Network Intrusion Detection Techniques and Open Source Tools

Dileep Kumar Singh¹, Praveen Kaushik²
¹Department of CSE, SOET, Jagran Lakecity University, Bhopal INDIA
²Department of CSE, MANIT Bhopal, INDIA

ABSTRACT
Today most of the human activities required the aid of computer network and internet services such as in banking, health, marketing, research etc. These systems are required to be monitored and protected from any intrusion attack in order to provide consistent and secure services to the users. To protect the confidentiality, Integrity and the availability (CIA) of network/internet based services/systems; Intrusion Detection Systems (IDS) are designed. There are various commercial as well as open source IDS tools are available with its own strength & weakness. This paper provides the general discussion and various features and comparison of the available open source IDS tools such as snort and bro.

Keywords— Intrusion Detection Systems, open source IDS tools, snort, bro.

I. INTRODUCTION
The number of intrusion incidents and attacks are increasing and becoming a biggest challenge in front of the network or system administrators to monitor and protect the networks or the services deployed, in order to provide consistent and secure services to the users. Annual report from the Asia Pacific Computer Emergency Response Team (APCERT) [1] indicates an increase in the security incidents each year. These intrusion incidents may destroy or disrupts the services consistency in terms of either confidentiality, Integrity, availability or the performance. So in order to maintain the user’s quality of services it is required to monitor the Network or computer services to prevent or detect and mitigate the intrusion incident and attacks.

An intrusion detection system (IDS) is a software or tool which monitors the network traffic for any suspicious activity and alerts the system or network administrator [2, 3]. There are various commercial as well as open source IDS tools are available such as snort and bro. This paper provides the general discussion and various features and comparison of the available open source IDS tools.

II. INTRUSION DETECTION SYSTEM (IDS)

An Intrusion Detection System (IDS) is a network security technology for detecting vulnerability exploits or deviation from the normal behavior against a target application or computer. There are Network based IDS (NIDS) and Host based IDS (HIDS) [4, 6]. NIDS perform the real time network monitoring for any intrusion attack in either in network segment or device and analyze the network protocol for any suspicious activity, whereas HIDS monitor a single device or host for any suspicious activities.

Figure 1: Intrusion Detection System
For detecting the intrusion in the network or host, there are two basic approaches – anomaly detection and the misuse detection/Signature based Detection [2, 3].

A. Anomaly detection:
This approach is based on the normal and abnormal behavior of the network or the system. If the network or the system will deviate from its normal behavior the IDS will detect it and generate the alert to the network or system administrator. Since this method is based on the system activity profile, it can identify and detect the new unknown intrusions. But the challenging part is to defining the normal behavior of the network or the systems.

B. Misuse detection/Signature based Detection:
This approach is based on the pattern matching of the predefined database of well known intrusion signatures/patterns. As soon as the match found the Signature based IDS will generate the alert to the network or system administrator. While Signature based Detection are very efficient for detecting the known intrusions, they are not be able to identify and detect the new unknown intrusions.

III. OPEN SOURCE INTRUSION DETECTION TOOLS

There are various open source intrusion detection tools are available, some of them are even equally or more powerful than the commercial IDS tools, such as snort, bro etc.

A. Snort IDS:
Snort IDS is leading amongst Open Source IDS from years. This network intrusion detection system excels in real time network traffic analysis and packet logging on IP networks. Snort detects intrusions by content searching & matching, protocol analysis and various pre-processors activities. Snort uses a flexible rule-based language to define traffic that it should log or pass with the detection engine. Snort uses libPcap (in UNIX) or winpcap (in Windows) for capturing the network traffic packets.

Snort Components – Main components of the snort IDS is shown in the figure-2 [7, 8].

