ISSN 2395-1621

Firewalls and Intrusion Detection and Prevention Systems

[#1]Anusha Vaidya, [#2]Prof. Shailesh P. Bendale

[1]vaidyaanu96@gmail.com,
[2]shailesh.bendale@sinhgad.edu

[#1]Department of Computer Engineering,
[#2]Prof. Department of Computer Engineering

NBN Sinhgad School of Engineering, Pune.

ABSTRACT

A constant need for safeguarding our network from vulnerable attacks has aroused due to expansion of web applications. Attacks can affect the network functionality, its life time, and security. This paper presents various attack details and also the various ways to detect the threats at various levels. Different intrusion detection and prevention systems are studied and compared based on their features. Firewalls, which limits the access to prevent intrusion is studied and compared with IDS. The paper presents various IDPS techniques and layering based Security approach. At the end, based on the literature review, conclusion and the advantages and disadvantages are specified.

Key words: Intrusion Detection Systems, Network Security, Firewalls.

ARTICLE INFO

Article History

Received: 22nd March 2017

Received in revised form :

22nd March 2017

Accepted: 24th March 2017

Published online :

6th April 2017

I. INTRODUCTION

Recently, there has been a rapid increase in the use of internet and web applications throughout the globe. The dependency on internet and its amenities is continuously growing. With all its positive uses, the threat of being attacked has also increased. The need for online services has increased the cyber crime rate. A new attacking technique is observed frequently. These attacks and threats should be handled in an effective way.

A mechanism like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) or Firewalls for monitoring and controlling these activities must be implemented. As the use of network is vast, there will never be enough security for network. But the implemented security should be reliable and must not affect the accuracy and performance of the system.

Intrusion Detection Systems (IDS) is a device or software application which monitors the network traffic for malicious activities. Whereas the Intrusion Prevention Systems (IPS), along with monitoring, it identifies the threat and the log information and attempts to block the activity and report it. The firewalls are systems which controls network traffic based on security rules.

IDS and IPS acts as a defensive security technique such as authentication and control. IDPS has become a necessity due to its importance of maintaining confidentiality, availability, integrity, etc. The purpose of paper is to give brief overview and study the developments in IDPS technology.

II. OVERVIEW OF SECURITY

A. Intrusion Detection Systems (IDS):

An Intrusion Detection System (IDS) is used for the detection of intrusions in the network using various methods and tools [1]. The IDS monitors the network traffic for any suspicious activities or vulnerabilities. In IDS, the network is monitored via promiscuous interface. Any kind of unauthorized activity is detected. The IDS should be reliable and should not introduce any weakness in the system. It should require fewer resources and should increase the overall performance of system.

B. Intrusion Prevention Systems (IPS):

Along with detecting the threats, IPS is able to prevent the threat immediately. The IPS attempts to block the threat and report it. Incriminated packets are discarded. IPS decides whether to drop the packet or allow it in the network. A little delay is introduced as every packet is examined with IPS [3]. Sometimes, IPS may also discard secure traffic due to mistaken rules.

C. Firewalls

A firewall examines every single packet according to a set of rules and it decides if the packet is allowed to enter or is discarded [3]. Access Control Lists (ACL) operates on a network. If TCP is not initiated from firewalls, it declares the connection as unwanted and discards it. The difference between IDS and firewalls is that firewall only examines the header part while IDS/IPS examines the payload.

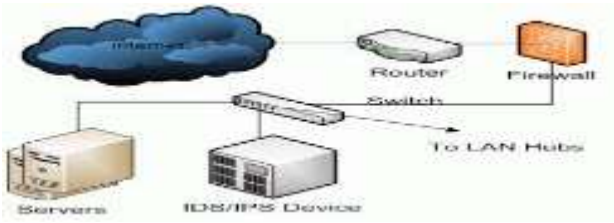

Fig 1. IDS, IPS and firewall systems.

Table I. Difference between IDS and Firewalls

Sr No.	Intrusion Detection Systems (IDS)	Firewalls
1.	An Intrusion Detection System (IDS) can be used for the detection of attacks in the network using various methods and tools [1].	A firewall examines every single packet according to a set of rules and it decides if the packet is allowed to enter in or is discarded [3].
2.	IDS examine suspected intrusions and then signal an alert.	Firewalls look separately for attacks to avoid them.
3.	IDS look for attacks before it originates.	Firewall limits use of the network.
4.	IDS examine the payload (application layer) along with the header section.	Firewalls examine only the header section of the packet.

III. Intrusion Detection and Prevention Techniques.

The intrusion detection and prevention systems (IDPS) use a deep packet inspection to examine multiple layers for vulnerabilities and protocol based firewalls. Database of malware signatures provides effective safety against intrusion. Basic steps to avoid intrusions are:

1. Block malicious attacks.
2. Provide network bandwidth.
3. Granular control.

A. Network Based IDPS(NIDPS):

Network based IDPS monitors network traffic to identify harmful attacks. In NIDPS, it involves hardware components placed at different locations or the software is installed at various systems in the network. It intercepts all network traffic passing to find for attacks, which either passes it on or blocks the request.

