An analysis of Network Intrusion Detection System using SNORT

Mr. Nishidh D. Patel [1] Prof. Vrushank Shah [2] Prof. Kruti j. Pancholi [3]
[1]M.E. [Electronics and Communication] Student [2, 3]Assistant Professor
[1, 2, 3]Department of E & C Engineering
[2]Indus University, Ahmedabad, Gujarat, India
[1, 3]L.J.institute of engineering and technology, Ahmedabad, Gujarat, India

Abstract— This paper describes the analysis of signature based intrusion detection systems. Snort which is a signature based intrusion detection system are used for this purpose. We use DARPA dataset for the evaluation of Intrusion detection system.

Keywords: Intrusion detection system, Snort, DARPA dataset.

I. INTRODUCTION

In the field of computer network system security is a main concern. With the rapid expansion of computer networks during the past few decades, security has become a crucial issue in the computer. The purpose of network security is to protect the network from unauthorized access and disclosure. The recent Advancements in the field of network security help in the protection of computer systems and computer networks. One of the techniques used for making the network secure and detecting intrusions is Intrusion Detection System. Intrusion Detection System is a mechanism that detects unauthorized and malicious Activity present in the computer systems.

II. OVERVIEW OF IDS

An *intrusion detection system (IDS)* is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection systems (IDS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDS for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies.

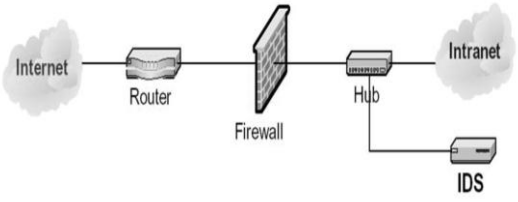

Fig. 1: A Typical scenario in any Network

An intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators.

A. *Snort IDS [1, 8]*

It is free, extremely powerful and widely used by researchers. Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998. Snort is now developed by Source fire, of which Roesch is the founder and CTO In 2009, Snort entered InfoWorld Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time". Snort is a Network Intrusion Detection system, which is used to detect malicious activity in the network traffic. It is a widely used NIDS and this motivated us to study its architecture and analyze the different components of an IDS. Snort can be configured to run in four different modes i.e. as packet sniffer, packet logger, Network-based Intrusion Detection System and Inline Mode (IPS).

1) Sniffer mode: - In this mode Snort uses a packet capturing tool to sniff packets from the network traffic and display it on console. No logging is done in Sniffer mode.

2) Logger mode: - In this mode packets are logged on to secondary storage for future reference.

3) *NIDS mode:* - In this mode Snort will analyze the contents of a packet, compare them with set of pre-defined rules and generate alerts if a match is found (i.e. if a packet is found to be malicious).

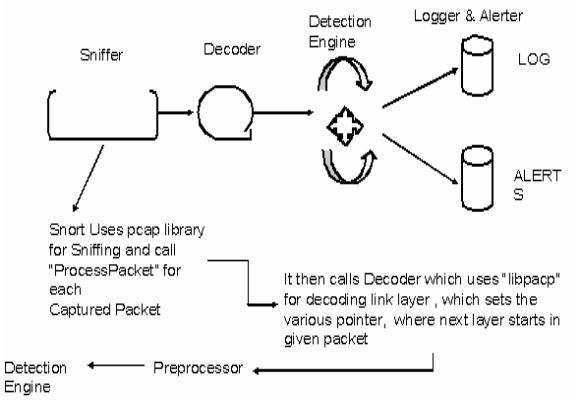

Fig. 2: Snort Architecture

4) Inline mode: - This mode is known as Intrusion Prevention mode. In this mode Snort will take raw data from IPTABLES and check it against its rule set. If any alerts are generated then IPTABLE rules are updated accordingly to prevent that malicious activity from occurring.

Packet Sniffer

Sniffer module is used to sniff the packets from network. It uses pcap library (Packet Capture) for doing so. Once the packet is captured it is passed to the decoder for placing various pointers for future processing.

A packet sniffer is a device (either hardware or software) used to tap into networks. It works in a similar fashion to a telephone wiretap, but it's used for data networks instead of voice networks. A network sniffer allows an application or a hardware device to eavesdrop on data network traffic.

