iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** X **Month of publication:** October 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

SNORT: Network and Host Monitoring Intrusion Detection System

D. Sakthivel[1], Dr. B. Radha[2]
[1,2]*Department of Computer Science, Sree Saraswathi Thygaraja College, Pollachi, Tamilnadu - 642006*

Abstract: Security is a big issue for all networks in today's enterprise environment. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, and virtual private networks. Intrusion detection is a relatively new addition to such techniques. Intrusion detection methods 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. Snort is an open source Network Intrusion Detection System (NIDS) which is available free of cost. NIDS is the type of Intrusion Detection System (IDS) that is used for scanning data flowing on the network. There is also host-based intrusion detection systems, which are installed on a particular host and detect attacks targeted to that host only. Although all intrusion detection methods are still new, Snort is ranked among the top quality systems available today. [1]

Keywords: IDS, NIDS, HIDS, Signatures, Logs, Alerts, SNORT, ACID, SnortSam

I. INTRODUCTION

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intrusion detection systems fall into two basic categories: signature-based intrusion detection systems and anomaly detection systems. Intruders have signatures, like computer viruses, that can be detected using software. You try to find data packets that contain any known intrusion-related signatures or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts. Anomaly-based intrusion detection usually depends on packet anomalies present in protocol header parts. In some cases these methods produce better results compared to signature-based IDS. Usually an intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it. Snort is primarily a rule-based IDS, however input plug-ins are present to detect anomalies in protocol headers [1].

A. Essential Components

1) *IDS:* Intrusion Detection System or IDS is software, hardware or combination of both used to detect intruder activity. Snort is an open source IDS available to the general public. IDS may have different capabilities depending upon how complex and sophisticated the components are. IDS appliances that are a combination of hardware and software are available from many companies. As mentioned earlier, IDS may use signatures, anomaly-based techniques or both.[1]
2) *Network IDS or NIDS***:** NIDS are intrusion detection systems that capture data packets travelling on the network media (cables, wireless) and match them to a database of signatures. Depending upon whether a packet is matched with an intruder signature, an alert is generated or the packet is logged to a file or database. One major use of Snort is as a NIDS.[2]
3) *Host IDS or HIDS:* Host-based intrusion detection systems or HIDS are installed as agents on a host. These intrusion detection systems can look into system and application log files to detect any intruder activity. Some of these systems are reactive, meaning that they inform you only when something has happened. Some HIDS are proactive; they can sniff the network traffic coming to a particular host on which the HIDS is installed and alert you in real time.[1][2]
4) *Signatures:* Signature is the pattern that you look for inside a data packet. A signature is used to detect one or multiple types of attacks. Signatures may be present in different parts of a data packet depending upon the nature of the attack. [3]
5) *Alerts:* Alerts are any sort of user notification of an intruder activity. When an IDS detects an intruder, it has to inform security administrator about this using alerts. Alerts may be in the form of pop-up windows, logging to a console, sending e-mail and so on. Alerts are also stored in log files or databases where they can be viewed later on by security experts. Snort can generate alerts in many forms and are controlled by output plug-ins. Snort can also send the same alert to multiple destinations.[3]

6) *Logs:* The log messages are usually saved in file. By default Snort saves these messages under /var/log/snort directory. However, the location of log messages can be changed using the command line switch when starting Snort. Log messages can be saved either in text or binary format. The binary files can be viewed later on using Snort or tcp dump program. A new tool called Barnyard is also available now to analyze binary log files generated by Snort. Logging in binary format is faster because it saves some formatting overhead. In high-speed Snort implementations, logging in binary mode is necessary. [2]
7) *False Alarms:* False alarms are alerts generated due to an indication that is not an intruder activity. For example, misconfigured internal hosts may sometimes broadcast messages that trigger a rule resulting in generation of a false alert.[2]
8) *Sensor:* The machine on which an intrusion detection system is running is also called the sensor in the literature because it is used to "sense" the network.

