International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015) pp 38228-38240
© Research India Publications. http://www.ripublication.com

A Technical Review on Intrusion Detection and Prevention Systems (IDPS) Methodologies

S.Bharath Reddy
Research Scholar,
Department of Computer Science and Engineering,
SRM University, Kattankulathur,
Kancheepuram District
Bharath.bittu945@gmail.com

D.Malathi,
Professor,
Department of Computer Science and Engineering
SRM University, Kattankulathur,
Kancheepuram District
mala_kam@yahoo.com

Abstract— over a past few decade's security is a challenging issue in networks. By introducing Intrusion Detection and Prevention Systems (IDPS) we can provide security on data and we can prevent hackers from accessing data. Intrusion Detection and Prevention Systems, are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about the activity, attempt to block/stop it, and report it. Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. In this paper we analyze some of the recent methodologies used in IDPS to prevent unauthorized access to data, such as anomaly based signature based, stateful protocol analysis, and a hybrid system that detects and respond to security threats. It gives a clear explanation of each methodology and all these methodologies are analyzed and compared using various parameters.

Keywords: Anomaly Based Detection, Hybrid Based Detection, Intrusion Detection and Prevention Systems (IDPS), Signature Based Detection, Stateful Protocol Analysis Based Detection.

Introduction

Intrusions tries to attack the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer system or network (illegal access).Intrusions have many causes, such as malware (worms, spyware, etc…), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized.

Even though several intrusions are detrimental in nature, many others are not; for example: a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization intrusion detection is the method of checking the events occurring in a computer system or network and analyzing them for signs of possible intrusions (incidents).

Intrusion Detection System (IDS) is a software that automates the intrusion detection process. The main responsibility of an IDS is to detect unwanted and malicious activities. Intrusion Prevention System (IPS) is a software that has all the capabilities of an intrusion detection system and can also attempt to stop possible attacks.

This paper bridges the gap by offering an explanation on four major underlying IDPS methodologies and a way to compare them. The four main detection methodologies used by IDPS are signature based, anomaly based, stateful protocol analysis based, and hybrid based. The remaining part of this paper is organized as follows: Section II gives an overview of related works. Section III offers a detailed description of the four main methodologies, while Section IV compares and evaluates IDPS methodologies. Section V concludes the paper and suggests future work.

Related Work

Intrusion detection and prevention systems are a combination of intrusion detection systems and intrusion prevention systems. Intrusion prevention came out from short comings of intrusion detection. Intrusion detection came from report that proposed a threat model [1]. This is the basic intrusion detection systems by presenting a model for identifying abnormal behavior in computer systems. This model categories threats into three groups namely internal and external penetrations, and misfeasance. In 1987 a model for a real-time intrusion-detection expert system was produced [2]. By using audit logs they identify the security breaches to any systems. It consists of metrics, profiles, statistical models, and rules for analyzing the logs.

The authors have proposed a framework for a general-purpose intrusion-detection system and expert system [3]. They combine two methodologies used in intrusion detection and prevention systems to form a Collaborative Intelligent Intrusion Detection System (CIIDS) [4]. This work looked at current challenges to collaborative intrusion detection system and the algorithms they employ for alert correlation. They analyses how to reduce false positives and how to increase the detection accuracy rate.

In [5] a structured approach to IDS by defining and classifying the components of an IDS system is offered. This classification offered a clear understanding of all the parts that make up intrusion detection systems and the challenges the systems faces.

By observing the intrusion detection system that how these systems are structured to the techniques they use to detect and identify potential security threats [6]. This explains how an intrusion detection system responds to violations of the security policies they are monitoring. After they observed intrusion detection and prevention systems suffer from scalable and efficiency problems. To overcome these problems the authors [7] used high performance deep packet pre-filtering and memory efficient technique. This allows the IDPS to have high performance and high accuracy rates.

Anomaly detection method has introduced with high rates of false positives and a new detection system has been developed. After that they Combined both systems into one that uses both anomaly and signature based detection methodologies that produce a better detection system [8] Here the data pre-processing with the anomaly detection engine and then passing the results to the signature based engine. By this they achieved very high accuracy rate and very low false positives.

All intrusion detection/prevention systems such as IDSs, Honeypots, Snorts, Firewalls, etc. are provided a collaboration platform to detect/prevent any anomaly by centralized control via distributed verified servers. They accomplished this work by a protocol named Detection. With this, all intrusion detection/prevention Systems can detect and prevent any anomaly accurately and advance to standardization and service oriented Approaches. They also considered several scenarios and showed that the overhead traffic in network was decreased and balanced by time [20]

A way to prevent intrusion [21], without any additional cost is by proposing Snort. Snort is a free open source IDS, which has been integrated with a Cisco router to prevent intrusions. Cisco routers are very common in today's networks. Other routers like Juniper, or even simple ADSL or SOHO routers can be used but with minor changes for the router specific configuration. As ADSL is very common nowadays, ADSL routers are present everywhere and they can easily replace the Cisco router and provide intrusion prevention capabilities for homes and businesses which otherwise are not able to afford it. Router and computer (to be used as a sensor) are fundamental components of every major network, so this system does not need any additional hardware. Snort is used as an IDS and alerts are logged to a database from where they are read and router Access Control List (ACL) rules are generated based on Snort intrusion alerts and then these ACL rules are configured on the router to block the potential intrusions. Method for removing ACL rules, which may be required under some circumstances. In a fine tuned Snort IDS, false alarms will be minimum and most of the alerts will indicate intrusions. Hence, proposed system can work best to prevent intrusions with a fine tuned Snort IDS.

Here they explored the scope of the DDoS flooding attack [22] problem and attempts to combat it. Categorize the DDoS flooding attacks and classify existing counter measures based on where and when they prevent, detect, and respond to the DDoS flooding attacks. Moreover, highlight the need for a comprehensive distributed and collaborative defense approach. The intention is to stimulate the research community into developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during and after an actual attack.

