International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2| ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195215

Efficient Working of Signature Based Intrusion Detection Technique in Computer Networks

Dr. Abid Hussain[1], Dr. Praveen Kumar Sharma[2]
[1]Assistant Professor, School of Computer Applications, Career Point University, Kota, Rajasthan, India
[2]Vardhman Mahaveer Open University, Kota, Rajasthan, India

ABSTRACT

The subject of Computer Network Intrusion Detection System (IDS) is a very interesting research topic actively pursued by many investigators. The goal of intrusion detection is to monitor network assets and to detect anomalous behaviour and misuse. This concept has been around for the past several years but only recently, it has seen a dramatic rise in interest of researchers and system developers for incorporation into the overall information security infrastructure. In today's world, the concept of information has been moved to the digital size from conventional size. Protection of the data stored in the digital archive and is easily accessibility at any time have become a quite important phenomenon. In this concept, intrusion detection and prevention systems as security tools are widely used today [1]. In this paper, a signature based intrusion detection system approach has been proposed for computer network security. This paper is based on the efficient working of the Signature based intrusion detection method and protects the computer network against the intrusion or the unspecified packets.

Keywords: IDS, Signature, Security, IPS, Information Security, Attacks, Threats, Snort, Packet Decoder, Detection Engine.

I. INTRODUCTION

As we know that we all are dependent on the Computer Network for performing any kind of network operations. Network security is the big challenge among the researchers. There are so many network security tools available such as antivirus, firewall, etc.but they are not able to cover all security risks in the network. The main work of intrusion detection system is to identify the intrusion in the network [2] and for that it collects important information from the network, process it and if identify attack then alert for the possible attack.

The purpose of network security is to protect the network from unauthorized access and disclosure. The recent advancements in the field of network security helps in the protection of computer systems and computer networks. One of the techniques used for making the network secure and detecting intrusions is Intrusion Detection System. Intrusion Detection System is a mechanism that detects unauthorized and malicious activity present in the computer systems [3].

II. SIGNATURE BASED IDS

In Signature based IDS, every signature requires an entry in the database. Each packet is to be compared with all the entries in the database. Signature based IDS matches the signatures of already known attacks

that are stored into the database to detect the attacks in the computer system. Signature based IDS suffer from the huge number of signatures stored in its database [4]. Some researchers provided the concept of frequent signature database to solve database size problem but never discussed how to deal with new signatures and the old signature that became unnecessary. In a signature based detection a predetermined attack patterns in the form of signatures and these signatures are further used to determine the network attacks [5].They usually examine the network traffic with predefined signatures and each time database is updated. An example of Signature based Intrusion Detection System is SNORT.

A. Advantages

- There are low false positives as long as attacks are clearly defined in advance.
- Signature-Based Detection is easy to use
- High true positive rate for known attacks
- Lightweight
- Low false positive rate
- Simple to implement

B. Disadvantages

- It can be seen that misuse detection requires specific knowledge of intrusive behavior. Collected data before the intrusion could be out of date and yet many times it is hard to detect newer or unknown attacks.
- Misuse detection has a well-known problem of raising alerts regardless of the outcome. For example, a window worm trying to attack a Linux system, the misuse IDS will send so many alerts for unsuccessful attacks which may be hard to manage.
- This model may not always be so practical for inside attacks involving abuse of privileges.
- The knowledge about attacks is very dependent on the operating system, version and application hence tied to specific environments.

III. WORKING OF SIGNATURE IDS

This mechanism protects against known threats. A signature is a known pattern of a threat, such as:

- An e-mail with an attachment containing a known malware with an interesting subject (for example, an e-mail with the subject “I love you”).
- A “remote login” by an admin user, which is a clear violation of an organization's policy.

Signature-based detection is the simplest form of detection because it just compares the traffic with the signature database. If a match is found then the alert is generated, if a match is not found then the traffic flows without any problem.