II. LITERATURE REVIEW

1) **"***Effectiveness of Intrusion Prevention Systems (IPS) in Fast Networks*" [6] Computer systems are facing biggest threat in the form of malicious data which causing denial of service, information theft, financial and credibility loss etc. No defence technique has been proved successful in handling these threats. Intrusion Detection and Prevention Systems (IDPSs) being best of available solutions. These techniques are getting more and more attention. Although Intrusion Prevention Systems (IPSs) show a good level of success in detecting and preventing intrusion attempts to networks, they show a visible deficiency in their performance when they are employed on fast networks This paper describes how to reduce the responding time for IPS when an intrusion occurs on network, and how can IPS be made to perform its tasks successfully without effecting network speed negatively.
2) *"Intrusion and intrusion detection"[7]* Assurance technologies for computer security have failed to have significant impacts in the market place, with the result that most of the computers connected to the internet are vulnerable to attack. This paper looks at the problem of malicious users from both a historical and practical standpoint. It traces the history of intrusion and intrusion detection from the early 1970s to the present day, beginning with a historical overview. The paper describes the two primary intrusion detection techniques, anomaly detection and signature-based misuse detection, in some detail and describes a number of contemporary research and commercial intrusion detection systems. It ends with a brief discussion of the problems associated with evaluating intrusion detection systems and a discussion of the difficulties associated with making further progress in the field. With respect to the latter, it notes that, like many fields, intrusion detection has been based on a combination of intuition and brute-force techniques. We suspect that these have carried the field as far as they can and that further significant progress will depend on the development of an underlying theoretical basis for the field.
3) *"A Novel Network Intrusion Detection System (NIDS) Based on Signatures Search of Data Mining" [8]* Network security has been a very important issue, since the rising evolution of the Internet. There has been an increasing need for security systems against the external attacks from the hackers. One important type is the Intrusion Detection System (IDS). There are two major categories of the analysis techniques of IDS: the anomaly detection and the misuse detection. Here we focus on misuse detection, the misuse detection collected the attack signatures in a database as the same as virus protection software to detect the relate attacks. They proposed an algorithm to use the known signature to find the signature of the related attack quickly.

III. IDS FUNCTIONING MODELS

The Intruder tries to attack hosts present on this network. Snort sensor captures the intruder's data and stores it in MySQL database using output plug in. A user looking at intrusion data collected by Snort through web browser.[1][2]

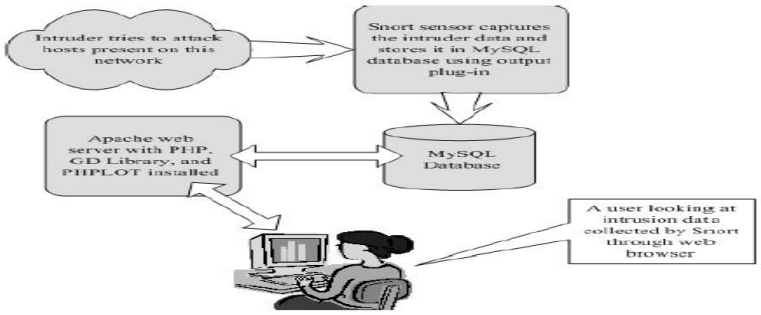


Figure 3.1 Block Diagram of Intrusion Detection System

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

Snort stores this data in the MySQL database using the database output plug-in. Apache web server takes help from ACID(Analysis Control for Intrusion Database), PHP, GD library and PHPLOT package to display this data in a browser window when a user connects to Apache. A user can then make different types of queries on the forms displayed in the web pages to analyze, archive, graph and delete data. In essence, you can build a single computer with Snort, MySQL database, Apache, PHP, ACID, GD library (graphic display library) and PHPLOT (tool to draw graphs).

IV. COMPONENTS OF SNORT

Snort is logically divided into multiple components. These components work together to detect particular attacks and to generate output in a required format from the detection system. A Snort-based IDS consists of the following major components: [3]

A. Packet Decoder
B. Preprocessors
C. Detection Engine
D. Logging and Alerting System
E. Output Modules

Figure 4.1 shows how these components are arranged. Any data packet coming from the Internet enters the packet decoder. On its way towards the output modules, it is either dropped, logged or an alert is generated.

