ISSN : 2278 – 1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 6, August 2012

A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems

Pritika Mehra

Post Graduate Department of Computer Science and Applications,

Khalsa College for Women, Amritsar, Punjab, India.

***Abstract* - Security administration plays a vital role in network management tasks. The intrusion detection systems are primarily designed to protect the availability, confidentiality and integrity of critical network information systems. There are plenty of IDSes to choose from, both commercial and open source. Since most of the commercial intrusion detection systems are at typically thousands of dollars and they tend to represent a significant resource requirement in themselves, for small networks, use of such IDS is not feasible. Therefore mostly open source IDS are being used. This paper provides a general working behaviour, features and comparison of two most popular open source network IDS - SNORT & BRO.**

Keywords-alerts, intrusion, logging, network traffic, open source, packets

I. INTRODUCTION

Intrusion detection system is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).There are two types of IDS - Network and Host IDS. A Network Intrusion Detection System (NIDS) is an intrusion detection system that tries to identify malicious action such as denial of service attacks; port scans or even attempts to crack into computers by monitoring network traffic. A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyzes the internals of a computing system rather than the network packets on its external interfaces. A network intrusion by malicious or unauthorized users can cause relentless disruption to networks. Therefore the development of a robust and reliable network intrusion detection system (IDS) is increasingly important. Open Source IDS are increasingly being used as they offer benefits and ease in the prevention of security issues brought to network and system administrators. They can dynamically examine a network by providing security from intrusions in the open traffic of the Internet. There are several open source Network based IDS such as Snort, Bro, Shadow, M-Ice, Shoki, Spade, Prelude, Firestorm, AAFID etc. The most popular and widely used among these are Snort and Bro. This paper provides a general working behavior, features and comparison of two most popular open source network IDS - SNORT & BRO.

This paper is organized as follows: Section II and III give an overview & general working behavior of Snort and Bro respectively. Section IV compares Snort and Bro based on different parameters and features. Finally in section V conclusion is provided.

II. SNORT

SNORT is a free and open source network intrusion detection and prevention system created by Martin Roesch in 1998. Snort has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. It performs protocol analysis, content searching, and content matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

There are three main modes in which Snort can be configured: sniffer, packet logger, and network intrusion detection. Sniffer modes read the network packets and display them on the console in a continuous stream. Packet logger mode logs the network packets to the disk. Network intrusion detection mode is the most complex mode. Network Intrusion detection mode monitors network traffic and analyze it against a rule set defined by the user and then perform a specific action based on what has been identified.

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:

a. Packet Decoder
b. Preprocessors
c. Detection Engine
d. Logging and Alerting System
e. Output Modules

a. *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.

b. *Preprocessors or Input Plug-ins*: 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. They are also used to

ISSN : 2278 – 1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 6, August 2012

normalize protocol headers, detect anomalies, packet reassembly and TCP stream re-assembly.

c. *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.

d. *Logging and Alerting System*: It generates alert and log messages depending upon what the detection engine finds inside a packet.

e. *Output Modules*: Output modules or plug-ins process alerts and logs and generate final output.