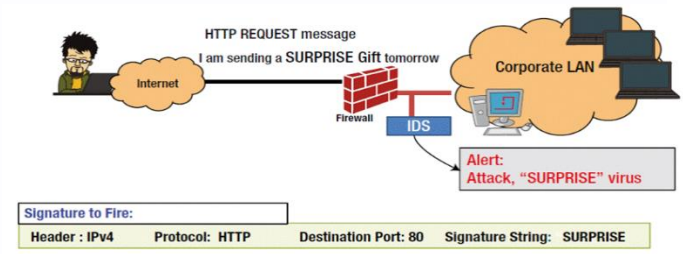

Figure 3.1. Working of Signature Based IDS

In signature-based detection, detection is based on comparing the traffic with the known signatures for possible attacks (see Figure 3.1). They can only detect known threats and hence, are not efficient in detecting unknown threats [7]. To detect an attack, the signature matching has to be precise, otherwise, even if the attack has a small variation from the known threat signature, then the system will not be able to detect. For example, in the above example, instead of “I love you” if the subject is “love you”, the system may not detect the threat. Hence, it is very easy for the attackers to compromise and breach into the trusted network.2

Signature database needs to be updated constantly, almost on a daily basis from the anti-virus labs such as McAfee, Symantec, Trend Micro, and other security providers. If the signature is not up to date, chances are that the IDS systems will fail to detect some of the intrusion attacks. The other disadvantage is that they have very little information about previous requests when processing the current ones.

Signature-based detection can offer very specific detection of known threats by comparing network traffic with the threat signature database. The detection can be enhanced if the network traffic inside the network can be made to learn specific patterns, thus reducing false positives [8]. Signature detection engines tend to degrade in performance over a period as more and more signatures are added to the database. It takes more and more time for the engine to do a pattern search as the signature database is always growing as more and more definitions are added to it. Hence, a robust platform is needed for signature detection considering this growth.

IV. COMPONENTS OF SIGNATURE BASED IDS

This system works on the principle of matching. The data is analyzed and compared with the signature of known attacks. In case of any matching, an alert is issued. An advantage of this system is it has more accuracy and standard alarms understood by user.

A signature-based IDS analyzes packets from a computer network and matches them against a set of signatures that trigger on known intruder techniques. In a typical setup, an IDS analyzes all packets flowing through some point in the network. The signature-based IDS detect whether the packets match any of its signatures and delivers matching packets to on analysis backend [8]. The performance of the detection process is an important metric in the evaluation of a signature-based IDS.

.

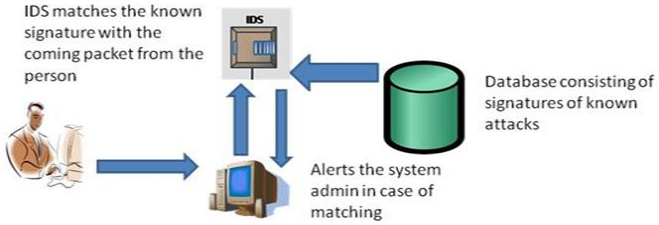

Figure 3.2. Components of Signature based IDS

V. TOOLS OF SIGNATURE BASED IDS

To use Signature based Intrusion Detection System in the Computer Network; we need to install some network security tools in the current network like SNORT.

1. SNORT

Snort is an open-source security software product that looks at network traffic in real time and logs packets to perform detailed analysis used to facilitate security and authentication efforts. Snort is built to detect various types of hacking and uses a flexible rules language to determine the types of network traffic that should be collected. Snort rules can be written in any language, its structure is also good, it can be easily read, and rules can be modify also [9]. In buffer overflow attack, snort can detect the attack by matching the previous pattern of attacks and then will take appropriate action to prevent from attack. In signature based IDS system if pattern matches then attack can be easily found but when a new attack comes then system fails but snort overcome this limitation by analysing the real-time traffic. Whenever any packet comes into network then snort checks, the behaviour of network if performance degrades of network then snort stop the processing of packet, discards the packet and stores its detail in the signature database.