1) Packet Decoder: The packet decoder takes packets from different types of network interfaces and prepares the packets to be preprocessed or to be sent to the detection engine. The interfaces may be Ethernet, SLIP, PPP and so on.[3]
2) Preprocessors: Preprocessors are components or plug-ins that can be used with Snort to arrange or modify data packets before the detection engine does some operation to find out if the packet is being used by an intruder. Some preprocessors also perform detection by finding anomalies in packet headers and generating alerts. Preprocessors are very important for any IDS to prepare data packets to be analyzed against rules in the detection engine.[3]

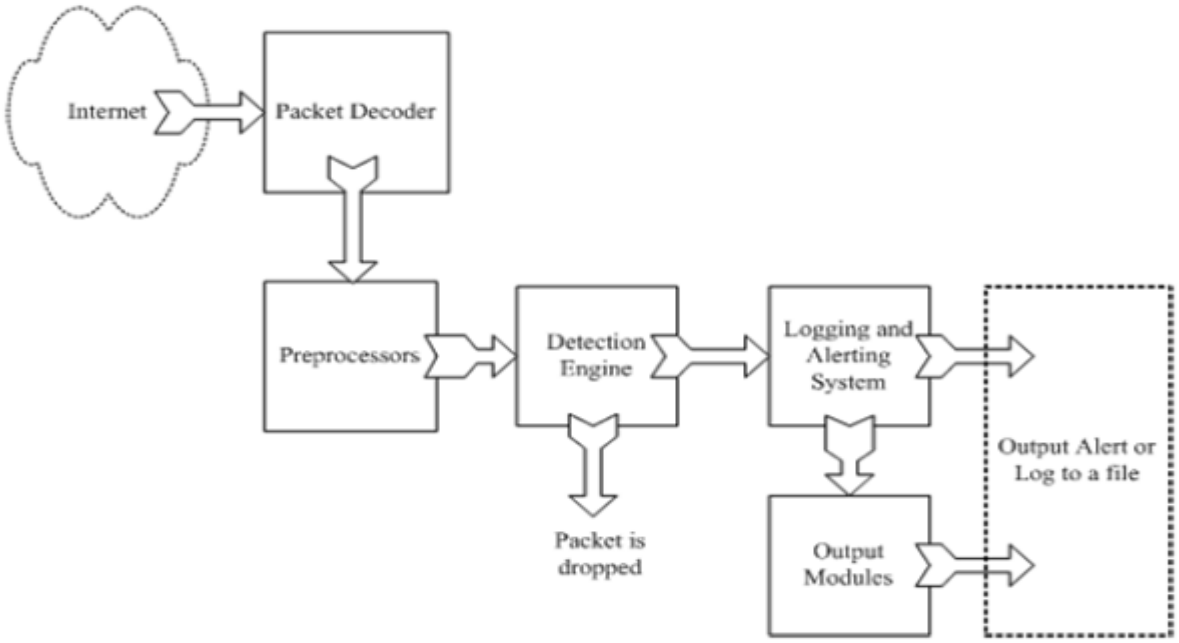


Figure 4.1: Components of Snort.

3) The Detection Engine: The detection engine is the most important part of Snort. Its responsibility is to detect if any intrusion activity exists in a packet. The detection engine employs Snort rules for this purpose. The rules are read into internal data structures or chains where they are matched against all packets. If a packet matches any rule, appropriate action is taken; otherwise the packet is dropped. Appropriate actions may be logging the packet or generating alerts.[3]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

The detection engine is the time-critical part of Snort. Depending upon how powerful your machine is and how many rules you have defined, it may take different amounts of time to respond to different packets. If traffic on your network is too high when Snort is working in NIDS mode, you may drop some packets and may not get a true real-time response. The load on the detection engine depends upon the following factors:

a) *Number of rules*
b) *Power of the machine on which Snort is running*
c) *Speed of internal bus used in the Snort machine*
d) *Load on the network*

