International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

A Comparative Study of Intelligent IDS

Sameer*

Shah Satnam Ji P.G Boys' College, Sirsa, India

Accepted 16 June 2016, Available online 30 June 2016, **Vol.6, No.3 (June 2016)**

Abstract

Present era is the information age where information is money and its security is the primary concern. If the organization has faster access to accurate and up-to-date information then correct business decisions can be taken in time to achieve business excellence and uphold an edge over competitors. Various kinds of security mechanisms like cryptography, steganography and Intrusion Detection, etc. are extensively employed to keep the information secure and to send it over the network. Out of all the above mentioned available options, Intrusion Detection Systems (IDS)is the most robust one. It is also a secure product that protects the network and system in real time from attacking, and now becomes a hotspot of research in network security domain An IDS is either a hardware or software that monitors real time network traffic in order to detect unsolicited activity and events such as illicit and malevolent traffic, traffic that violates refuge policy, and traffic that violates conventional use policies. One such primary IDS tool is Snort which is also an open source software. It is widely used in the intrusion anticipation and uncovering domain in the world. This paper proposes the idea of using Snort as intrusion and detection system for small scale clients.

Keywords*: IDS, firewall, domain ,intrusion, hotspot, prevention, Detection*

1. Introduction

With the rapid development of internet, network security becomes a more and more serious problem. To prevent network attacks intrusion detection system (IDS) has been widely deployed. According to detection strategy, there are two types of intrusion detection, misuse-based detection and anomaly-based detection. Misuse-based detection is named knowledge-based detection too. Knowledge-based detection is equipped with a database that contains a number of signatures about known attacks. The audit data collected by the IDS is compared with the content of the database and, if a match is found, an alert is generated. Events that do not match any of the attack models are considered as a part of legitimate activities. The main advantage of misuse-based systems is that they usually produce very few false positives. But this approach has drawbacks. It cannot detect previously unknown attacks, and sometimes it even cannot detect the variations of known attacks. Anomaly-based detection is a behavior-based detection method. It is based on the assumption that all anomalous activities are malicious and all the attacks are subset of anomaly activities. By building a model of the normal behavior of the system, then it looks for anomalous activities that do not conform to the established model. Since it can detect unknown attacks, it is the research hotspot at present. However, since it is impossible to describe all the activities of all users in system, it leads to relative high false positive rate. Most of current IDSs use one of the two detection methods. To improve the performance of IDS, how to combine misuse-based detection with anomaly detection becomes the current research hotspot of IDS.

2. Methods for IDS

a) Snort

It fills an important ‘‘ecological niche’’ in the realm of network security: a cross-platform, lightweight network intrusion detection tool that can be deployed to monitor small TCP/IP networks and detect a wide variety of suspicious network traffic as well as outright attacks. It can provide administrators with enough data to make informed decisions on the proper course of action in the face of suspicious activity. Snort can also be deployed rapidly to fill potential holes in a network’s security coverage, such as when a new attack emerges and commercial security vendors are slow to release new attack recognition signatures, rules-based traffic collection engine, as well as new and different applications where it can be very useful as a part of an integrated network security infrastructure.

Snort is a tool for small, lightly utilized networks. It can be analyzed in many modes via Sniffer mode, which simply reads the packets off of the network and

*Corresponding author: Sameer

displays them for you in a continuous stream on the console (screen).Packet Logger mode, which logs the packets to disk. Network Intrusion Detection System (NIDS) mode, the most complex and configurable configuration, which allows Snort to analyze network traffic for matches against a user-defined rule set and performs several actions based upon what it sees. Inline mode, which obtains packets from iptables instead of from libp cap and then causes iptables to drop or pass packets based on Snort rules that use inline- specific rule types.

Components of Snort: It is logically divided into multiple components. Following components are work together to detect particular attacks and to generate output in a required format from the detection system.

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 inter- faces may be Ethernet, SLIP, PPP and so on.

2. Preprocessors: These 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. Hackers use different techniques to fool an IDS in different ways. For example, you may have created a rule to find a signature "scripts/iisadmin" in HTTP packets. If you are matching this string exactly, you can easily be fooled by a hacker who makes slight modifications to this string. For example:• "scripts/./iisadmin"• "scripts/examples/../iisadmin",• "scripts\iisadmin",• "scripts/.\iisadmin".

