Comparative Study and Analysis of Network Intrusion Detection Tools

Dhanashri Ashok Bhosale
Department of Computer Engineering
Ramrao Adik Institute of Technology
Nerul, Navi mumbai, India
dhanashripatil313@gmail.com

Vanita Manikrao Mane
Department of Computer Engineering
Ramrao Adik Institute of Technology
Nerul, Navi mumbai, India
vanitamane1@gmail.com

***Abstract*—Security has a significant influence in network management. One of the most common way to secure information in the computer from malicious use is IDS Intrusion detection system(IDS) is most prominent to secure a computer and network against intrusion. IDSs primarily intended to preserve the availability, confidentiality and Integrity(CAI)of network and computer.IDS can be broadly classified in two categories: Network intrusion detection system (NIDS) and Host intrusion detection system(HIDS). NIDS is main part of any network security architecture, which monitors network traffic for predefined suspicious activity or patterns and alert system administrators. Nowadays ,many IDSs tools are available such as commercial as well as open source tools. Open source tools promotes a global access through free license. In paper we found study of three popular NIDS tools : Snort, Suricata, Bro.**

Keywords— alert; authentication; intrusion; vulnerability

I. INTRODUCTION

Organization's information system available to wholesome internet users. Hostile users or hackers can get access to an organization's confidential systems in various way. These are, software flaws called vulnerabilities , cease in network management tasks, leaving systems to default configuration. Avoid such intrusions IDS acts complementary to firewall. To protect network and computers from malicious traffic IDS are useful.

Range of Open Source platforms are available for the users, as per the applications requirement. This paper is an overview of different tools Snort, Bro and Sucricata. Many Open Source IDS tools are available for the consumers. Each tool is appropriate for distinct application as it follows different methodology.

A. Overview of Intrusion Detection System

Intrusion detection is the process of observing the activities in a network and analyzing them for indication of an intrusion. Intrusion is an attempt to compromise the integrity, availability or the confidentiality of the network or computer[6] .

Basically, there are two different possibilities to collect information in a network. Either the IDSs analyze the network packets captured form the backbone of the network or it analyze data generated by the host, that is the application or the operation system on the individual nodes. In the following network-based and host-based approaches are introduced:

*2) Host-Based IDSs:*HIDS scans and analyze file system modification,application logs, system calls and other host activities.This analysis helps to identify the intrusion such as illegitimate remote login attempt to acess restricted data.Generally ,HIDS works with NIDS[7].

3) Network-Based IDSs: NIDS scans network traffic to identify hostile activity like aim to break into computer, denial of service attacks ,port scans by using approach such as packet sniffing to gather network traffic data[7].

B. Intrusion Detection Methodologies:

After gathering of data from the activities and events in the network, the information has to be processed to detect attacks. This is done by the IDS analysis. As describes for this purpose misuse detection or signatures- based detection and anomaly detection. Whereas introducing a third method, named specification-based detection. These three methods are being discussed in the following[4]: introduced:

1) Misuse Detection: To detect attacks misuse detection uses a large database of known attacks and matches them with the occurring events. In the known attacks the system looks for a unique pattern, the so called signature. Therefore, this technique is sometimes also named as **signature-based detection** or **Knowledge based detection**.

*2) Anomoly Based Detection:*Anomaly detection operates with a profile that represents the status of all activities, i.e. activities that do not belong to an attack or to the preparation of one. Whenever an event is monitored that does not into the profile, the system has to decide whether it is an attack. For this purpose it works with a threshold. once the threshold is exceeded, it raises an alarm.

3) Stateful Protocol Analysis: A system that uses Stateful protocol analysis (SPA). It defines a set of constraints for a correctly behaving program or protocol. These constraints define exactly, what an application is allowed to do. It monitors the operations of the program or protocol against the constraints. The technique has an ability to identify unknown attacks with a lower false positive rate than the anomaly

978-1-4673-9223-5/15/$31.00 ©2015 IEEE

detection.SPA helps to detect unknown attacks with a minimal false positive rate than anomaly detection. It is also known as **specification-based detection**.

II. OPEN SOURCE INTRUSION DETECTION TOOLS

There are many open source IDS tools are available in open space, but in this paper our analysis is restricted to three popular NIDS tools: Snort, Suricata, Bro.