The impact of security enforcement levels on the performance and usability of an enterprise information system [23]. A new analytical model is developed to investigate the relationship between the IDPS performance and the rules mode selection. In particular, they analyze the IDPS rule-checking process along with its consequent action (i.e., alert or drop) on the resulting security of the network, and on the average service time per event. Simulation was conducted to validate their performance analysis study. The results illustrate that applying different sets of rules categories and configuration parameters impacts average service time and affects system security. The results demonstrate that it is desirable to strike a balance between system security and network performance.

As the IPv4 has been largely put into the market and widely used, in a long period, there will be a situation of coexistence of network IPv6 and IPv4, which will finally became a hybrid network. Here mainly focused on the characteristics of both networks, analyzed the characteristics of the fuzzy boundary and dynamic change of topology structure of the hybrid network [24]. And based on this, a host and endpoint oriented defense thinking will be proposed, a hybrid model of intrusion detection and prevention will be presented and its effectiveness of defense various attraction will be demonstrated.

There have been some studies highlighting Network Intrusion Prevention System on Windows platform, whereas the most current available implementations of NIPS on

Windows recur to the third party firewalls lack of universality and portability. It [25] presents a new approach to filter the malicious network traffic by configuring IPSec automatically when detecting dangerous alert by cooperation of Snort and IPSec which is embedded in Windows 2000, Windows XP and Windows Server 2003. Firstly, the dynamic configuration and removal of IP Filter by programming are analyzed. Then the implementation of cooperation of Snort and IPSec is examined dissectionally. Finally, the comprehensive testing of the rewritten Snort is performed. The results of experiments prove this method can insulate and control dangerous data packets efficaciously without the third party firewalls and any amendments in Windows System Kernel

Detecting attacks disguised by evasion techniques is a challenge for signature-based Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs). Here [26] examines five common evasion techniques to determine their ability to evade recent systems. The denial-of-service (DoS) attack attempts to disable a system by exhausting its resources. Packet splitting tries to chop data into small packets, so that a system may not completely reassemble the packets for signature matching. Duplicate insertion can mislead a system if the system and the target host discard different TCP/IP packets with a duplicate offset or sequence. Payload mutation fools a system with a mutative payload. Shell code mutation transforms an attacker’s shell code to escape signature detection. The effectiveness of these techniques on three recent signature-based systems, and among them, explains why Snort can be evaded. The results indicate that duplicate insertion becomes less effective on recent systems, but packet splitting, payload mutation and shell code mutation can be still effective against them.

With the growing popularity of cloud computing, the exploitation of possible vulnerabilities grows at the same pace; the distributed nature of the cloud makes it an attractive target for potential intruders. Despite security issues delaying its adoption, cloud computing has already become an unstoppable force; thus, security mechanisms to ensure its secure adoption are an immediate need. Here, they focus on intrusion detection and prevention systems (IDPSs) to defend against the intruders. In [27] they propose a Distributed, Collaborative, and Data driven Intrusion Detection and Prevention system (DCDIDP). Its goal is to make use of the resources in the cloud and provide a holistic IDPS for all cloud service providers which collaborate with other peers in a distributed manner at different architectural levels to respond to attacks. They present the DCDIDP framework, whose infrastructure level is composed of three logical layers: network, host, and global as well as platform and software levels. Then, they review its components and discuss some existing approaches to be used for the modules in their proposed framework. Furthermore, they discuss developing a comprehensive trust management framework to support the establishment and evolution of trust among different cloud service providers

False positives and false negatives happen to every intrusion detection and intrusion prevention system. The contrivance for false positive/negative assessment with multiple IDSs/IPSs to collect FP and FN cases from real-world traffic and statistically analyze those cases in [28]. Over a period of 16 months, more than 2000 FPs and FNs have been collected and analyzed. From the statistical analysis results, we obtain three interesting findings. First, more than 92.85 percent of false cases are FPs even if the numbers of attack types for FP and FN are similar. That is mainly because the behavior of applications or the format of the application content is self-defined; that is, there is not complete conformance to the specifications of RFCs. Accordingly, when this application meets an IDS/IPS with strict detection rules, its traffic will be regarded as malicious traffic, resulting in a lot of FPs. Second, about 91 percent of FP alerts, equal to about 85 percent of false cases, are not related to security issues, but to management policy. For example, some companies and campuses limit or forbid their employees and students from using peer-to-peer applications; therefore, in order to easily detect P2P traffic, an IDS/IPS is configured to be sensitive to it. Hence, this causes alerts to be triggered easily regardless of whether the P2P application has malicious traffic or not. The last finding shows that buffer overflow, SQL server attacks, and worm slammer attacks account for 93 percent of FNs, even though they are aged attacks. This indicates that these attacks always have new variations to evade IDS/IPS detection.

While Internet and network technology have been growing rapidly, cyber-attack incidents also increase accordingly. The increasing occurrence of network attacks is an important problem to network services. A network based Intrusion Detection and Prevention System (IDPS) [29], which can efficiently detect many well-known attack types and can immediately prevent the network system from network attacks. Their approach is simple and efficient and can be used with several machine learning algorithms. We actually implement the IDPS using different machine learning algorithms and test in an online network environment. The experimental results show that our IDPS can distinguish normal network activities from main attack types (Probe and Denial of Service) with high accuracy of detection rate in a few seconds and automatically prevent the victim’s computer network from the attacks. In addition, we apply a well-known machine learning technique called C4.5 Decision Tree in their approach to consider unknown or new network attack types. Surprisingly, the supervised Decision

Tree technique can work very well, when experiencing with untrained or unknown network attack types.

