ARPN Journal of Science and Technology

http://www.ejournalofscience.org

Intrusion Detection and Prevention System: Classification and Quick Review

[1] Bilal Maqbool Beigh, [2] Prof.M.A.Peer
[1] Research Scholar, Computer Science Department, University of Kashmir, India
[2] Chairmen BOPEE J&K India
[1] bilal.beigh@gmail.com, [1] bmbeigh@gmail.com,
[2] drpeerma@gmail.com

ABSTRACT

Besides the growth of information technology, the security has remained a main challenging issue for organizations. Most of the organizations are facing an increasing number of threats every day in the form of viruses and attack etc. Since many different mechanisms were opted by organizations in the form of intrusion detection and prevention system to protect its organizations for these kinds of attacks. As we are using IDPS for security but still there are security breaches in every organization. In order to understand the security risks and IDPS, we will make a quick review in the form of classification of these IDPS and classifying them in certain groups, we will make a parameter based comparative analysis of different intrusion detection and prevention tools. This paper will mainly focus on classification and comparative analysis of IDPS.

Keywords: *Security, Issue, Threats, Viruses, attacks, Intrusion, detection, Prevention, Parameters, IDPS, analysis.*

1. INTRODUCTION

From last two decades, the networking of computers has been a revolutionary field to improvise. In this field of intrusion detection and prevention system, the possibility and opportunity are limitless, so too are risks and chances of malicious/ dedicated attacks towards the networks.

It is very important for an organization to design security mechanisms that prevent unauthorized access to system resources and confidential data of the company. However the complete control of security breaches seems to be impossible at present. But, we can try to detect these intrusion attempts and accordingly actions may be taken to mitigate them. This field of study is called as intrusion detection prevention. We will provide a brief overview of intrusion detection systems in this paper according to the field from which the basic domain is attached.

Anderson, while introducing the concept of intrusion detection in 1980's, defined an intrusion as attempt or a threat to be potential possibility of a deliberate unauthorized attempt to:

a. Information Availability.
b. Information Usage.
c. Render a system unrealistic or unusable

Or

Intrusion detection provides the following:

a. Monitoring and analysis of user and system activity.
b. Checking and comparing vulnerabilities.
c. Availability of critical data files
d. Statistical analysis of activity patterns based on the matching to known attacks
e. Abnormal behavior analysis
f. Operating system analysis and comparison with stable state.

Thus intrusion detection can be defined as technology designed to observe computer activities for the purpose of finding security violations or we can say Intrusion detection is the process of identifying and responding to malicious activity targeted at computing and networking sources [1]. Also Intrusion preventions techniques such as user authentication and information protection have been used to protect computer systems as a first time of defense. Intrusion prevention alone is not sufficient because as system become more complex, there is always exploitable weakness in the systems due to design and programming errors. Now a day's ID is one of high priority task for the network administrators and professionals. We will discuss the classification of ID&PS and their trends towards the defenses and also will elaborate the findings in each category of IDS and their respective methods.

ARPN Journal of Science and Technology

http://www.ejournalofscience.org

2. WHAT INTRUSION DETECTION SYSTEM CAN AND CAN NOT PROVIDE

The IDS is not the full fledged solution to the security issues we face in today's world, But IDS will serve the purpose of making our system secure in some cases. Before you will choose IDS you must be familiar with what you can and cannot expect from your intrusion detection system. In the following subsections, I will try to show a few examples of what an Intrusion Detection Systems are capable of, but each network environment varies and each system needs to be tailored to meet your enterprise environment needs [2].

2.1 The IDS CAN provide the following:

a. CAN add consummate to the rest of you infrastructure.
b. CAN trace user activity from point of entry to point of impingement.
c. CAN check and report alterations to data.
d. CAN automate a task of monitoring the Internet searching for the latest attacks.
e. CAN detect when your system is under attack.
f. CAN detect errors in your system configuration.
g. CAN guide system administrator in the vital step of establishing a policy for your computing assets.
h. CAN make the security management of your system possible by non-expert staff.

2.2 The IDS CAN NOT provide:

a. CAN NOT compensate for a weak identification and authentication mechanisms.
b. CAN NOT conduct investigations of attacks without human intervention.
c. CAN NOT compensate for weaknesses in network protocols.
d. CAN NOT compensate for problems in the quality or integrity of information the system provides.
e. CAN NOT analyze all the traffic on a busy network.
f. CAN NOT always deal with problems involving packet-level attacks.
g. CAN NOT deal with some of the modern network hardware and features.

3. THE IDS LIFE CYCLE

The software developers/ Network Scientist made new intrusion detection system and releases these new IDS products to compete the market requirements. In evaluating these new types of systems comprehensive product evaluation information is lacking very much. It is a huge challenge to big organizations to Hiring and retaining personnel to competently administer security in general and intrusion detection in particular are increasingly challenging [3]. Rapid development and changes in information technology make it difficult for an organization to implement an effective, long-term security strategy. Thus there should be some guidelines which will help the network administrator to pick the ID system for their security purpose. In order to understand IDS in general, we should be able to grasp the life cycle of IDS. The overall life cycle if IDS can be categorized in the following sections:

a. Rating and Choice
b. Placing IDS
c. Operation and Use
d. Sustenance.

