Journal of Education and Policy Review

www.cenresinpub.org
ISSN: 2277-0100
Volume 9, Number 1, 2017

REVIEW PAPER ON SNORT PERFORMANCE BOTLENECK SOLUTION AND PACKET INSPECTION

Abubakar Abdulkadir Mukhtar Abdulkadir
Department of Computer Education
Isa Kaita College of Education Dutsin-Ma, Katsina State
Email: Combuba2@yahoo.com, Elmukhtardtm@yahoo.com

Abstract: The increasing network performance in term of network packet rate had resulted performance bottleneck on snort malware detection as a result, many authors proposed solution to such problem. The paper describes some of the proposed system, their drawback, solution to the snort performance as well as packet inspection in snort intrusion system.

INTRODUCTION

As a result of vast increase in technology and lack of integrating good security practice in software and hardware design which has leads to backdoors, bugs and e.t.c a number of network attacks are increasing dramatically, ranging from denial of services, IP spoofing eavesdropping, mitnick, (MITM) man in the middle attack masquerading and malware attacks (Snehal and jadhav, 2010). These attacks have made traditional network security mechanism ineffective, which requires additional defense mechanism that can analyze, detect and mitigate these attacks. However, in order to address these challenges, intrusion detection system is now widely used as a network perimeter security. Intrusion detection has been almost studied nearly 20 years back (Ning and Jajodia,2001). Intrusion detection system is deployed in conjunction with other security mechanism to provide a better network defense against unauthorized access by user and malicious code attacks. However, several reasons make deployment of intrusion detection system to be unavoidably part of the entire defense system. Many systems and applications are deployed without much security consideration and this is as a result of lack of good security practices in computer related application design. An example of signature-based technique is Snort tool, which also experience a higher number of packet drooping. Snort tool is an

open source intrusion detection system widely deployed in middle sized industries and in most Campus networks. Because of its nature of flexible code, it has attract many researchers toward developing additional features that can meet user requirements or needs e.g. Snort MySQL pre-processor plug-in to monitor communication between Client and MySQL Server and to be able to detect any anomalous packets (Geddes Linda, 2009).

Organization of the Paper

The paper is organized in two (2) different part the first part deals with intrusion detection techniques, snort historical background and snort components while the second part deals with Snort performance bottleneck and solution and the snort network inspection.

Intrusion

The term intrusion can be described as a violation of security policy of systems with the aim of destroying or de-stabilizing its activities. In other word Intrusion is an unauthorized access to the network computing devices by the legitimate or un-legitimate user.

Intrusion Detection System

Nowadays, intrusion detection system is the most widely used and top growing network security technology used by many industries. These systems unlike firewall and other security related systems such as Honey pot are mainly designed to detect intrusion into a network. According to work by (Rani, 2009) many different forms of open source and commercial intrusion detection are obtainable to the best of user requirement e.g Snort, NitroGuard and Niksu netdetector. However, according to (Geddes Linda, 2009) say it has been estimated that the open source intrusion detection system has higher popularity in middle size industries than the commercial systems. These are as a result of high cost, real time support and ability to be configured to suite the user needs and platform implementations.

Network Intrusion Detection System

Network intrusion detection system is deployed in the network segment to observe and analyzes incoming network packets. The captured and analyzed

data is used to detect known attacks using the stored patterns or signatures of the system database. And also all of illegal activities are detected by scanning traffic for example illegal connection to the network services such as HTPP, SPOP and SMTP.

Host-Based Intrusion Detection

According to Suman (2010) defined host-based intrusion detection as software based intrusion detection system usually installed in the host computer that requires specific configuration. Therefore, based on the operating system, the host intrusion detection system is configure to deal with detection of security policy violations by analyzing the host local logs audit files, software calls and others. Basically, many types of host-based intrusion detection system combined both intrusion detection and prevention functions like network intrusion detection systems.