They introduces the realizing process management tools of developing HIPS (host-based intrusion active defense system) [30] under Windows XP. Based on the principle of Windows process management, this paper describes the function realization of process management in this system in details such as theoretical knowledge, code, data structure and charts in various aspects. Firstly "sentence core list" is detailed. Then it explains how to realize the whole process with the “sentence core list”. After that, this paper describes the realization theory and specific method of processing thread, forced closing process and processing process module**.**

The world is more interconnected now due to the exponential growth of internet and its viability to the number of users through its various applications. This has also introduced many naïve and attack prone users to the network. The biggest challenge for today is to protect these users from any incident that can lead their mistrust towards the whole system. Intrusion is an act which is undesirable and can lead to losses in many forms of different magnitudes. IDPS (Intrusion detection and prevention) is a very important tool which not only detects the intrusion of unauthorized and suspicious activities that can compromise the security pillars (Authentication, availability, Confidentiality and Integrity) of data or information but also prevents the unexpected event. A new scheme for IDPS with the integration of Mobile Agents[31] which looks after the anomalies and responds by taking suitable measures with the help of agents.

Network Intrusion Detection and Prevention Systems (NIDPS) are one of the fundamental network components to monitor and analyze traffic to find possible attacks. Several works have been done to introduce an applicable NIDPS architecture, but none of them could cover all current NIDPS requirements. The comprehensive architecture for NIDPS [32] which is comprised of the main components and the data flow between them. This architecture consists of all NIDPS components including capture and decoding module, preprocessing, detection, response and management. The detection module will cover both misuse based and anomaly based approaches. Moreover, anomaly based detection module includes traffic and protocol anomaly detection as well as learning based approaches. The proposed architecture is designed to perform in four modes of operation: passive response mode, active response mode, fast prevention mode, and perfect prevention mode. Moreover, it is capable to work in high speed networks due to the existence of fast prevention mode. They also designed a complete management module for NIDPS which provides more useful functionalities in relation with the other modules to help them to operate in a proper manner.

Wireless sensor networks (WSNs) are vulnerable to security attacks due to the broadcast nature of transmission and limited computation capability. After intrusion detection systems (IDSs) identifies a mobile intruder, IDS may broadcast the blacklist to all nodes in network. This method is energy inefficient because all nodes have to receive and forward the alarm packet so as to exhaust communication bandwidth and node energy, especially when there are a large number of sensor nodes in the network. An energy efficient intrusion prevention mechanism in WSNs called green firewall [33]. It can isolate an intruder with less overhead, and track the intruder to continually prevent the attack. The overhead cost of the green firewall has been scrutinize and compares it with the flooding broadcast method. Extensive analysis and simulations show that green firewall can prevent the attack and effectively reduce redundant alarm packet transmissions which results in less energy consumption.

Intrusion Detection and/or Prevention Systems (IDPSs) are now a crucial defensive measure to defend against attacks intended to breach the security and operation of enterprise information systems. The IDPS configuration can, however, have a negative impact on network performance in terms of end-to end delay and packet loss. An analytical queuing model based on the embedded Markov chain [34] which analyzes the performance of the IDPS and evaluates its impact on performance. Through extensive simulations, they validate the proposed model and the numerical equations that estimate various performance metrics. Their results show that this model can be leveraged to assess and set up an effective configuration for the IDPS, achieving simultaneously the trade-off between security enforcement levels on one side and network Quality of Service (QoS) requirements on the other.

Many network attacks on the internet such as Denial of Service, Port Scanning, and Internet Worm can cause a lot of problems to a network system and tend to be more severe. Therefore, awareness of internet attacks is important. The centralized management framework of network-based Intrusion Detection and Prevention System (IDPS) via web application[35], which allows the network administrator to remotely and efficiently manage the security of network system. In new framework design, multiple network-based IDPSs can be placed in various locations to inspect internet packets in the network. Each IDPS can be easily managed from anywhere and anytime by using a personal computer or a mobile device through a web browser. The web-based management system allows the network administrator to remotely monitor and handle security issues such as managing network port and IP address, updating new network information to identify new malware attacks, as well as displaying the system performance and result analysis. In addition, our network-based IDPS approach can efficiently detect network attacks and internet worms within a short time (i.e., within 2-3 seconds). Several well-known machine learning algorithms can be applied as traffic classification technique in our IDPS approach. From experimental results, the network-based IDPS can analyze internet traffic which include normal packets and malware packets with high accuracy (more than 99%) as well as can immediately protect the network after intrusion detection.

The theoretical model of IDPS which combines application tracing and user decisions for building user profiles [36]. This novel idea is based on fact that we have seen nearly all kind of malware since Intrusion Detection System was widely deployed. The solution presents “deny any” policy as default action. Thus all behavior that is not seen before is considered as malicious. The several novel approaches, such as building four various databases used for software description and one profile database for describing user behavior, opposite existing solutions which mainly uses just one database for specifying malware. Presented architecture of this approach outlines predispositions to use this solution with crowd sourcing.

Types Of IDPS

A. Network-based

It performs packet sniffing and analyzes network traffic to identify and stop suspicious activity. They are typically deployed inline. Like a network firewall. They receive packets, analyze them, decide whether they should be permitted, and allow acceptable packets to pass through. Allow some attacks such as network service worms, e-mail .borne worms and viruses with easily recognizable characteristics (e.g., subject, attachment filename), to be detected on networks before they reach their intended targets (e.g., e-mail servers, Web servers). Most products use a combination of attack signatures and analysis of network and application protocols. Network-based products might be able to detect and stop some unknown threats through application protocol analysis. Some products allow administrators to create and deploy attack signatures for many major new malware threats in a matter of minutes. Although poorly written signature triggers false positives that block benign activity, a custom signature can block a new malware threat hours before antivirus signatures become available. However, network-based products are generally not capable of stopping malicious mobile code or Trojan horses.

We can place the Network IDPS at outside firewall, inside firewall, behind remote access server, between business units, between corporate network and partner networks, sensors may need to be placed in all switched network segments

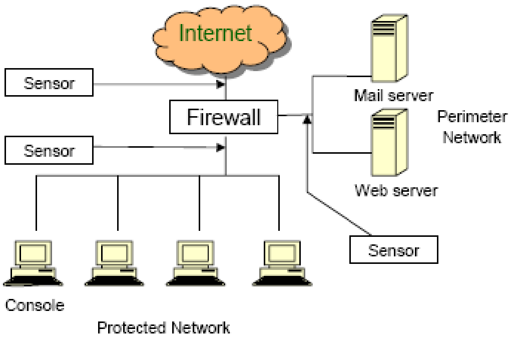

Fig. 1.Network based IDPS system.