Packet sniffers have various uses:

- Network analysis and troubleshooting
- Performance analysis and benchmarking
- eavesdropping for clear-text passwords and other interesting tidbits of data

Encrypting your network traffic can prevent people from being able to sniff your packets into something readable, like any network tool, packet sniffers can be used for good and evil.

Decoder

Decoder will place various pointers in the packet structure to make it easy for other modules to get data of specific layer. Once the pointers are set packet is passed to the pre-processor.

Preprocessor

As snort is rule based intrusion detection system, it can't detect anomaly spread over multiple Packets. Preprocessor is the remedy for this. Preprocessor is a separate plug-in module which can be loaded by making entry in Snort configuration file. Once snort is started with pre-processor support it will detect anomalies based on the type of pre-processor.

Detection Engine

Once packets have been handled by all enabled preprocessors, they are handed off to the detection engine. The detection engine is the meat of the signature-based IDS in Snort. The detection engine takes the data that comes from the preprocessors and its plug-ins, and that data is checked through a set of rules. If the rules match the data in the packet, they are sent to the alert processor [4].

Earlier in this chapter, we described Snort as signature-based IDS. The signature-based IDS Function is accomplished by using various rule sets. The rule sets are grouped by category (Trojan horses, buffer overflows, and access to various applications) and are updated regularly.
The rules themselves consist of two parts:

- *The rule header:* The rule header is basically the action to take (log or alert), type of network packet (TCP, UDP, ICMP, and so forth), source and destination IP addresses, and Port.
- *The rule option:* The option is the content in the packet that should make the packet Match the rule.

The detection engine and its rules are the largest portion (and steepest learning curve) of new Information to learn and understand with Snort, Snort has a particular syntax that it uses with its rules. Rule syntax can involve the type of protocol, the content, the length, the header, and other various elements, including garbage characters for defining butter overflows rules. Once you get it working and learn how to write Snort rules.

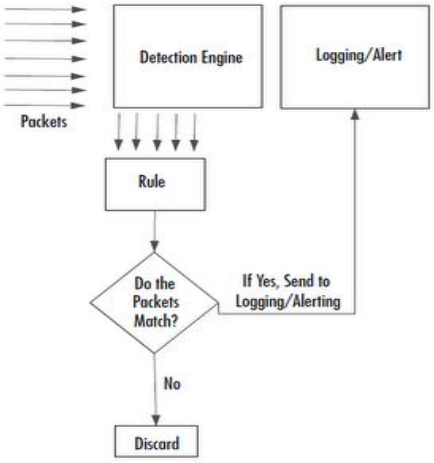

Fig. 3: Snort detection Engine

III. EVALUATION OF SNORT IDS

Snort is evaluated on the 1999 DARPA off-line IDS Evaluation data set [4]. The set consists of network traffic tcpdump files. The week 3, 4 and 5 data is taken as input set.

A. Result of Snort

Snort is evaluated on week 3, week 4 and week 5 data. The week 3 data is attack free and can be used to train Snort. The week 4 and week 5 data consist of attacks and is used in testing phase. During testing phase, Snort generates a number of alarms.

Day	1	2	3	4	5
No of Events	18557	6392	2092	3490	7780

Table 1: Events logged by Snort

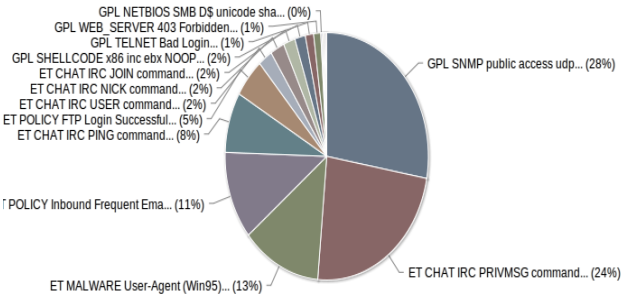

Fig. 4: Signature generated by Snorby

As shown in figure 4 the result of signature generated in snort which is responsible to generate snort events using front end GUI snorby