3.Detection Engine: It 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. 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.

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, tcp dump-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.

5. Output Modules: These modules or plug-ins can do different operations depending on how user 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 system. Depending on the configuration, output modules can do things like the following:

•Simply logging to /var /log/snort/alerts file or some other file.
•Sending SNMP traps.
•Sending messages to syslog facility.
•Logging to a database like My SQL or Oracle.

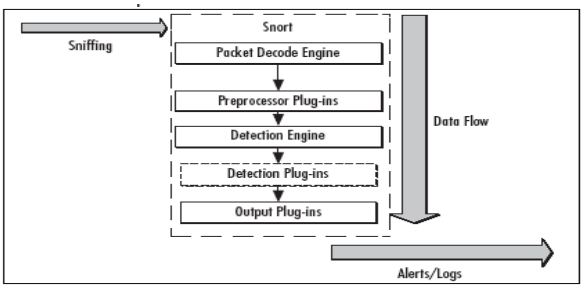

Figure 1 Components of Snort

b) Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet,. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.Net filter / iptables is an IP packet filtering system integrated by the kernel (2.4) of Linux, it consists of two components Net filter and iptables. Net filter component called the kernel space, it provides an operational framework for IP packets. Iptables component called the user space, It is the tools for user to insert, delete and modify the filtering rules, which stored in the Net filter component.

c) Support vector machine

SVM is a learning method based on the statistical learning theory, the key point of its is to improve the generation ability of the learning machine according to the Vapnik structural risk minimization principle, namely obtain small errors according to the limited training sets sample, and ensure the independent test sets keeping small errors. Moreover, the SVM algorithm is a convex optimization problem. Thus the local optimal solution must be the global optimal solution which other algorithms cannot achieve. It can also used in the limited sample data and not be sensitive to data dimensions. Therefore, SVM is adapted to the intrusion detection field high dimension heterogeneous imbalance data set character, and it can be applied to intrusion detection.

3. Implementation of snort

Before, the setup of Snort is very complex process, which involves detecting the integrity of compiling environment and the setup of Apache, Mysql, PHP, ADODB and ACID components. Now, the Snort official website has provided some simple installation guides for Windows xp, Solaris10 (SPARC) and Linux. We can quickly and easily build our intrusion detection system according to the guide of installation documents. Taking into account the stability and security of operating system, we refer the Snort_Base_Minimal.pdf to build Snort, Apache, SSL, PHP, My SQL, BASE and NTOP on Linux. The following is the installation steps:
1) Setup the operating system with minimal model.
2) Make the unnecessary services disable.
3) Setup the compiling environment using "yum" command and install the Apache, Mysql and PHP component.
4) Download and install the Snort source code and rule.
5) Modify the profile o/Snort.
6) Build the Snort database with My sql.
7) Install the ADODB and BASE.
8) Start all the required service.
S
nort monitors the network in the bypass mode. It catches the suspected data which attaches the Intranet. The monitoring result is shown on the Basic Analysis and Security Engine (BASE), which can intuitively analyze the catched data and display it. So the network security was improved by the reference data of Snort. Figure 2 is the home of BASE. The BASE mainly shows the statistical result by time, IP address and port. We can find SSH login test, SQL detecting overflow, ICMP redirect host and other malicious acts as soon as the Snort is setup .Figure 2 is the detail information of warning for a target
IP.

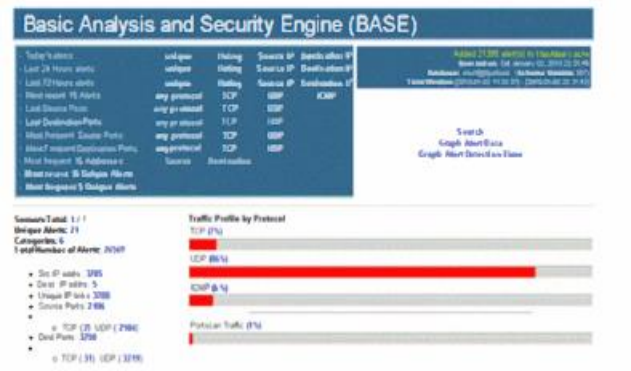

Figure 2 Home of base

4. Analyzing Source code of Snort

a) The working process of Snort

The Snort Main implements the initialization and monitoring of Snort. Figure 3 is the working process.