B. *Host-based:*

These are similar in principle and purpose to network-based , except that a host-based product monitors the characteristics of a single host and the events occurring within that host, such as monitoring network traffic (only for that host), system logs, running processes, file access and modification, and system and application configuration changes. They often use a combination of attack signatures and knowledge of expected or typical behavior to identify known and unknown attacks on systems. If a host-based product monitors the host’s network traffic, it offers detection capabilities similar to a network-based. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information. For example: attempted changes to files can be effective at detecting viruses attempting to infect files and Trojan horses attempting to replace files, as well as the use of attacker tools, such as rootkits, that often are delivered by malware.

We can place the Host-based IDPS at Key servers that contain mission-critical and sensitive information, Web servers, FTP and DNS servers, E-commerce database servers and other high value assets. May also emplace these randomly to obtain probabilistic measure of hosts becoming compromised.

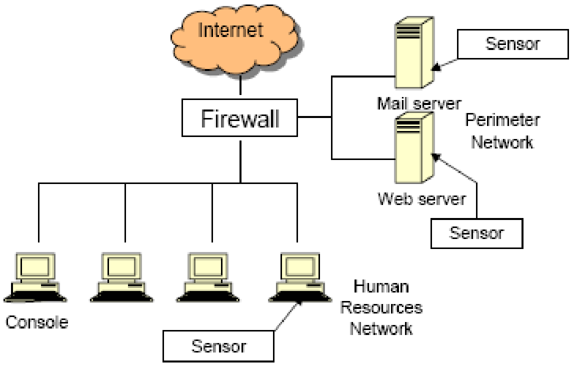

Fig. 2.Host based IDPS system

C. *Network Behavior Analysis (NBA):*

It examines network traffic to identify threats that generate unusual traffic flows, such as denial of service (DoS) and distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on an organization's internal networks, and are also sometimes deployed where they can monitor flows between an organization's networks and external networks (e.g., the Internet, business partners' networks).

D. *Wireless:*

It monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. It is most commonly deployed within range of an organization's wireless network to monitor it, but can also be deployed to locations where unauthorized wireless networking could be occurring. Organizations should consider using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity. For most environments, a combination of network-based and host-based IDPSs is needed for an effective IDPS solution. NBA technologies can also be deployed if organizations desire additional detection capabilities for DoS & DDoS attacks, worms, and other threats that NBAs are particularly good at detecting. Wireless IDPSs may also be needed if the organization determines that its wireless networks need additional monitoring or if the organization wants to ensure that rogue wireless networks are not in use in the organization's facilities.

IDPS METHODOLOGIES

There are many different methodologies used by IDPS to check the changes on the systems they monitor. These changes can be from internal personnel or external attacks. Among the many methodologies, four are standard and widely used. They are the signature based, anomaly based, Stateful protocol analysis based, and hybrid based. Most current IDPS systems use the hybrid Methodology which combines other methodologies to get better detection and prevent methods. All the methodologies use the same general model and the main difference is processing the data after collecting from the monitored environment to determine if a violation of the set policy has occurred. The architecture of IDPS system is shown in Fig.1. This architecture was developed by the Intrusion Detection Working Group and has four functional blocks, the Event block which gathers events from the monitored system and will be analyzed by other blocks, then the Database block which stores the events from the event blocks, then the Analysis block which processes the events and sends an alert, and final the Response blocks whose purpose is to respond to an intrusion and stop it [9]

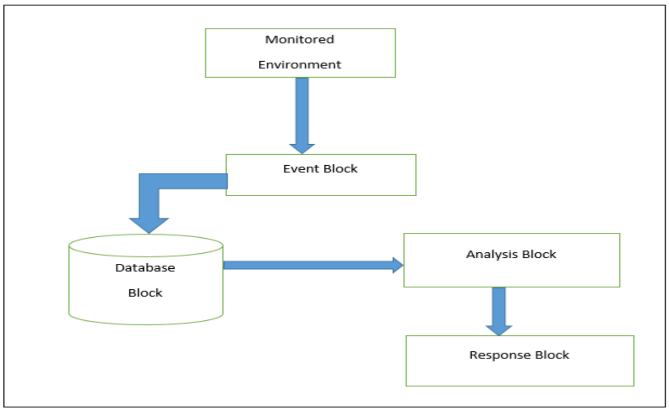

Fig. 3.General architecture of an IDPS system.

A. Signature Based Methodology

Signature based methodology works by comparing observed signatures to the signatures on file. This file can be a list of known attack signatures or database. Any signature observed on the monitored environment that matches the signatures on file will marked as a thread for security policy or as an attack. The signature based IDPS has little drawback since it does not inspect every activity or network traffic on the monitored environment. Instead it only searches for known signatures in the database or file. The signature based methodology system is easy to deploy since it does not need to learn the environment [10]. This methodology works by simply comparing, searching, and inspecting the contents of captured network packets for known threats signatures. It also compares behaviour signatures against allowed behaviour signatures.

Signature based methodology also analyzes the systems calls for known threats payload [11]. Signature based methodology is very effective against know attacks/violations but it cannot detect new attacks until it is updated with new signatures. Signature based IDPS are easy to evade since they are based on known attacks and are dependent on new signatures to be applied before they can detect new attacks [12]

Signature based detection systems can be easily bypassed by attackers who modify known attacks and target systems that have not been updated with new signatures that detect the modification. Signature based methodology requires significant resources to keep up with the potential infinite number of modifications to known threats. Signature based methodology is simpler to modify and improve since its performance is mainly based on the signatures or rules deployed [13]. The general architecture of a signature based methodology is shown in Fig. 2. This architecture uses the detector to find and compare activity signatures found in the monitored environment to the known signatures in the signature database. If a match is found, an alert is issued and there is no match, then the detector does nothing.