Signature Based Detection Technique

Signature detection techniques is an intrusion detection techniques in which a record of known attack signature is kept in the database and intrusion is detected by comparing signature pattern and the pattern that exist in the packet payload. In addition, network packet is search to indentify malicious byte. In this technique the signature is very easy to form, for efficient pattern matching to be done a reasonable amount of power is needed in respect to a specific number of rules. In addition, signatures of exploit are easily generated based on the specific service port it communicated with, for examples, system that communicate through the following services Domain name server (DNS), internet control message protocol (ICMP) and SMTP.But fixed behavioral pattern detections, increasing number of novel attack and inability to detect self modifying worm and virus has become catastrophic to this techniques (*Jyothsna et. al*, 2011).Similarly, advanced technologies are used to avoid this techniques also increasing in number of attack signatures contributed to the performance degradation.

Anomaly Based Detection Techniques

Basically, in anomaly based detection network behavior is learned and the learned network behavior is compared with the incoming network traffic to

detect an intrusion. (*Sandhu et. al,* 2011).In this technique many possibilities are used to detect anomalous behaviors. Data such as Kernel information, system logs records information of various software running in the system and normal packet characteristic are also collected and stored. Therefore, any deviation to this gathered information are recorded as anomalous metric used to measure and detect the deviation of the system behavior and Alarm is usually generated if deviation is found. The model development comprises of three different stages namely parameterization, training and detection stage .However, as the working stile of this technique defines on some protocols as such it's problem in rule setting and produce higher rate of false alarm the strength of this techniques over signature based engines is its ability to be able to deter any novel attack whose pattern has deviated normal traffic pattern (Ning, and Jajodia, 2001).

HISTORICAL BACKGROUND OF SNORT

Snort intrusion detection is an open source intrusion detection which is a signature based. Snort tool was originally design as a packet sniffer in 1998 by Marty Roesch which was named APE (Linda Geddes, 2009). Despite the function perform by the APE, Marty Roesch wanted to have a sniffer that can have additional feature or that can perform many functions such as ability to function in many different operating systems platforms. Windows Linux and UNIX are few among the interested operating system platform Marty Roesch wanted to have snort tool working on. Another desire by the Marty Roesch is the ability for the sniffer (APE) to display multiple difference network packets in the unique form. Much advancement on sniffer features come to being including the sniffer ability to not only capture packet but it can also filter it. This application is named libpcap. However, In December, 1998, snort become packet storm which has only one thousands and six hundred (1600) lines of code that are compiled in only two files. Marty's uses snort to perform many work such as monitoring his cable modern and debugging his network applications at around January 1999 snort become a fully features signature based detection system. In addition on December 1999 a new version of snort 1.5 was released, which was used as a light weight intrusion detection system at that time snort used many different plug-in

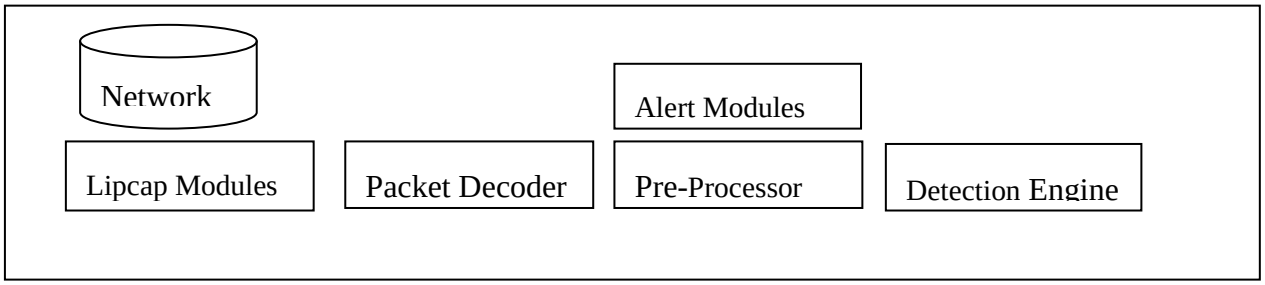
that are being used now. The latest version of snort tool came to being in 2003 snort 2.x.x.x has 75,000 line of code.