Another aspect of NIDPS is that the system can suspect suspicious events and rewrite it so that the hack attempt fails. But in some instances, it may block useful and legitimate packets.

B. Host Based IDPS (HIDPS):

Host based IDPS monitors a single host for suspicious activities. HIDPS also monitors activity logs, running processes, file access and modification, configuration changes, etc. HIDPS is commonly deployed on critical hosts and systems containing sensitive information. HIDPS analyzes the internals of the computer. Whenever it suspects any suspicious activity, only then it notifies the user or administrator.

C. Wireless IDPS:

Wireless IDPS monitors wireless traffic for suspicious activity along with its networking protocols. This does not monitor high layer network protocols such as TCP/UDP, etc. Wireless IDPS works within the product range of wireless technology.

D. Network Behavior Analysis (NBA):

Network Behavior Analysis finds the unusual traffic flow such as the Denial of Service (DOS) attack, etc. This also detects any kind of malware or policy violations. NBA systems mainly deployed in internal networks. The changes of deployment in inner networks and external sites if quite less.

IV. Layer-based security Approach

Layer	Attacks	Approach
Application Layer	Malicious nodes.	Manages Data collection, Ensure data reliability. Detection.
Transport Layer	Flooding. De-synchronisation.	Establish communication for external networks. Authentication.
Network Layer	Wormholes. Sinkholes. Sybil.	Routing of messages. Secure Routing. Verification. Key management authentication.
Data Link Layer	Collision. Jamming.	Multiplexing of data stream, error detection and correction. Encryption. Correction Code.

Physical Layer	DoS. Jamming.	Signal detection, frequency selection, etc. Region mapping. Mode change.

V. LITERATURE SURVEY

There are different methods to detect intrusions and to prevent them. The three basic methods are:-

1) Signature based Detection.
2) Anomaly based Detection.
3) Stateful Protocol analysis.

1) Signature Based Detection:

Signature based Detection is also known as Rule based detection. A couple of key facts are predefined considering security. Sensor network behavior is analyzed based on these predefined rules. Signature based IDS matches the signature with the previously stored signature in the database. Due to matching of signatures, suspicious activities can be detected.

It is generally used as each attack has distinct signatures and can be easily identified. Signature based IDS includes use of ICMP (Internet Control Message Protocol), DNS querying and email routing analysis. Foot printing or finger printing activities are examples of Signature based IDS.

The drawback of Signature based IDS is that its database needs to be continuously updated. If not updated, it may allow attacks with new strategies. Sometimes, attackers purposefully attack slowly to slip undetected by their signatures. To overcome this vulnerability, Signature based IDS must analyze data for longer periods of time. A popular signature based technique used is:-

SNORT: Snort is a lightweight open source NIDS. Snort is packet sniffer which monitors real network traffic and examines packets closely for attacks. When attack is detected, it sends alert to the system logs.

2) Anomaly Based Detection:

An anomaly based detection system monitors the network for intrusions. It uses heuristic approach that classifies it either normal or anomalous. It works as per certain rules rather than signatures. It detects all activities which will fall outside normal operations. Anomaly based detection relies on the behavior development during the training period. Intrusions are detected using a threshold value. When a value is above the threshold, it is considered as an intrusion. Anomaly based detection has the ability to detect unknown or previous attacks. This is considered as a main advantage. A popular anomaly based technique used is:-

PHAD (Packet Header Anomaly Detection): PHAD is based on assumptions of events. If probability of occurrence of event is p, then result received is 1/p. If the assumptions are true, user can modify the threshold.

3) Stateful Protocol Approach:

Stateful Protocol approach is a resource intensive approach to intrusion detection. It is also called as deep packet inspection. Stateful Protocol Analysis "relies on vendor-developed universal profiles that specify how particular **protocols** should and should not be used" [1]. Unexpected sequence of commands can be recognized. It has the capability of understanding and responding to attacks. Protocol performs authentication and the IDPS can keep track of the authenticator.

VI. COMPARISON BASED ON SURVEY

PHAD and Snort are evaluated on 1999 DARPA off-line IDS evaluation data set. They consist of tcpdump files. The week 3, 4 and 5 results are used as inputs. Week 3 is attack free. Week 4 and 5 data consist of attacks and are used in testing. Comparison between PHAD and Snort can be done using three parameters:-

1. Number of attacks detected protocol wise.
2. Number of attacks detected data wise.
3. Detection rate.

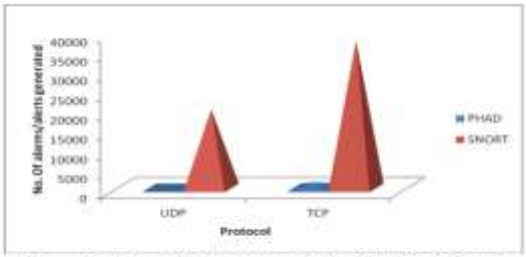

Figure 2: Alarms/alerts generated by PHAD and Snort protocol wise

Fig.2 shows alerts generated on basis of protocol.