3.1 Rating and Choice

Every organization wants to secure their confidential resources, for that they have to make some selection in terms of firewalls, IDs etc. Before going for any products, the company should consider all the available resources for basic system operation and maintenance. Thus should be able to pick the appropriate IDS which will meet the needs within the constraints laid down by company. This task is very difficult, As there is no industry standard against which we will compare IDS. Hence there is a need of providing a standard benchmark for IDS. The new product cycle for commercial IDSs is rapid, and information and systems quickly become obsolete. Steven Northcutt recommends the use of product guides that are updated at least monthly. Relatively little objective third party evaluation of IDSs is available, while trade press reports are generally spotty and superficial. Setting up a facility to objectively compare IDSs will be prohibitively expensive for all but the largest potential users, and some third-party or industry sponsored effort is needed. Marketing literature rarely describes how well a given IDS finds intruders and how much work is required to use and maintain that system in a fully functioning network with significant daily traffic. IDS vendors usually specify which prototypical attacks their systems can find, but without access to deployment environments, they cannot describe

ARPN Journal of Science and Technology

http://www.ejournalofscience.org

how well their systems detect real attacks while avoiding false alarms. Edward Amoroso and Richard Kwapniewski recently provided guidance in selecting IDS [4].

3.2 Placing IDS

Once an ID system is selected, a number of decisions will determine whether it is deployed effectively. These include decisions about how to protect the organization's most critical assets, how to configure the IDS to reflect the organization's security policies, and what procedures to follow in case of an attack to preserve evidence for possible prosecutions. Organizations must also decide how to handle alerts from the IDS and how these alerts will be correlated with other information such as system or application logs.

An ID does not prevent attacks. In fact, if attackers realize that the network they are attacking has IDS, they may attack the IDS first to disable it or force it to provide false information that distracts security personnel from the actual attack. Many intrusion detection tools have security weaknesses that could include failing to encrypt log files, omitting access control, and failing to perform integrity checks on IDS files. The Intrusion Detection Working Group of the Internet Engineering Task Force is developing a common alert format that will let IDS alerts from different systems be reported to a common display console.

3.3 Operation and Use

After choosing , deploying and configuring IDS, the system must monitor for alerts and should report the same successfully. The IDS should be able to monitor the alert and response should be activated for blocking the attack or the information should be send to administrator immediately, so that he will stop the attack manually. IDSs themselves are logical targets for attack. Smart intruders who realize that an IDS has been deployed on a network they are attacking will likely attack the IDS first, disabling it or forcing it to provide false information (distracting security personnel from the actual attack in progress). In addition, many commercial and research ID tools have security weaknesses resulting from flawed design assumptions. These can include failing to encrypt log files, omitting access control, and failing to perform integrity checks on IDS files.

3.4 Sustenance

An IDS must be constantly monitored after it is deployed. Procedures must be developed for responding to alerts; these procedures will determine how staff members analyze and act on alerts, and how staff monitors the outcomes of both manual and automatic responses. In addition, as upgrades become available, they should be installed to keep the IDS as current and secure as possible.

Technology alone cannot maintain network security; trained technical staff are needed to operate and maintain the technology. Unfortunately, the demand for qualified intrusion analysts and system/network administrators who are knowledgeable about and experienced in computer security is increasing more rapidly than the supply.

When AN ID is properly maintained, it can provide warnings about when a system is being attacked, even if the system is not vulnerable to the specific attack. The information from these warnings can be used to further increase the system's resistance to attacks. An IDS can also confirm whether other security mechanisms, such as firewalls, are secure. If the necessary time and effort is spent on IDS through its life cycle, its capabilities will make it a useful and effective component of an overall security plan.

4. WORKING PHASES OF INTRUSION ANALYSIS

Intrusion analysis process is very important for the networks and the system sand can be broadly broken into four phases and the phases are as follows:[22]