A. Snort

Snort was created in 1998 by Martin Roesch. Snort is able to seize live traffic within a network, logs packets and along with this it does analysis of captured packets. Snort is compatible with most operating system such as Linux, Mac OS X, FreeBSD, Open BSD, UNIX and Windows[10].Snort can be operated in IDS and IPS mode as well[5]. Structure of snort is illustrated in fig. 1.The packet capture module, the detection rules, preprocessor and alert output these are components of Snort which can be configured separately[10] . Snort is single threaded engine.

1) Packet Capture Library: It captures packets from different network interfaces within a network[3]. On Linux and UNIX like systems it uses libpcap library and on Windows systems uses WinPcap.

2) Packet Decoder: Packet inspects packet headers and examines for any peculiarities. Packet data is then decrypted for furthermore processing.

*3) Preprocessor:*It put together TCP stream and decrypts HTTP URI after that delivers data to detection engine.

4) Deletion Engine: Detection engine is most important part of Snort, It applies rules to packets Checks packages against the various options in the snort rule files.

5) Output Plugins: It gives final output by analyzing logs and alerts.

Snort having following advantages: Snort can easily be installed on any type of network, Snort is having detailed and scrutinized database of signatures, lightweight, Snort can act as a Intrusion Prevention System(IPS) also. Even though snort is most popular open source IDS/IPS it has the disadvantages also information overload , rules database is very large, monitoring packets in large network is an expensive task[9], fails to detect fragmented packets at high speed networks (greater than 5Gbps)[3].

Features of Snort:

Some of the key features of snort are:

- Scalability
- Flexibility and Usability
- Live and Real-Time
- Flexibility in Deployment
- Speed in Detecting and Responding to Security Threats
- Modular Detection Engine[2]

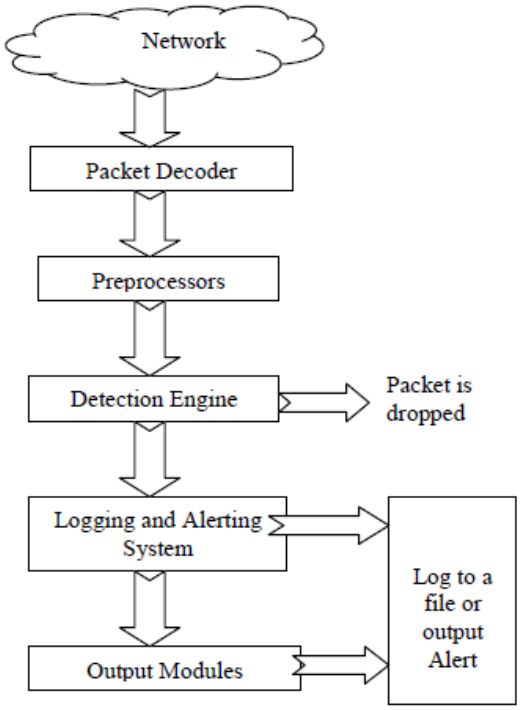

Fig. 1. Structure of Snort [3]

B. Suricata

The suricata is a somewhat newly discovered open-source IDS. It is evolved by Open Information Security Foundation(OISF).Suricata is suitable for many operating systems like Mac, UNIX, Linux, Free BSD, Windows.

The working mode of Suricata are same as Snort. It can be deployed as a IDS or as an IPS. In Suricata data flow is like packets are seized, decrypted, processed and then analyzed as shown in fig.2.Suricata follows a multithreaded approach whereas Snort is single threaded[2].

1) Capture Module: Once a device is initialized it will begin collecting packets and passing them to Suricata .Suricata then acts as a thin wrapper around the data provided, making it compatible with the link type decoders[11].

2) Decode Module:Decode module decodes packets captured by capture module into Suricata supported data structure. The currently supported link types are as follows: LINKTYPE_LINUX_SLL,LINKTYPE_ETHERNET, LINKTYPE_PPP, LINKTYPE_RAW[11].

3) Detect Module: Following tasks such as loading all signatures, initializing detection plug ins , creating detection groups for packet routing and finally running packets through all rules , are taken care by detection module[11].