Snort Intrusion Detection System

According to Rani and Singh (2010) defined snort as a single threaded network security mechanism that can work based on four difference configuration mode, Packet sniffer mode, packet logger mode, detection mode and prevention mode or inline mode. Snort is an open source network intrusion detection system which is configured in a network PC as a network IDS. However, snort is incorporated in third party solutions, snort tool get wide acceptance by many industries all over the world with millions of a download. The detection of malicious traffic by snort is done by using transmission control protocol stack. A deep packet payload inspection is done by matching the observed packets and pre-defined snort signature. In a network, snort can be implemented in many different platforms such as Linux, FreeBSD, windows but snort has higher performance when deployed in a Linux platform because of its higher supportability, stability, security and reconfigurable network subsystem. Also snort performance is optimized by using Berkeley filter (BPF) using BPF only interested network packet are allowed to pass for analyzes by the snort components(Terrence *et. al*, 2010).

Snort Intrusion Detection Component

Snort intrusion detection system have many component according to many literatures each of these components has a vital roles to play in detecting malwares in the networks. Some of these Components includes packet decoders, lipcaps, preprocessor and the detecting engine. The descriptions of these components are given bellow:



Snort Decoder

The packet received by the snort tools needs to be further prepared for further processing by the snort components, at this phase the protocol elements is get to be decode by the specific decoder e.g. IP protocol, this make up series of packet decoders whose functions work up the network stack, decoding down from the first OSI model layer (data link frame) up to last layer services such as SMTP. The decoded packets are kept in the data structure ready to serve as an input to the remaining components(snort document, 2010). firstly, the decoder start with data link frame Ethernets, token ring and then proceed to decodes the Internet protocol and followed by the transmission transfer protocols and universal data protocol (Andrew,2004).However, according(Sallah *et.al*, 2011) The information generated by the snort decoder is used for further processing by snort detection engine and pre-processor (snort article 2009).

Snort pre-processor

Pre-processor is the next to the packet decoder components in the snort tools which perform numerous operations on the decoded network packets also enabled plug-in e.g. remote procedure call (RPC) are used in analyzing packet for a distinct malicious behavior some of the packet analyzes by the pre-processor includes hypertext transfer protocol (HTTP) and port scanning. In addition many pre-processor plug-in are utilized to extend the functionality of the snort tool.

Snort Detection Engine

Snort detection Engine is most important segment of the snort IDS. The detection engine act almost like a processor in a computer, indeed, the detection engine detects any intrusion that is associated with the packet data by matching it with the set of rules in the signature database. If a match is found, an appropriate action is taken against the detected intrusion such as alert that is send to the output plug-in or logged, otherwise the packet is dropped (Intrusion not detected) (Geddes and Linda 2009).

In addition, snort detection engine is a customizable components that allow many different pattern matching algorithm to be configures i.e Aho-corasick, Boyer Moore and many more pattern matching algorithm.

However, snort detection engine performance depends on its inner core pattern matching algorithm efficiency to match the pre-defined signature pattern with the incoming packet pattern. Therefore, this make snort detection engine as the most computationally intensive part as more CPU time is required to perform pattern matching against all the pre-defined thousands of rules(Terrence *et.al*,2010).

Snort Alerting

Alert and logging component are components through which result is generated by the snort detection engine when a match is found with a pre-defined signature, the alert is sent to the log files in a real time. However, alert generated by the snort are stored in a databases, log files, Syslog servers, SNMP traps, and Win Popup Messages.

Despite, contribution made to enhance snort performance none of these solutions are adopted by the snort manufacturer due to the un-changed snort deployment settings. Snort experience performance degradation when it is subjected to the high traffic network, these problems facing snort has attracted attentions of many researchers toward analyzing snort performance under different platforms and reviewing the general architecture of snort to meet the modern day network traffic requirement.

Performance of snort under high traffic network

Despite, contribution made to enhance snort performance few of these solutions are adopted by the snort manufacturer due to the un-changed snort deployment settings. Snort experience performance degradation when it is subjected to the high traffic network, these problems facing snort has attracted attentions of many researchers toward analyzing snort performance under different platforms and reviewing the general architecture of snort to meet the modern day network traffic requirement. one of these solution can be counter measured by using difference techniques, such as removing traditional network stack and socket interface mechanism snort article(2009). (Joshi,2011) had proposed systems that used entropy based anomaly detection and integrating it with real-time snort, the proposed system takes advantages of both anomaly and signature based detections. But the main drawbacks of this proposed is it producing higher no of false alarm

because it uses the current data to detect anomalies. Also ability to identify and ignore processing of identical malicious packets will limit the processing overhead and increased the performance of snort tool.