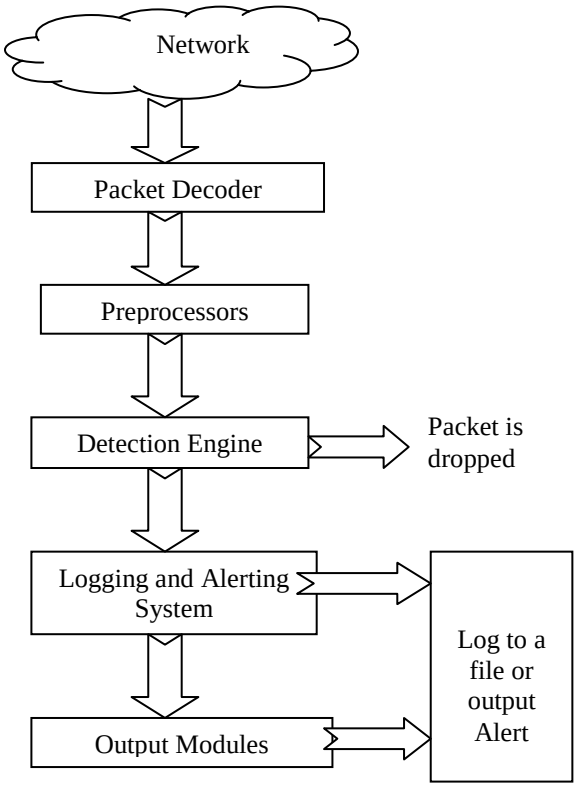

Fig 1 Components of Snort

Snort is supported on a number of hardware platforms and operating systems. Currently Snort is available for the following operating systems: Linux, OpenBSD, FreeBSD, NetBSD, Solaris (both Sparc and i386), HP-UX, AIX, IRIX, MacOS, and Windows. Thus Snort toolkit runs on any modern operating system and any old hardware one has. It helps to fix a number of network problems and intrusion detections.

III. BRO

Bro is an open-source, Unix-based Network Intrusion Detection System (NIDS) that passively monitors network traffic and looks for suspicious activity. Bro was developed by Vern Paxson in the Network Research Group at Lawrence Berkley National Lab, and by the International Computer Science Institute in 1998. BRO has the ability to perform multi-layer analysis, Behavioral monitoring, Policy enforcement, Policy-based intrusion detection and Logging network activity Bro detects intrusions by first parsing network traffic to extract its application-level semantics and then executing event-oriented analyzers that compare the activity with patterns deemed troublesome. Its analysis includes detection of specific attacks (including those defined by signatures, but also those defined in terms of events) and unusual activities (e.g., certain hosts connecting to certain services, or patterns of failed connection attempts). Bro analyze the traffic in three phases. First Bro filters the traffic, discarding elements of minimal importance to its analysis. The remaining information is sent to its "event" engine, where Bro interprets the structure of the network packets and abstracts them into higher-level events describing the activity. Finally, Bro executes policy scripts against the stream of events, looking for activity that the rules indicate should generate alerts or actions, such as possible intrusions.

Components of Bro

Bro IDS consists of the following major components:

a. libpcap
b. Event Engine
c. Policy Script Interpreter

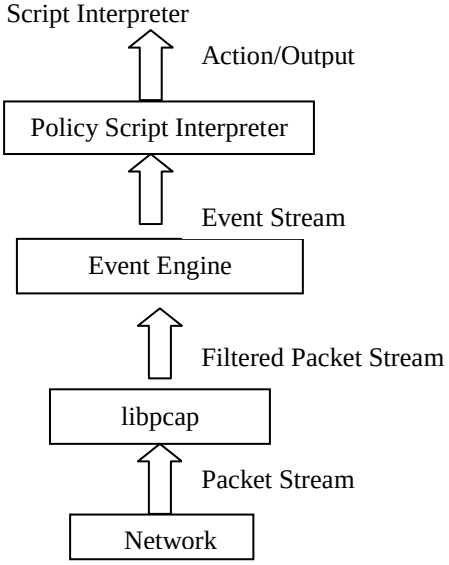

Fig 2 Components of Bro

a. *Libpcap*: Bro needs the pcap library to capture packets from the network interfaces. The name for this API is libpcap in Unix-like systems (WinPcap in Windows).libpcap takes care of all the traffic that comes from the network layer and filters out the non-important elements. The filtered packet stream is forwarded to the Event engine.

ISSN : 2278 – 1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 6, August 2012

b. *Event Engine*: It captures the packets from the libpcap and puts them together to become events explaining the performed actions. Event Engine is written in C++.

c. *Policy Script Interpreter*: The Policy Script Interpreter takes the high-level events generated by the Event Engine and compares these with the policy scripts in the system. The events are sorted in a FIFO list which means the first that comes along are the first that is processes. Policy Script Interpreter takes action if it detects any suspicious and dangerous actions or it discards other events not defined in the policy scripts. Traffic that seems like attacks but aren't (false negatives), can be detected at this point, but if the policy scripts are good, this will be minimal. It is written in Bro language.

To be able to run Bro in a computer network a computer running a UNIX-like system is needed. The system can run Linux and Solaris distributions or FreeBSD.

Bro targets high-speed (Gbps), high-volume intrusion detection. It is intended for use by sites requiring flexible, highly customizable intrusion detection. Bro has been developed primarily as a research platform for intrusion detection and traffic analysis.