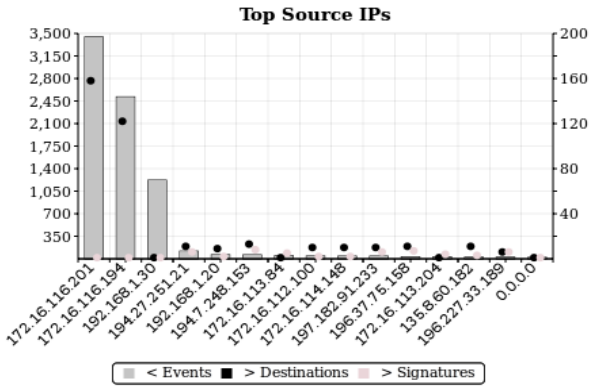

Fig. 5: Top source IPs in Event log

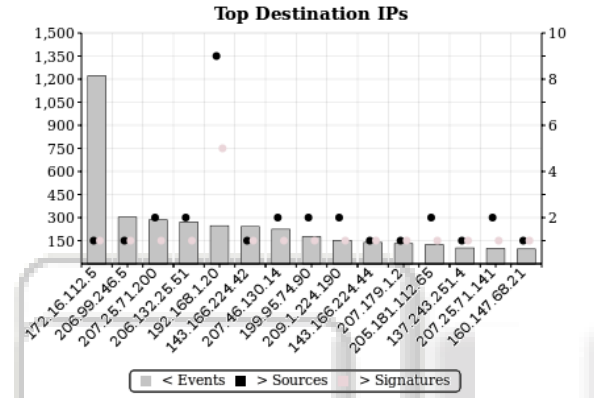

Fig. 6: Top Destination IPs in event log

B. Detection Rate

The performance of Intrusion Detection Systems can be measured in terms of number of attacks detected by it. The Intrusion detection rate denoted by δ is defined by

$$\delta = d/n$$

Where d is the no. of detected attacks and n is the no. of actual attacks.

The no. of attacks detected by Snort is 105 out of the total number of attack present in the input dataset. So detection rate of Snort is,

$$\delta = 105/201 * 100 = 52.23\ \%$$

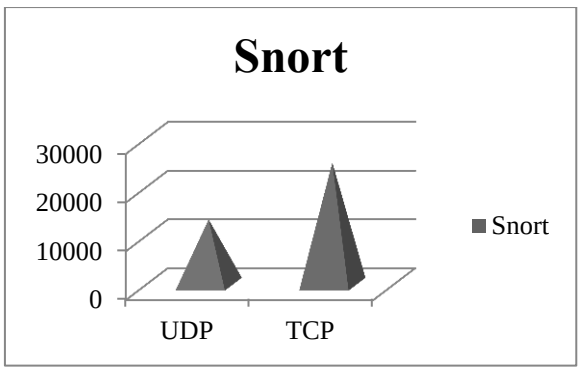

Fig. 7: Alerts generated by snort protocol wise

IV. CONCLUSION

For the experimentation purpose DARPA Intrusion Detection System Evaluation dataset which was created in MIT Lincoln Laboratories is used to evaluate the performance of Snort. The analysis of snort is done based on the alert generated day wise, alert generated protocol wise and based on detection rate. It has been found and conclude that snort detection rate is needed to improve and also the false alert should be reducing to improve overall performance of snort.

REFERENCES

[1] Martin Roesch, Snort- Lightweight Intrusion Detection for Networks. In Proc. of 13th USENIX conference on system administration LISA '99, CA, USA, 229-238.

[2] MIT Lincoln Laboratory DARPA Intrusion Detection system Evaluation dataset. Available: http://www.ll.mit.edu/mission/communications/cyber/cstcorpora/ideva/index.html

[3] Information Assurance Tools Report – Intrusion Detection Systems, 1999, IATAC, Herndon, VA.

[4] D. E. Denning, "An intrusion detection model," in Seventh IEEE Symposium on security and privacy, 1987, pp.119-131

[5] Denning, Dorothy. (February, 1987). An Intrusion-Detection Model IEEE Transaction on Software Engineering, Vol. SE-13, No. 2

[6] Yousef Farhaoui, Ahmed Asimi. Model of effective intrusion detection on LAN in international general of computer applications (0975-8887), volume 41-No.11, March 2012

[7] Snort open source intrusion detection system, Available: http://www.snort.org