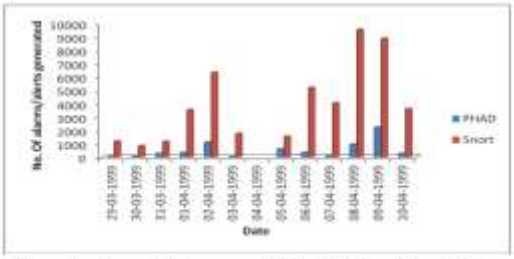

Figure 1: Alarms/alerts generated by PHAD and Snort date wise

Fig. 3 shows alerts generated on basis of date.

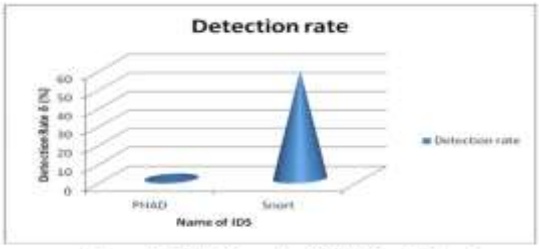

Figure 3: Detection rate of PHAD and Snort

Fig.4 shows alerts generated on basis of detection rate.

The detection rate of Snort is much higher than that of PHAD. The alerts generated based on date of Snort is higher than PHAD.

The detection of signature based is much higher than anomaly based detection methods.

DETECTION RATES:

The performance of an Intrusion Detection System can be detected based on the number of attacks. The detection rate if IDS 'δ' is defined as:-

$\Delta=d/n$

Where,

d = number of attacks detected

n = total number of attacks.

The overall number of attacks is 201.

The average amount of attacks detected by PHAD is calculated as 5. Hence,

$\Delta=5/201*100=2.4\%$.

Hence, the detection rate of PHAD is 2.4%.

While total amount of attacks in Snort is 116. Hence,

$\Delta=116/201*100=57.7\%$.

Hence, the detection rate of Snort is 57.7%.

VII. CHALLENGES IN IDS

The IDS offers great value in guarding system from attacks. The effectiveness of IDS is evaluated based on potential to classify events as normal or intrusive. It faces challenges from developing to deployment to performance.

A) Issues:

The main issue is to appropriately classify the packet as a normal packet or an intrusive packet. Sometimes, packets might also be classified wrongly which is termed as misclassification. An additional issue is the failure to handle data in high speed networks. The traditional IDS are unable to appropriately classify packets attacks with equal level of accuracy. IDS have the lack of ability to be resilient to stress and failures.

B) Motivation:

Hybrid intelligent approach for developing IDS is considered as an improved approach. It combines the strong points of the classifiers and avoids their weaknesses. Hence, improving the IDS performance is the key aim.

C) Human intervention is essential.

Network based IDPS can be used between the firewalls and Host based IDPS can be used on all critical hosts.

D) It is necessary to define the expectations properly as it undergoes lots of improvements. Some of the other issues include integration of multiple forms, testing/evaluation of IDPS, diagnosis algorithms, etc.

VIII. CONCLUSION AND FUTURE WORK

An IDS offers a basic mechanism to determine violation in strategies. IDS are an essential part which complements firewalls in defending our network. In terms of performance, IDPS is accurate. IDS and firewalls are being used together for preventing attacks and intrusions. The literature review shows that firewalls work effectively and are feasible in defence. Firewall acts as first type of protection against network attacks. Intrusion detection system (IDS) reduces security spaces and strengthens security of a network by examining the network assets for anomalous behavior and wrong use. Real time detection with prevention by Intrusion Detection and Prevention Systems (IDPS) takes the network security to an advanced level by protecting the network against mischievous activities. The future work consists of the use of all the three techniques i.e. Intrusion detection, Intrusion prevention and firewalls for the prevention of attacks and misuse of the network.

REFERENCES

[1] Sonu Duhan and Padmavati Khandnor, "Intrusion Detection System in Wireless Sensor Networks: A Comprehensive Review", 2016

[2] Xiaobo Huang and Xiaoyan Wang and Shisong Zhu, "Study on Intelligent Firewall System Combining Intrusion Detection and Egress Access Control", China 2010

[3] Filip Hock and Peter Kortiš, "Commercial and open-source based Intrusion Detection System and Intrusion Prevention System(IDS/IPS) design for an IP networks, Zilini, Slovakia 2015.

[4] Ryan Proudfoot, Kenneth Kent, Eric Aubanel and Nan Chen, "High Performance Software-Hardware Network Intrusion Detection System", Canada2007.

[5] V. Vaidehil, N. Srinivasan', P. Anand', A.P. Balajil, V. Prashanthl and S. Sangeethal, "A Semantics Based Application Level Intrusion Detection System", India 2007, pp.338-343

[6] Farid Lawan Bello, Kiran Ravulakollu, Amrita, "Analysis and evaluation of Hybrid Intrusion Detection System Models", India 2015