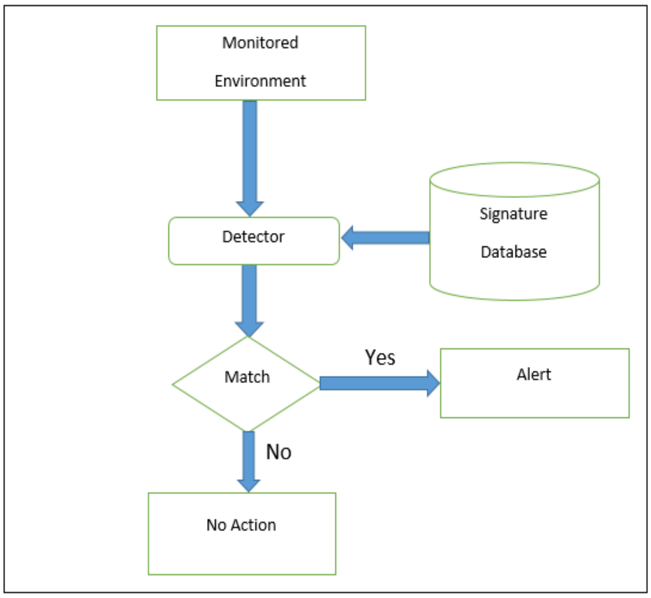

Fig. 4. Signature based methodology architecture

B.Anomaly Based Methodology

Anomaly based methodology works by comparing observed activity against a baseline profile. The baseline profile is learning the normal behaviour of the monitored system and is developed during the learning period where the IDPS learns the environment and develops a normal profile of the monitored system. This environment can be networks, users, systems and so on.

The profile can be fixed or dynamic. A fixed profile does not change once established while a dynamic profile changes as the systems have been monitored [14]. A dynamic profile adds extra over head to the system as the IDPS continues to update the profile which also opens it to evasion. An attacker can evade the IDPS that uses a dynamic profile by spreading the attack over a long time period. In doing so, the attack becomes part of the profile as the IDPS incorporates the changes into the profile as normal system changes. Using a predefined threshold any deviations that fall outside the threshold are reported as violations. A fixed profile is very effective at detecting new attacks since any change from normal behaviour is classified as an anomaly.

Anomaly based methodologies can detect zero-day attacks to environment without any updates to the system. Anomaly intrusion detection methodology uses three general techniques for detecting anomalies and these are the statistical anomaly detection, Knowledge/data-mining, and machine learning based [14]. The statistical anomaly techniques are used to build the two required profiles, one during the learning phase which is then used as the baseline profile and the current profile which is compared to the baseline profile and any differences that found a marked as anomalies depending on the threshold settings of the monitored environment [15]. The threshold must be tuned according to the requirements and behaviour of the environment being monitored for the systems to be effective. The knowledge/data-mining technique is used to automate the way the technique monitor searches for anomalies and this process places a very high overheard on the system. The technique produces the most false positives and false negatives due to the high overhead that result from the complicated task of identifying and correctly categorizing observed events on the system [16]. The machine learning technique works by analyzing the system calls and it is the widely used technique [17].

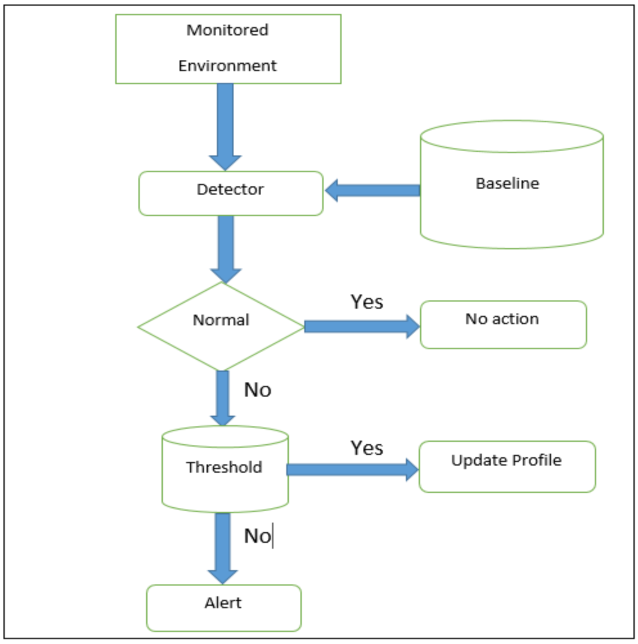

Fig. 5. Anomaly based methodology architecture

The general architecture of an anomaly based IDPS system is shown in Fig 3. The monitored environment is examined by the detector to observe events against the baseline profile. If the observed events match the baseline, no action is taken, but if it does not match the baseline profile and it is within the acceptable threshold range then the profile is updated. If the observed events do not match the baseline profile and falls outside the threshold range they are marked as an anomaly and alert is issued.

C.Stateful Protocol Analysis Based Methodology

The Stateful protocol analysis methodology works by comparing established profiles of how protocols should behave against the observed behaviour. The established protocol profiles are designed and established by vendors. Unlike the signature based methodology which only compares observed behaviour against a list, Stateful protocol analysis has a deep understanding of how the protocols and applications should interact/work. This deep understanding/analysis places a very high overhead on the systems [14]. Stateful protocol analysis blends and compliments other IDPS methodologies well which has led to rise of Hybrid methodologies [13]. Stateful protocol analysis's deep understanding of how protocol should behave is used as a base for developing IDPS that understand web traffic behaviour and are effective at protecting websites [13]. Although the Stateful protocol analysis has a deep understanding of the monitored protocols, it can be easily evaded by attacks that follow and stay within the acceptable behaviour of protocols. Stateful protocol analysis methodologies and techniques have slowly been adapted and integrated into other methodologies over the past decade.