Some of the advantages of Suricata are: Multithreaded architecture, Supports all operating system, Automatic detection of protocols with high performance, Network Security Monitoring (NSM), Filtering of alerts and events. Although Suricata is having some advantages and some

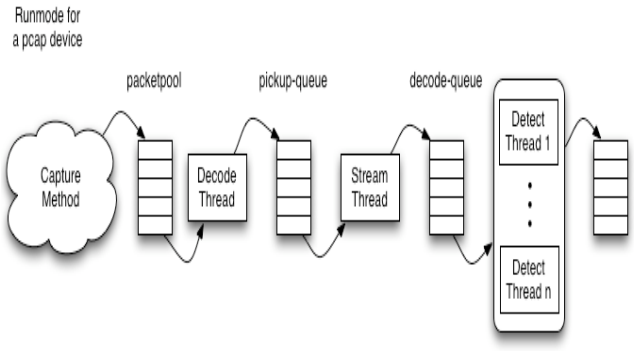

Fig.2. Structure of Suricata[2]

disadvantages, which are : CPU utilization is more and up to date information is not available.

Features of Suricata:

The salient features of Suricata are[11]:

- IDS/IPS
- High Performance
- Automatic protocol detection
- Network Security Monitoring

C. Bro

Bro IDS is emphasizing on network security. It gives extensive for network traffic analysis. Bro identifies peculiarities while scanning network traffic. It detects anomalies while inspecting network traffic. Bro is fully functional IDS and not entire IPS. Bro works with only UNIX like systems.

Sructure of Bro is as shown in fig. 3. It is made up of following modules such as libpcap, Event Engine, Policy Script Interpreter [12].

1) Libpcap: Bro uses libpacap packet capture library to capture packets within a network. It strains insignificant traffic coming from network interfaces at network layer[3].

*2) Event Engine:*Event engine receives filtered traffic from libpcap. This layer performs various integrity check to assure that packets are well formed , for that it verifies the IP headers checksum is correct or not. To this place IP fragments are put together therefore network layer analyzer able to access entire IP packets. It sends events to the policy layer.

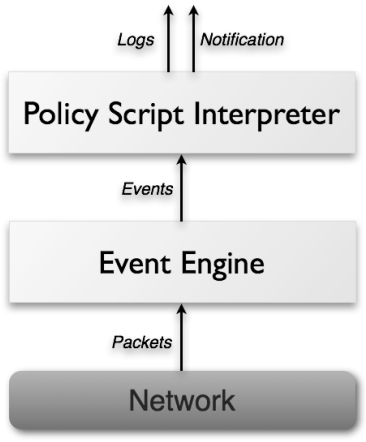

Fig.3. Structure of Bro[12]

3) Policy Script Interpreter:It is important to note that Bro policy scripts (rules) are written in its own Bro scripting language that does not rely on traditional signature detection. It analyzes network while trying to detect anomalies[1].

Bro is having some advantages which are : Bro can detect, not only attacks hidden by natural TCP segmentation, but also an important type of subterfuge attacks, Bro-ids is capable to perform application level deep packet inspection, Bro is capable in doing tunnel detection and analysis, improved forensic capabilities with the support of time machine, a high-performance packet bulk recorder with a Bro interface. Along with this advantages it is having some disadvantages also. Bro requires a UNIX like platform, it is command line interpreter, reports information to log files[9].

Features of Bro:

Bro supports a wide range of analyses through its scripting language. Yet even without further customization it comes with a powerful set of features[12]:

- Deployment:
- Analysis
- Scripting Language
- Interfacing

III. Comparison and Analysis

Table I shows the comparison of Snort ,Suricata and Bro on basis of different features such as: Supported platform ,License ,IPS feature, PGP signed, Support to high speed network ,Configuration of graphical user interface(GUI), Offline analysis,Threads,IPV6 Support, Installation and Deployment, Event logging.

Snort and Suricata supports almost all popular operating systems and whereas Bro runs on UNIX like operating system only.

Snort and Suricata is licensed under GNU(General Public License). The main idea is that the software released under GPL is free. You have the freedom to freely share it and change it. In exchange, you have to share any modifications you make to the code or else ask the owner to relicense the code under a different license that meets your needs. Bro is distributed comes under the BSD (Berkeley Software Distribution) license. BSD license allows you to do practically anything with the software. It is less restrictive than the GPL.

Snort in inline mode or with Q option act as a IPS. In Suricata enable nfqueue to activate IPS mode. While Bro is not supporting IPS feature.

Bro is suitable to run in high speed environment and able to capture data from Gbps networks. whereas Snort drops packets and slowdowns traffic in high speed environment.