When designing a Network Intrusion Detection System, you should keep all of these factors in mind. Note that the detection system can dissect a packet and apply rules on different parts of the packet. These parts may be:

e) The IP header of the packet.
f) The Transport layer header. This header includes TCP, UDP or other transport layer headers. It may also work on the ICMP header.
g) The application layer level header. Application layer headers include, but are not limited to, DNS header, FTP header, SNMP header, and SMTP header. You may have to use some indirect methods for application layer headers, like offset of data to be looked for.
h) Packet payload. This means that you can create a rule that is used by the detection engine to find a string inside the data that is present inside the packet.
4) *Logging and Alerting System:* Depending upon what the detection engine finds inside a packet, the packet may be used to log the activity or generate an alert. Logs are kept in simple text files, tcpdump- style files or some other form. All of the log files are stored under /var/log/snort folder by default. You can use –l command line options to modify the location of generating logs and alerts. [3]
5) *Output Modules:* Output modules or plug-ins can do different operations depending on how you want to save output generated by the logging and alerting system of Snort. Basically these modules control the type of output generated by the logging and alerting systems. Depending on the configuration, output modules can do things like the following:

Simply logging to /var/log/snort/alerts file or some other file[3]

1) Sending SNMP traps
2) Sending messages to syslog facility
3) Logging to a database like MySQL or Oracle. You will learn more about using MySQL later in this book
4) Generating eXtensible Markup Language (XML) output
5) Modifying configuration on routers and firewalls.
6) Sending Server Message Block (SMB) messages to Microsoft Windows-based machines

V. ANALYSIS CONSOLE FOR INTRUSION DATABASES (ACID)

It is a tool used to analyze and present Snort data using a web interface. It is written in PHP. It works with Snort and databases like MySQL, and makes information available in the database to the user through a web server. ACID consists of many Pretty Home Page (PHP) scripts and configuration files that work together to collect and analyze information from a database and present it through a web interface. A user will use a web browser to interact with ACID.[9]

ACID offers many features:

1) Searching can be done on a large number of criteria like source and destination addresses, time, ports and so on, as shown in
2) Packet viewing is used to view different parts of packet. You can view different header parts as well as the payload.
3) Alerts can be managed by creating alert classes, exporting and deleting and sending them to an e-mail address.
4) Graphical representation includes charts based upon time, protocol, IP addresses, port numbers and classifications.
5) Snapshots can be taken of the alerts database. As an example, you can view alerts for the last 24 hours, unique alerts, and frequent alerts and so on.
6) You can go to different who is a database on the Internet to find out who owns a particular IP address that is attacking your network. You can then contact the responsible person to stop it. The who is database contains information about owners of domain names and IP addresses.

VI. SNORTSAM

SnortSam is a tool used to make Snort work with most commonly used firewalls. It is used to create a Firewall/IDS combined solution. You can configure your firewall automatically to block offending data and addresses from entering your system when intruder activity is detected. It is available from http://www.snortsam.net/ where you can find the latest information. The tool consists of two parts:[10]