This has led to the decline of IDPS that utilize just stateful protocol analysis methodology. The majority of the research on IDPS methodologies mainly concentrates on anomaly, signature, and hybrid methodologies which further reduce the viability of Stateful protocol analysis as a standalone IDPS methodology. The general architecture of Stateful protocol analysis is shown in fig.4. This architecture is identical to that of the signature based methodology with one exception, instead of the signature database the Stateful protocol analysis has database of acceptable protocol behavior.

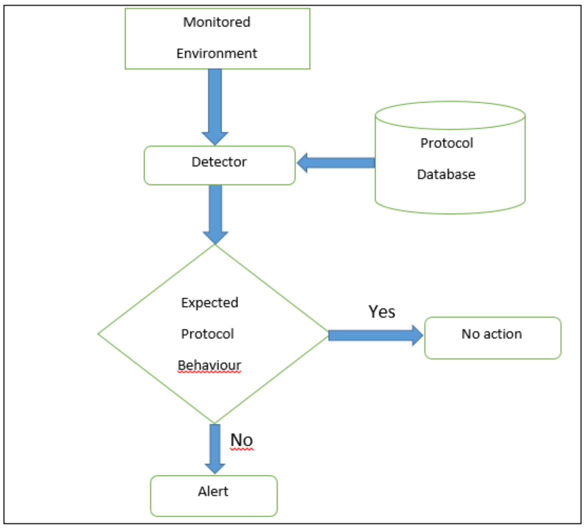

Fig.6. Stateful protocol analysis based methodology architecture

D. *Hybrid Based Methodology*

The hybrid based methodology works by combining two or more of the other methodologies. The result is a better methodology that takes strengths of the combined methodologies. Prelude is one of the first hybrid IDS that offered a framework based on the Intrusion Detection Message Exchange Format (IDMEF) an IETF standard that allows different sensors to communicate[17]. In [18] Snort is modified by adding an anomaly based engine to its signature based engine to create a better detection and then the new hybrid systems is tested against the regular Snort using same test data. The hybrid system detected more intrusions than the regular one. A hybrid intrusion detection system of cluster-based wireless sensors networks was proposed that worked by breaking the detection into two, first it used anomaly based model to filter the data and then it used signature based model to detect intrusion attempts. Another model for a hybrid methodology was proposed based on how the human immune system works [19]. The proposed system is based on the framework of the human immune system, that uses a hybrid architecture which applies both anomaly and misuse detection approaches" [19]. A general over view of a hybrid based methodology is shown in Fig. 5 in which three methodologies are combined. The monitored environment is analyzed by stateful protocol analysis methodology and passed to the signature based methodology and then finally to anomaly based methodology. This produces a better system.

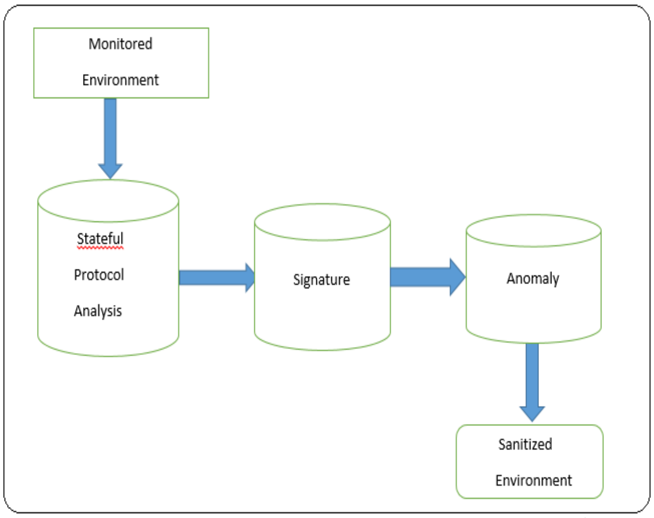

Fig. 7- Hybrid based methodology architecture

Parametric Evaluation

This section offers a description of ways for evaluating intrusion detection and prevention system (IDPS) methodologies and the systems that are based on these methodologies. Table 1 can be used to evaluate any intrusion detection and prevention system (IDPS) whether it uses one of the three main methodologies or a combination of the other methodologies. The parameters used for evaluating IDPS methodologies are discussed in section *A* to *M*

A. High Accuracy Rate

An IDPS should have a high accuracy rate when detecting and analyzing possible threats. The signature based methodology has a high accuracy rate on known threats but its overall rate is lower that the anomaly based methodology which can detect previously known threats. The hybrid based methodology offers the best accuracy rates.

B.Market Share

Market share is the measure of the methodology's dominance in the deployed systems. The signature based methodology far outweighs the other three methodologies, followed by Stateful protocol analysis. The anomaly and hybrid based methodology are the bottom but their adaption is growing much faster and will soon surpass the first two methodologies.

C.Resistance to evasion

The intrusion detection and prevention system (IDPS) should be able to detect evasion attempts and stop them. These attempts are more common with the signature and stateful protocol analysis based intrusion detection and prevention system (IDPS) due their dependence on signatures. Anomaly based intrusion detection and prevention system (IDPS) have better resistance to evasion, but the hybrid based system offers the best resistance to evasion attempts due to the combination of other methodologies

D.Maturity Level

Maturity level looks at how long a methodology has been around and how stable it is. The signature based methodology is the most mature, followed by the Stateful protocol analysis and anomaly based methodologies. The hybrid methodology is at the bottom of this list, but it is growing at a much faster than the others.

E.Maintenance

The anomaly based methodology requires the least amount of maintenance since it does not require updates to detect new threats. The other three methodologies require constant signature updates in order to keep up with new threats. This constant updating of signatures adds to the resources required to maintain the methodology.

F.Scalability

Scalability is the ability of an IDPS to scale and grow with environment once deployed. The signature and Stateful protocol analysis based methodologies are easy to scale since they are based on signatures that can be easily scaled. A hybrid based methodology can be easily scale depending on the underlying methodologies. The anomaly based methodology is the least scalable methodology due the time it requires to learn and build its baseline profiles.