A proposed approach by (Roozbahani *et. al.*,2010) re-structures snort architecture to be able to detect the identical attacks and discard it before sending it to the detection engine. The design system consists of pre-processor put at the network entrance whose task is to convert the capture packet in to standard form. Secured mobile agent and few snort tools are configured in some selected network host. However, no doubt implementing this has reduced the processing overhead and increase the system performance of the network. . Another study is conducted under budget values different from the current default value (300) of Linux configuration networking subsystem, this demonstrated that the performance of snort can be increased in both malicious and normal packet processing by choosing the NAPI budget values smaller than the default value of 300.However, the changing of NAPI default parameter was because the snort's detection engine requires more CPU power to perform rule and string matching..

Snort Packet Inspection

Packet inspections are considered compulsory for any incoming packet in the network in order to ensure secure and congestion free network. This is done to identify whether the packets has matches with any signature defined in the system signature database. The signatures are represented based on attack type e.g. Vulnerability, virus, worm and denial of service attacks. However, there are many types of packet inspection carried out by network security system such as firewall and intrusion detection systems. In a state full packet inspection only three layers of protocol are examine source transport layer address which includes transmission control protocol and user datagram protocol (TCP or UDP), destination transport IP address also network layer protocol which includes internet protocol of the source system and the IP address of the destination system(Chaudary and Sardana,2011).

The service used to connect from the destination system is inspected, such as File transfer protocol and hypertext transfer protocol e.tc. In medium packet

inspection the communication between internal system and outside network is done via a proxy server application which provides packet filtering capabilities. But in deep packet inspection which is considered the best according Hassan, (2012) the whole packet payload is inspected by the security appliances. Indeed, more efficient techniques are needed in deep packet inspection while using pattern matching algorithms for finding malicious packets. However, according to (Zhang, 2010) this presents a lot of challenges as more time is required for the snort pattern matching algorithms e.i. boyer moore, Ac corasicks and Wu- Moore and their modified families to thoroughly inspect a network incoming packets, among the challenges includes consumption of almost half of snort processing time as rated by (Hassan and Abdulrashid,2012).

CONCLUSION

The paper highlighted different techniques adopted by snort intrusion detection system, their techniques of identifying intrusion to network Snort components and their working procedures. The paper also highlighted or presented some performance bottle neck and their proposed solutions.

REFFERENCE

Jyothsna, V., Prasad, V. V. R., & Prasad, K. M. (2011). A Review of Anomaly based. *Snorts. doi:10.1109/ICCEE.2009.270.*

Snort, D. (n.d.). Dissecting Snort. Network. Tekniska, K. (n.d.). Intrusion Detection *Systems*

Rajasekhar, K., Babu, B. S., Prasanna, P. L., Lavanya, D. R., & Krishna, T. V. (2011). An Overview of Intrusion Detection System Strategies and Issues. Network, 8491, *127–131.*

Salah, K. Ã., & Kahtani, A. (2010). Journal of Network and Computer Applications

Performance evaluation comparison of Snort NIDS under Linux and Windows Server. Journal of Network and Computer Applications, 33(1), 6-15.

Snort, D. (n.d.). Dissecting Snort. Network. Tekniska, K. (n.d.). Intrusion Detection *Systems.*

Hassan and Abdulrashid enhancing snort performance intrusion detection journal 2017.

Terrence a survey of intrusion detection techniques for cyber physical system,2010

Zhang, Tiezhu et al., "Study on the Application of Dynamic Balanced Scorecard in the Service Industry", 2008 International Conference on Intelligent Computation Technology and Automation, Digital Object Identifier: 10.1109/ICICTA.2008.359, pp. 1158-1162 (2008).

Andras, Peter, "The Equivalence of Support Vector Machine and Regularization Neural Networks," Neural Processing Letters, 65, pp. 97-104 (2002).

Reference to this paper should be made as follows: Abubakar Adulkadir Mukhtar *Abdulkadir* (2017), Review Paper on Snort Performance Bottle neck Solution and Packet Inspection. *J. of Education and Policy Review,* Vol. 9, No. 1, Pp. 56 - 65