IV. COMPARISON OF SNORT & BRO

Comparison of Snort and Bro is made on the basis of different parameters such as speed, signatures, flexibility, deployment, interface and operating system capability.

a. *Speed*: Bro IDS has the ability to run in high-speed environments. Bro is very effective and able to capture data from Gbps networks. This makes it suitable for more large scale networks whereas Snort IDS is not able to run prefect in high speed networks without dropping packets or slowing down the traffic.

b. *Signatures*: When it comes to the signatures used for detecting intrusions, the Bro signatures are more sophisticated than the signatures used in Snort.

c. *Flexibility*: Bro is a flexible intrusion detection system with the possibility of being configured and then specified for its intended computer network. Bro comes with pre-written policy scripts which can be used right out of the box and these will detect the most well known attacks. If you want to add more features and want to detect more attacks, you can customize own policy scripts containing your own rules. Snort has no provision for customization and is less flexible. New functionality in Bro is added through policy Scripts which are written in Bro Language. New functionality in Snort is added through C language.

d. *Deployment*: Compared to Snort, which is more a "plug and play" system, Bro is more difficult and time consuming to deploy and to understand.

e. *Interface*: Snort has a graphical user interface which makes it more popular. Bro's lack of a user interface (GUI) can also be considered as a disadvantage since one should have good knowledge of how a UNIX system works and be able to handle shell commands to understand this system.

f. *Operating System Compatibility*: The Snort can run on all of today's most popular operating systems and is not confined to a fully vested server hardware platform whereas Bro is confined to UNIX like operating systems.

Snort is packet oriented whereas Bro is connection oriented.

Parameter	Bro	Snort
Contextual signatures	yes	no
Flexible site customization	high	medium
High speed network capability	high	medium
Large user community	no	yes
Configuration GUI	no	yes
Analysis GUI	a few	a lot
Installation /deployment	difficult	Easy
Operating System compatibility	Unix	Any

Table 1: Comparison of Snort & Bro

V. CONCLUSION

There are several IDS systems available in the market and some of them are open-source free of charge IDS systems and others are not. Snort & Bro is a free of charge IDS system and available for download at their WebPages by everyone. Other commercial IDS system can be very expensive so Snort, Bro and other freeware IDS systems are therefore a good choice if you don't want to invest too much money in such systems.

When choosing an intrusion detection system, Bro may not be the best choice if user is not an UNIX expert and want to apply a main IDS system to computer network. On the other hand, as described by the developers themselves, Bro IDS is a system for experimentation. So if one wants to experiment or want an extra Intrusion Detection System as a supplement to main IDS, one should choose Bro. If user wants to customize IDS according to his network then also Bro is a good choice. Bro is more effective for Gbps networks as compared to Snort.

Snort is not suitable for very high speed networks. It is not a system for experimentation and customization. Snort focuses on performance and simplicity which makes it best choice to be run on any operating system. Snort is one of the best known lightweight IDS. Snort can easily be deployed on any node of a network, with minimal disruption to operations.

Study can be further extended to compare Snort and Bro with more parameters such as false alarms, maintenance, firewall interactivity etc.

REFERENCES

[1] Rafeeq Ur Rehman, Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, Prentice Hall PTR
[2] Douglas J. Brown, Bill Suckow and Tianqiu Wang, A Survey of Intrusion Detection Systems.
[3] Hilmi Gunes Kayacik, A. Nur Zincir-Heywood, A case study of three open source security management tools.
[4] Vern Paxson, Jim Rothfuss, Brian Tierney, Bro Quick Start Guide, University of California and the International Computer Science Institute.
[5] Martin Roesch, Snort - Lightweight Intrusion Detection for Networks, 13th USENIX Systems Administration Conference – LISA '99, Seattle, Washington, November 1999.
[6] Vern Paxson, Bro: A system for Detecting Network Intruders in Real-Time, Network Research Group, Lawrence Berkeley National Laboratory, 1999.
[7] Rebecca Bace and Peter Mell, NIST Special Publication on Intrusion Detection Systems, August 2001.
[8] Anders Orsten Flaglien, BRO - An intrusion detection system, Gjovik University College, November 2007.
[9] Alexandre Bartel, Comparison of Open Source Network Intrusion Detection System, November 2009.
[10] http://www.snort.org, Snort, last accessed April 2011
[11] http://en.wikipedia.org/wiki/Snort_(software), last accessed April 2011
[12] http://www.ohloh.net/p/bro-ids, Bro, last accessed April 2011.
[13] http://www.bro-ids.org, Bro intrusion detection system, last accessed April 2011.