G.Overhead on Monitored System

The intrusion detection and prevention system (IDPS) should not place a lot of overhead on the monitored systems; it should work without affecting the performance of monitored systems. Signature and Stateful protocol analysis places the least overhead on the monitored systems. The hybrid based methodology can place a high overhead burden on the monitored system depending on the combined methodologies. The anomaly based methodology places the most overhead on the monitored system.

H.Performance

The intrusion detection and prevention system should be able to perform at peak performance under all condition on the monitored system without becoming a bottle neck or reducing its efficiency. The signature and Stateful protocol analysis based methodologies offers better performance than anomaly and hybrid based methodologies since they only check for well-defined signatures which do not require as much resources.

I.Protection against New Attacks

The intrusion detection and prevention system should be able to detect new threats. The anomaly based methodology does detect new attacks without any updates unlike the signature and Stateful protocol analysis that require their signatures to be updated before they can detect previously unknown threats. The hybrid based methodology can detect new threats if one of the underlying methodologies is anomaly based.

J.Easy to Use

The intrusion detection and prevention system should be easy to use and understand. This means it produces less false positives and false negatives which make it easier to analyze and understand the alerts. The signature and the Stateful protocol analysis methodologies are easier to use since they produce fewer alerts. The hybrid based methodology can be easier than the anomaly depending on its underlying methodologies. The anomaly requires more resources to manage the high volumes of alerts it produces.

K.Easy to Configure

The intrusion detection and prevention system (IDPS) should be easy to install and integrate with other security tools already in the environment. The signature and the Stateful protocol analysis methodologies are easier to install and configure. They do not require as much time to tune since they use signatures that can be updated automatically in some cases. The anomaly and the hybrid depending on the combined methodologies require more time to configure, learn, and tune the environment.

L.False Positives

False positives happen as a result of a methodology misclassifying a non-threat event as a threat. The anomaly based methodology is plagued by false positives. The signature and Stateful protocol analysis based methodologies produces the least number of false positives. The hybrid based methodology's level of false positives is low if anomaly based is not part of its underlying methodologies.

M.False Negatives

False negatives are a result on a methodology classifying threats as non-threats. The anomaly based methodology produces the most false negatives when compared with signature and the Stateful protocol analysis based methodologies. The hybrid based methodology produces less false negatives if it does not use anomaly based methodology as one of its underlying methodologies.

Using the above parameters we have evaluated IDPS systems. By using these, we can compare IDPS systems in a more effective manner as shown in table [1].

TABLE 1
PARAMETERS FOR EVALUATING IDPS METHODOLOGIES

Properties	Signature	Anomaly	Stateful protocol Analysis	Hybrid
Accuracy ra	Medium	Medium	Medium	High
Market Share	High	Medium	Medium	Medium
Resistance to Evasion	Low	Medium	Low	High
Maturity Level	High	High	High	Medium
Maintenance	Medium	Low	Medium	Medium
Scalability	High	Medium	High	Medium
Overhead on Monitored System	Low	Medium	Low	Medium
Performance	High	Medium	High	Medium
Protection against New Attacks	Low	High	Medium	High
Easy to Use	Low	Medium	Low	Low
Easy to Configure	Yes	No	Yes	No
False Positives	Low	High	Low	Low
False Negatives	Medium	High	Medium	Low

In the table we analyze different parameters with different methodologies. Hybrid-based method has more features when compared to other methodologies. It has low maintenance cost and it is better in false positives and false negatives. It is difficult to configure and use when compared to another methodologies. It is good in finding the new attacks when compared to others.

Conclusion

This paper presented the four main methodologies that are used in intrusion detection and prevention systems. These methodologies are signature based, anomaly based, stateful protocol analysis, and hybrid based. Although the anomaly based methodology has the edge on the other two on detecting new threats without any updates or input for the users, most current IDPS on the market utilizes a combination of the four main methodologies. The paper also offered parameters to easily compare and evaluate IDPS methodologies that are used by IDPS products on the market. In future we are planning to evaluate the parameters using some commercial and open source tools. We want to develop enhanced IDPS methodology with better performance.

References

[1] Animesh Patcha, Jung-Min Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends, Computer Networks,” The International Journal of Computer and Telecommunications Networking, Vol.51, No.12, August, 2007, pp.3448-3470.

[2] Rebecca Bace, “An introduction to intrusion detection and assessment for system and network security management.” ICSA Intrusion Detection Systems Consortium Technical Report, 1999.

[3] James P. Anderson, “Computer security threat monitoring and surveillance,” James P. Anderson Co., Fort Washington, Pennsylvania, technical Report, April 1980.

[4] Tarek S. Sobh, “Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art,” Computer Standards & Interfaces 28 , 2006, pp. 670–694.

[5] Fredrik.Valeur, Giovanni Vigna, Christopher Kruegel, Richard A. Kemmerer, “A comprehensive approach to intrusion detection alert correlation,” IEEE Transactions on Dependable and Secure Computing, Vol. 1, NO. 3, 2004.

[6] Xuan D. Hoang, Jiankun Hu, Peter Bertok, “A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference,” Journal of Net- work and Computer Applications 32, 2009, pp. 1219–1228.

[7] Elshoush H. Tagelsir, Izzeldin M. Osman, “Alert correlation in collaborative intelligent intrusion detection systems—A survey.” Applied Soft Computing 11, 2011, pp. 4349-4365.

[8] James Cannady, Jay Harrell, “A comparative analysis of current Intrusion detection technologies,” Houston 1996, Proc. 4th Technology for Information Security Conference.

[9] Terry Brugger, “KDD cup’99 dataset (network intrusion) considered harmful,” http://www.kdnuggets.com/news/2007/n18/4i.html, 2007.

[10] Dorothy, Denning. “An intrusion-detection model,” IEEE Transactions on Software Engineering, Vol. SE-13, No.2. February, 1987.