Bro does not have GUI and to work with Bro one should have good grip on shell commands whereas Snort and Suricata has a GUI which makes it more accepted .In Snort when compile with -enable -ipv6 option then it will support IPV6.

TABLE I. COMPARATIVE STUDY OF NIDS TOOL

Parameters	Snort	Suricata	Bro
Supported Platform	Win, MacOS, Unix	Win, MacOS, Unix	Unix like system, MacOS
License	GNU GPL V2	GNU GPL V2	BSD
IPS feature	Yes	Yes	No
PGP signed	Yes	Not Applicable	No
Support to high speed network	Medium	High	High
Configuration GUI	Yes	Yes	No
Offline Analysis	Yes for multiple files	Yes for single file	Yes for single file
Threads	Single Thread	Multithreaded	Single Thread
IPV6	Yes	Yes	No
Installation and Deployment	Easy	Easy	Difficult

Compared to Snort and Suricata, which is more a plug and play system, Bro is more difficult and time consuming to deploy and to understand.

IV. CONCLUSION

Network security have become necessary due to increased usage of internet. With increased usage of networks, the vulnerabilities have also increased into the network system. Hence using only intrusion prevention techniques are not enough. To detect this vulnerabilities we need intrusion detection. It helps to detect attacks or intrusions into networks. In this survey, we try to introduce the IDS methodologies, which may be a mainly used in various tools. Finally, we introduce the NIDS tools that can help to protect the networks. IDS methodologies, which may be a mainly used in various tools. Finally, we introduce the NIDS tools that can help to protect the networks.

Bro and snort have different functions and they behave differently in the architecture. Bro provides us with the facility of experimentation. It helps develop new ways of looking towards data. It is primarily suited for anomaly detection. If the IDS is required to be fine-tuned according to the network and applications then Bro is much better adapted and suitable for Gigabit network as compared to Snort. On the other hand Snort is not appropriate for high-speed networks or even for customization to a larger extent. Its highly simple to deploy and is capable of providing low-end IDS. It is mainly signature-based and is not up to the mark for anomaly identification and analysis.

Suricata is multi-threaded architecture requires more memory and CPU resources than Snort. We saw that the aggregate CPU use of Suricata was nearly double that of Snort, and Suricata used over double the amount of RAM used by Snort. This could be attributed to the overhead required to manage the multiple detection threads in Suricata. Considering these few significant differences its quite clear that Snort, Suricata and Bro perform differently as far as speed and efficiency if the network are concerned.

REFERENCES

[1] John Gerber,"Three Open Source IDS/IPS Engines".

[2] Suricata User Guide https://redmine.openinfosecfoundation.org/project /suricata/wiki/What_is_Suricata.

[3] Pritika Mehra, "A brief study and comparision of Snort and Bro Open Source Network Intrusion Detaction System International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 6, August 2012.

[4] ung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung, "Intrusion detection system: A comprehensive review, Journal of Network and Computer Applications, Volume 36, Issue 1, January 2013, Pages 16-24, ISSN 1084-8045.

[5] Adeeb Alhomoud, Rashid Munir, Jules Pagna Disso, Irfan Awan, A. Al-Dhelaan,"Performance Evaluation Study of Intrusion Detection Systems", Procedia Computer Science, Volume 5, 2011, Pages 173-180, ISSN 1877-0509.

[6] Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md. Abu Naser Bikas, "An Implementation of intrusion detection system using genetic algorithm", International Journal of Network Security and Its Applications IJNSA, Vol.4, No.2, March 2012.

[7] J. Deepa, V. Kavitha, "A Comprehensive Survey on Approaches to Intrusion Detection System", Procedia Engineering, Volume 38, 2012, Pages 2063-2069, ISSN 1877-7058.

[8] Herve Debar , Marc Dacier , AndreasWespi ,"Towards a taxonomy of intrusion-detection systems, Computer Networks 31 1999, 805822.

[9] Surya Bhagwan Ambati,Deepti Vidyarthi, "A brief study and comparision of Open Source Intrusion Detaction System Tools International Journal of Advanced Computational Engineering and Networking, Vol. 1, Issue 10, December 2013.

[10] Snort NIDS Tool available at https://www.snort.org/.

[11] Suricata NIDS Tool available at http://suricata-ids.org/features/.

[12] Bro NIDS tool available at https://www.bro.org/.