- **Packet Capture Engine** – Captures the network traffic using pcap (libpcap or WinPcap) and using filters passes them to the Snort application.
- **Decoders & Preprocessors** – Packets are collected from different type of network interfaces (Ethernet, PPP etc.) packets decoders and translates specific protocol elements into an internal data structure and make them available for the preprocessors. Decoder watches the structure of network packets to make sure they are constructed according to specification. If a packet has a strange size, strangely set options, or uncommon settings, Snort will generate an alert. Preprocessor plug-ins test and inspect packet data before sending it to the detection engine.
- **Detection Engine** – compare data within every packet it receives to the rule options and test whatever part(s) of each packet contain(s) a particular string or value associated with a rule or not.
- **Logging & Alerting System** – Snort produce information to be displayed to network or system administrator. Snort creates alerts based on alerting rules within the preprocessors, the decode engines, and the detection engine.

Snorts can be configured to work in one of the four modes: Packet sniffing mode, packet logger mode, detection mode (NIDS) and prevention mode.

B. Bro IDS:
Bro is an open source, UNIX based network intrusion detection system which monitor and detect the suspicious activity on the networks. Bro is also having the deep packet inspection at application level and the forensic capabilities. Bro supports real time high speed and large
volume traffic monitoring. Bro having its own scripting language called bro scripting language, which can be used to write new security policies [5].

Bro architecture – Main components of bro ids is shown in figure-3.

Figure 3: Snort Architecture

Bro ids having mainly two components: Bro Event Engine and Bro Policy Script Interpreter. Bro event engine take the stream of filtered packets from the networks (captured using libpcap) and first perform the integrity check for the packets, if everything is ok then it converts them into the higher level events representing the various network activities such as HTTP request will be treated as the http_request event. Policy script interpreter interprets the written site security policy in Bro Scripting language, against the generated events by the event engine in order to check if any deviations in the network activity from the defined site security policy on the incoming network packet streams. If any intrusion activity is found, Bro will generate the alert to the network administrator [5, 9, 10].

IV. DISCUSSION

Snort and Bro both are the open source network IDS with the ability of signature and anomaly based detection of intrusion incidents. Both are having their own strength and weakness.

Snort is one of the most widely used open source NIDS which uses the rule-based language. The rules are defined, if any abnormal activities find in the networks; it generates the alert to the administrator. It is mainly known for the signature based NIDS. Apart from the large number of predefined rules provided by snorts, intrusion analyzers can also write their own rules using the simple rules description language supported by the snort. Snort can log the stream of real time network traffic in the tcpdump format. Apart from Intrusion detection, snort also having the capability of basic intrusion prevention by using the rules such as reject, drop etc.

Bro uses policy scripts written in the Bro Scripting language, in order to detect any deviation from the normal networks activities. Bro generates alert to administrator if any intrusion incident is detected. It supports both signatures as well as anomaly based intrusion detection and having the capability of intrusion prevention. Large numbers of pre-written standard security policy scripts are available with the Bro IDS, but the security analyzer can also write their own site security policy scripts using the very strong scripting language supported by the Bro IDS. Bro can also log the stream of real time packets from the network traffic in the tcpdump format.

Snort is available for mostly all the well known operating systems such as windows and UNIX based OS. Whereas Bro is available only for the UNIX based operating systems. Bro provides more flexibility for site configuration in compare to the Snort. Apart from the Command Line Interface (CLI), Snort is also available with various Graphical User Interfaces (GUI) such as BASE, Snorby, SQueRT etc., but Bro IDS is available only with the CLI interface. For the beginners Bro seems to be more complex to understand compared to Snort, might be because of un-availability of large number of well written document, manual or video tutorials compared to the Snort. This can be one of the reasons that Snort is more popular compare to the Bro IDS. Bro is more powerful IDS in dealing with the high speed networks such as GB networks compared to the Snort IDS. Unlike Snort (Snort 1.x), Bro IDS can also deeply inspect the application layer data and detect application layer protocols intrusion incidents as well as having the efficient network forensic capability.

V. CONCLUSION

As intrusion incidents are increasing, that might disrupt the network services by affecting confidentiality, integrity, availability or performance. It is required that there should be an efficient & effective network IDS. The comparative features and the general discussion over the available efficient & effective open source tools of Network IDS are presented and discussed in this paper.

REFERENCES