[11] Alfonso Valdes, Keith Skinner, “Probabilistic alert correlation,” 4th International Symposium on Recent Advances in Intrusion Detection (RAID2001), 2001, pp.54–68.

[12] Indraneel Mukhopadhyay, Mohuya Chakraborty and Satyajit Chakrabarti, "A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems," Journal of Information Security, Vol. 2 No. 1, pp. 28-38.

[13] Justin Lee, Stuart Moskovics, Lucas Silacci, “A Survey of Intrusion Detection Analysis Methods,” CSE 221, University of California, San Diego, Spring 1999.

[14] Karen Scarfone and Peter Mell, “Guide to Intrusion Detection and PreventionSystems(IDPS),” http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, 2007.

[15] Pedro Garcı´a-Teodoroa, Jesus E. Dı´az-Verdejoa, Gabriel .Macia-Ferna´ndeza, Enrique Va´zquezb, “Anomaly-based network intrusion detection: Techniques, systems and challenge,” Computers Security 28.1-2, 2009, pp. 18-28.

[16] Chih-Fong Tsai, YuFeng Hsu, Chia-Ying Lin, W.Y.Lin, “Intrusion detection by machine learning: A review,” Expert Systems with Applications, Vol 36, No.10. December 2009, pp.11994-12000.

[17] Ning Weng, Luke Vespa, Benfano Soewito, “Deep packet pre-filtering and finite state encoding for adaptive intrusion detection system,” Computer Networks, Vol. 55, 2011, pp. 1648–1661.

[18] Ali M. Aydın, Halim A. Zaim, Gokhan K. Ceylan, “A hybrid intrusion detection system design for computer network security,” Computers and Electrical Engineering, Vol. 35, 2009, pp. 517–526.

[19] Kenneth L. Ingham, Anil Somayaji, “A Methodology for Designing Accurate Anomaly Detection Systems,” 4th international IFIPACM Latin American conference on Networking LANC 07, 2007, pp.139

[20] Leila Rikhtechi, Afshin Rezakhani Roozbahani, “Creating a Standard Platform for All Intrusion Detection/Prevention Systems,” Second International Conference on Computer Modeling and Simulation,2010,pp.41-44.

[21] Muhammad Naveed, Shams un Nihar, Mohammad Inayatullah Babar, “Network Intrusion Prevention by Configuring ACLs on the Routers, based on Snort IDS alerts,” 6th International Conference on Emerging Technologies (ICET),2010,pp.234-239.

[22] Saman Taghavi Zargar, James Joshi, David Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” IEEE COMMUNICATIONS SURVEYS & TUTORIALS,2013,pp.2046-2069

[23] Khalid Alsubhi, Nizar Bouabdallah , Raouf Boutaba, “Performance Analysis in Intrusion Detection and Prevention Systems,” IEEE International Symposium on Integrated Network Management 2011,2011,pp.369-376.

[24] Ke Yun, Zhu Jian, “Research of hybrid intrusion detection and prevention system for IPv6 network,” IEEE,2011.

[25] Jiqiang Zhai, Yining Xie, “Researh on Network Intrusion Prevention System Based on Snort,” IEEE 2011 The 6th International Forum on Strategic Technology,2011,pp.1133-1166.

[26] Tsung-Huan Cheng, Ying-Dar Lin, Yuan-Cheng Lai, and Po-Ching Lin, “Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems,” IEEE COMMUNICATIONS SURVEYS & TUTORIALS,2012,pp.1011-1020.

[27] saman taghavi,Hassan Takabi, “A Distributed, Collaborative, and Data-driven Intrusion Detection and Prevention Framework for Cloud Computing Environments,” International conference on collaborative computing ,2011,pp.332-341.

[28] Cheng-Yuan Ho, Yuan-Cheng Lai, I-Wei Chen, Fu-Yu Wang, and Wei-Hsuan Tai, “Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems,” IEEE Communications Magazine ,2012,pp.146-154.

[29] N. Wattanapongsakorn, S. Srakaew E. Wonghirunsombat, C. Sribavonmongkol,T. Junhom, P. Jongsubsook, C. Charnsripinyo, “A Practical Network-based Intrusion Detection and Prevention System,” IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications ,2012,pp.209-214.

[30] Xiaoyan Yang, Wen Dong and Ming Liu, “Design and Implementation of Process Management for Host Intrusion Prevention System,” Conference on Dependable Computing (CDC’2010), 2010,pp.343-345.

[31] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma, “A Novelty based Intrusion Detection and Prevention System,” Fourth International Conference on Computational Intelligence and Communication Networks, 2012,pp.695-699.

[32] Minoo Sadat Mirpuryan,Tinna Tavizi, Hossein Gharaee, “A Comprehensive Network Intrusion Detection and Prevention System Architecture,” 6'th International Symposium on Telecommunications (IST'2012), 2012,pp.954-958.

[33] Ping Yi, Ting Zhu, Qingquan Zhang , Yue Wu, “Green Firewall: an Energy-Efficient Intrusion Prevention Mechanism in Wireless Sensor Network,” Symposium on Selected Areas in Communications, 2012,pp.3037-3042

[34] Khalid Alsubhi, Mohamed Faten Zhani, Raouf Boutaba, “Embedded Markov Process based Model for Performance Analysis of Intrusion Detection and Prevention System,” Communication and information System Security Symposium, 2013,pp.898-903

[35] Ekgapark Wonghirunsombat , Teewalee Asawaniwed, Vassapon Hanchana, Naruemon Wattanapongsakorn, Sanan Srakaew ,Chalermpol Charnsripinyo, “A Centralized Management Framework of Networkbased Intrusion Detection and Prevention System,” 10th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2013,pp.183-188

[36] M. Tomášek, M. Čajkovský and I. Klimek, “Cloud-Centric Application Tracing and User Monitoring Intrusion Prevention System,” IEEE 17th International Conference on Intelligent Engineering Systems, 2013,pp.339-343.