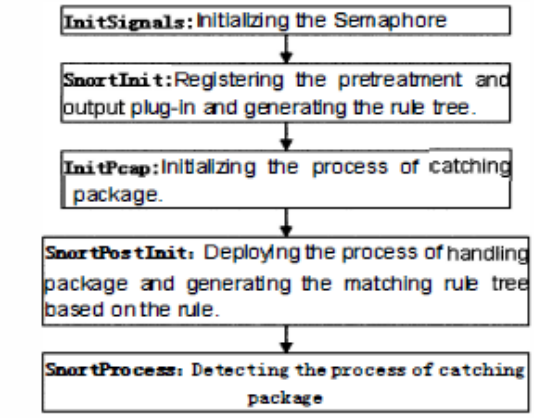

Figure 3 Working process o Snoot

b) The rule tree of Snort

The rule tree is the important data structure in Snort. It is helpful to grasp the rule matching of Snort. Figure 4 shows the structure of rule tree.

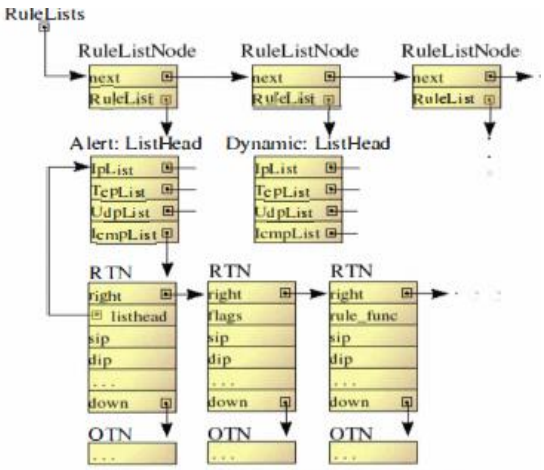

Figure 4 Structure of rule tree

Conclusion

This paper designed the intrusion prevention module of network intrusion prevention system which bases on intrusion detection system Snort. Intrusion prevention system provides real time and active prevention ability, prevents the attack effectively and assures the normal data stream. Because of the character of intrusion prevention system, it could only be connected in the network is series. This kind of connection position could lead to potential problems. Utilizing SVM in Snort intrusion detection system, reduces the rate of miss and error report, and needs little rules. Which makes Snort combines with firewall can improve the defensive ability of the system, and makes the IPS very intelligent.

References

Xiangning ;Zhiping JIANG ;Xinli TIAN ,The detection and prevention for ARP Spoofing based on Snort" proceeding

2010 International Conference on Computer Application and System Modeling (ICCASM 2010) ,v5-137

Sergei Egorov, Gene Savchuk ," SNORTRAN: An Optimizing Compiler for Snort Rules.

Zhou Zhimin; Chen Zhongwen ; Zhou Ti echeng; Guan Xiaohui ,"The Study on Network Intrusion Detection System of Snort" ,proceeding 2010 International Conference on Networking and Digital Society .194.

David Gullett; Symmetric Technologies ,014-snortinstallguide292.pdf

Kang Hong ;Zhang Jiangang ,"An Improved Snort Intrusion Detection System Based on Self-similar Traffic Model "by Kang Hong and Zhang Jiangang.(College of Economics and Management Shandong University of Science and Technology Qingdao, China ,978

Jiqiang Zhai; Yining Xie ,"Researh on Network Intrusion Prevention System Based on Snort "proceeding 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE) ,251.

Dihua Liu; Hui Li " Research on Intelligent Intrusion Prevention System Based on Snort " 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE),478.

Shiv Kumar; R.C.Joshi ,"Design and Implementation of IDS Using Snort, Entropy and Alert Ranking System" Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011) .264.

Xingkui Liu Xinchun Liu Ninghui Sun ," ,Fast and Compact Regular Expression Matching Using Character Substitution" proceeding 2011 Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems .85

Safaa O. Al-Mamory;Ali Hamid; Asala Abdul-Razak,;Zainab Falah."String Matching Enhancement for Snort IDS.1020.

Yaron Weinsberg ;Shimrit Tzur-David ;Danny Dolev,"One Algorithm to Match Them All:On a Generic NIPS Pattern Matching Algorithm", proceeding High Performance Switching and Routing Conference (HPSR'07).