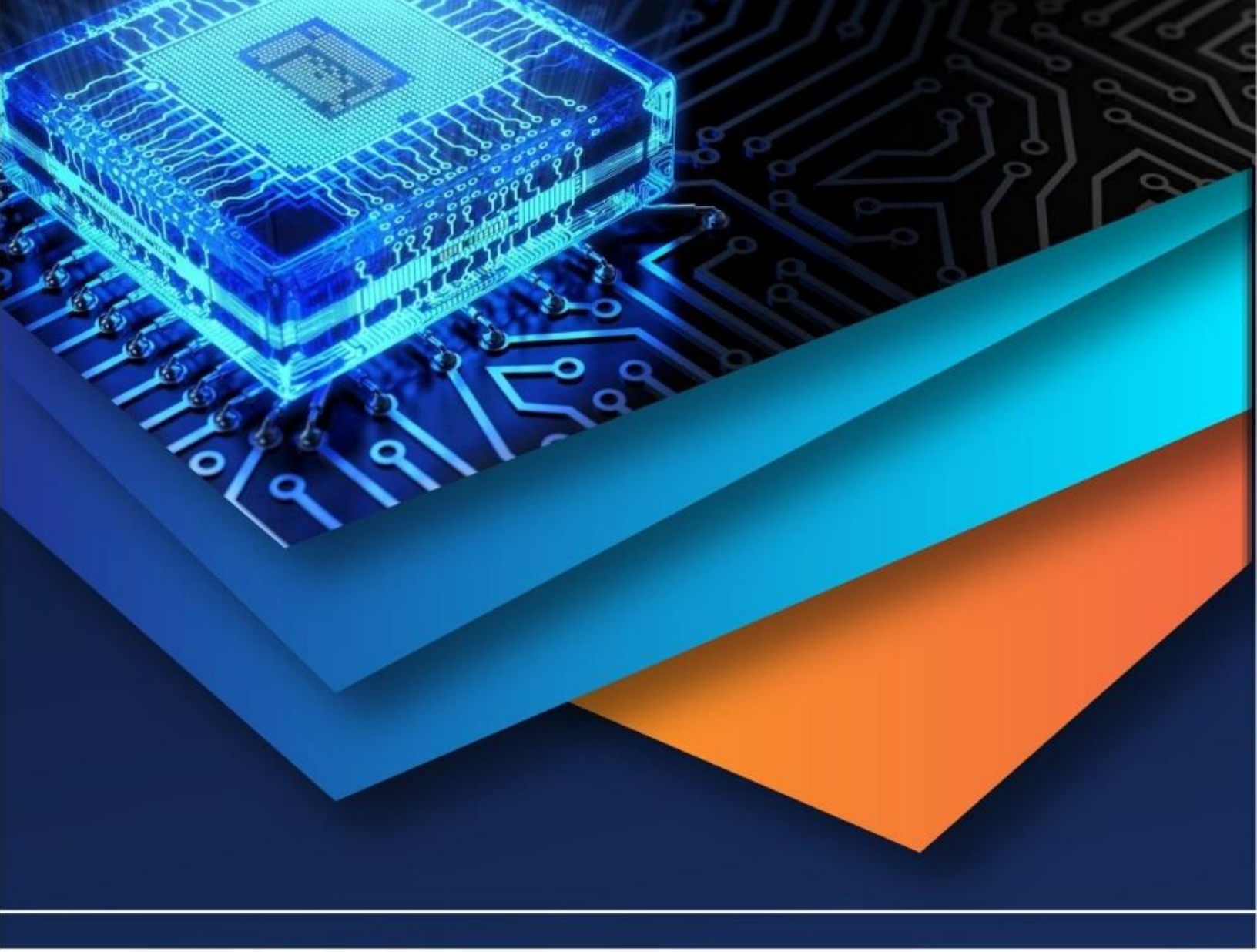
A. A Snort output plug-in that is installed on the Snort sensor.
B. An agent that is installed on a machine close to Firewall or Firewall itself. Snort communicates to the agent using the output plug-in in a secure way.

VII. CONCLUSION AND FUTURE WORK

Intrusion Detection System using Snort sensor ensures to detect anomaly attacks in both Network and Host systems .The IDS with ACID tool to analyse the information available in MySQL database. The System provides PHPLOT to display the amount of vulnerability attack using graphs. The Snort can be implemented based on the structure of your networks and hosts. In future IDS with Snort can be implemented in Cloud infrastructure to detect the unknown attacks and intruder's behaviour using data miming algorithms.

REFERENCES

[1] Intrusion detection FAQ at http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.html.
[2] Snort FAQ at http://www.snort.org/docs/faq.html.
[3] Snort web site at http://www.snort.org.
[4] Marc Norton, Daniel Roelker, "Snort 2: Protocol Flow Analyzer", 6/2002.
[5] SourceFire Inc., "Snort 2: Detection Revisited", 2/2002
[6] Muhammad Imran Shafi, Muhammad Akram, Sikandar Hayat, and Imran Sohai, l "Effectiveness of Intrusion Prevention Systems (IPS) in Fast Networks", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 6, JUNE 2010, ISSN 2151-9617.
[7] John McHugh, "Intrusion and intrusion detection", IJIS (2001).
[8] Hu Zhengbing, Li Zhitang,Wu Junqi," "A Novel Network Intrusion Detection System (NIDS) Based on Signatures Search of Data Mining",IEEE Computer Society,2008
[9] ACID is available from http://www.cert.org/kb/acid/
[10] SnortSam at http://www.snortsam.net/.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY