advances in in Intelligent Systems.

[11] Mounji. Rule-Based Distributed Intrusion Detection. PhD thesis, University of Namur 1997

[12] VG. C. F.M. Valtorta. Paid: A probabilistic agent-
Based intrusion detection system. In Computers & Security, pages 529–545, 2005.

[13] S. Zanero and S. M. Savaresi. Unsupervised Learning techniques for an intrusion detection System. In SAC "04: Proceedings of the 2004 ACM symposium on Applied computing, pages 412–419, New York, NY, USA 2004.