2. 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 fromthe detection system [10]. A Snort-based IDS consists of the following major components:

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules

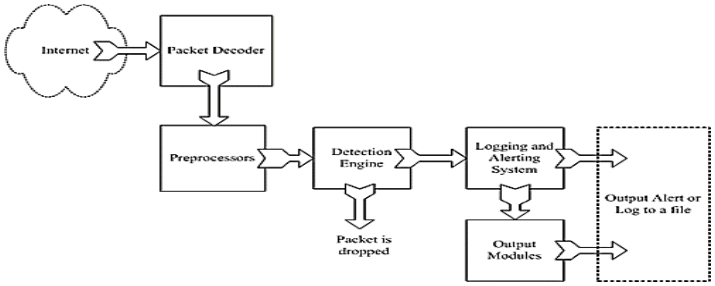

Figure: 5.1. Components of the Signature IDS Snort

- **Packet decoder**

The packet decoder collects packet from different-2 network interfaces and then send to be pre-processor or sent to the detection engine.

- **Preprocessors**

It works with snort to modify or arrange the packet before detection engine to apply some operation on packet if packet is corrupted. Sometimes they also generate alert if any anomalies found in the packet. Basically it matches the pattern of whole string so, by changing the sequence or by adding some extra value intruder can fool the IDS but preprocessor.

- **The Detection Engine**

Its main work is to find out intrusion activity exits in packet with the help of snort rules and if found then apply appropriate rule otherwise it drops the packet. It takes different time to respond different packet and also depends upon the power of machine and number of rules defines in the system.

- **Logging and Alerting System**

Whatever detection engine finds in the packet, it might generate an alert or used to log activity. All log files are kept by default under /var/log/snort folder and by using –l command line option, location can be changed.

- **Output Modules**

Output modules or plug-ins save output generated by the logging and alerting system of Snort depending on how user wants for different operation. Mainly it controls the different output due to logging and alerting system.

VI. CONCLUSION

This paper proposes the working process of Signature based Intrusion Detection System in the Network. This SIDS System demonstrated that it can detect and analyse the intrusion in real time network traffic. We have also discussed about the Network IDS tools like Snort. Snort is built to detect various types of hacking and uses a flexible rules language to determine the types of network traffic that should be collected. The future work is to develop a novel framework to filter, delete and validate the intrusion attack automatically in the computer network.

VII.REFERENCES

[1] D. E. Denning. “An Intrusion-Detection Model”. IEEE transactions on software engineering, Volume : 13 Issue: 2, February 1987.

[2] J.P. Anderson, “Computer security technology planning study”. Technical Report, ESDTR-73-51, United States Air Force, Electronic Systems Division, October 1972..

[3] Axelsson, S (2000). "Intrusion Detection Systems: A Survey and Taxonomy" (retrieved 21 May 2018)

[4] Brandon Lokesak (December 4, 2008). "A Comparison Between Signature Based and Anomaly Based Intrusion Detection Systems"(PPT). *www.iup.edu*.

[5] DP Gaikwad, P Pabshettiwar, P Musale, P Paranjape, AS. Pawar, "A proposal for implementation of signature based intrusion detection system using multithreading technique", *International Journal of Computational Engineering Research (ijceronline.com)*., vol. 2, no. 7, 2012

[6] https://www.elprocus.com/basic-intrusion-detection-system/ "Advantage and Disvantages of Signature based Intrusion Detection System"

[7] Philip Chan,"Signature based Intrusion Detection System", CS 598 MCC Spring 2013

[8] Hwang,K., Cai,M., Chen,Y and Qin,M. , "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes", IEEE Transactions on Dependable Computing, Volume: 4 Issue: 1, pp. 41- 55, 2007.

[9] Martin Roesch (2009), "Snort User Manual 2.8.5",available:http://www.snort.org/assets/125/snort_manual2_8_5_1.pdf.

[10] Yang Li, Research and Implementation of intrusion detection system based on Snort[J], Beijing:The Technology and Application of Network Security, 11 2009.

Cite this article as :

Dr. Abid Hussain, Dr. Praveen Kumar Sharma, "Efficient Working of Signature Based Intrusion Detection Technique in Computer Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5, Issue 2, pp.60-64, March-April-2019.
Available at doi :
https://doi.org/10.32628/CSEIT195215
Journal URL : http://ijsrcseit.com/CSEIT195215