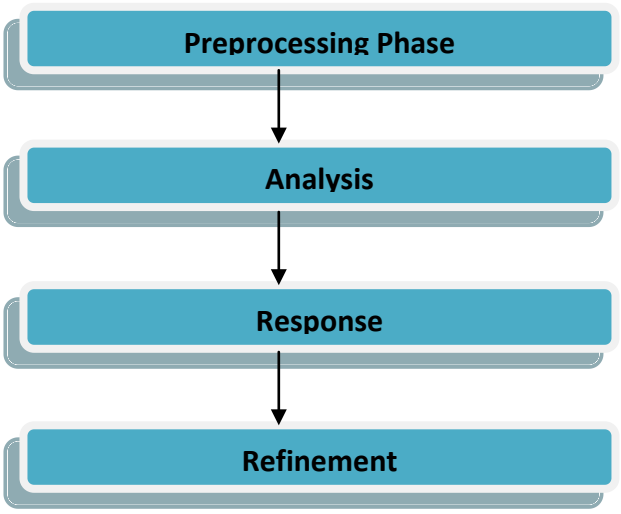

Fig 1: Phases of IDS or IPS

ARPN Journal of Science and Technology

http://www.ejournalofscience.org

4.1 Preprocessing

It is the first phase of the Intrusion detection system. The function of this Phase is to collects the activity from an IDs or IPS sensors. In this step, data are organized in some pattern for classification. This stage would help in determine the format the data are put into, which would be a canonical format or a structured database. Once the data are formatted they are further classified, this classifications depends upon the analysis schemas being used.

4.2 Analysis

Once the phase of preprocessing is completed, the analysis stage begins. The data record is compared with the Knowledge base. The data record will either be logged as an intrusion event or it will be dropped and next data record is analyzed.

4.3 Response

In the intrusion detection systems we get the information passively after the fact, so we would get an alert after the fact. The response can be set to be automatically performed, or can be done manually after someone manually analyzed the situation.

4.4 Refinement

This is the stage where fine tunings is done, based on the previous usage and detected intrusions. This helps in reducing false positive levels and to have more security tool. These are tool like CTR (Cisco Threat Response) that helps with the refining stage by actually making sure that an alert is valid by checking whether you are vulnerable to the attack or not. Rule based detection, even known as signature detection, pattern matching and misuse detection.

5. CLASSIFICATION OF INTRUSION DETECTION SYSTEM

In order to discuss IDS properly it is necessary to distinguish between the different IDS. Therefore the classification of ID systems is very important. Here in this paper, we are attempting to classify the ID system via two patterns.

5.1 Scheme I

The first classification is based on the place where ID systems can be placed and the second one is based on analysis of the technique used. While taking the first scheme into consideration, the ID system has been classified in three groups.

a. Host Based Intrusion Detection System
b. Network Based Intrusion Detection System.
c. Hybrid Based Intrusion Detection System

a. Host Based Intrusion Detection System:

A HIDS works with a software agent on a host. It is derived from mere log file analyzers. Modern host based Intrusion Detection Systems are designed as host based applications running in the background of presumed critical, sensitive hosts, such as Mail Servers, DNS Servers, web servers, database servers, etc. It identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. You can see in Fig. 1 how aHIDS is built. In fact there are also some application-based IDS which a part of this category. One good example is OSSEC [6]which is a open source IDS.

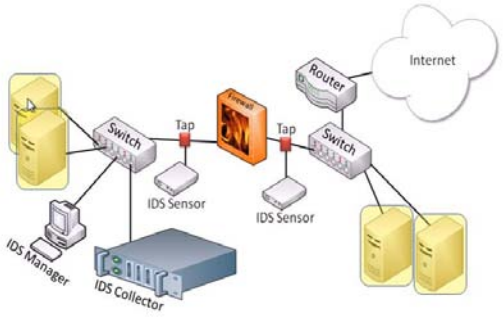

Fig.2: Host based Intrusion detection system

b. Network Intrusion Detection Systems

A NIDS is an independent platform that identifies intrusions by examining network traffic and monitoring multiple hosts. NIDSs gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ)or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious

traffic. In Fig. 2 you can see a typically built NIDS. An often used Software example of a NIDS, is SNORT.

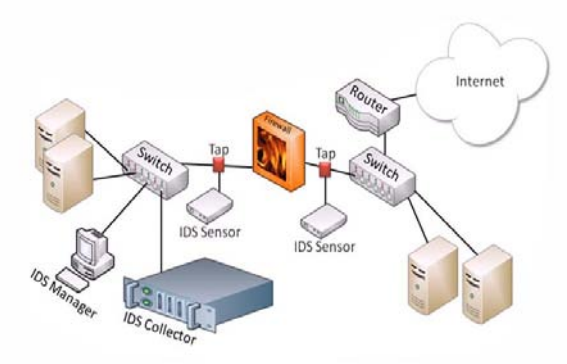

Fig 2: Network Intrusion Detection System

c. Hybrid Intrusion Detection Systems:

Different types of Intrusion Detection Systems can also be combined. Combined systems are called Hybrid Intrusion Detection Systems. To completing this overview it must be mentioned, that IDSs can also be system-specific. This means they can use custom tools and Honey pots for getting a better efficiency [7].

5.2 Scheme II

In the second classification scheme, we will classify the ID systems based on analysis of the intrusion system. Therefore the second classification scheme is based on analysis pattern of the intrusion detection system. This scheme pattern can be broadly divided into two groups:

a. Mis-use Based Intrusion Detection System
b. Anomaly Based Intrusion Detection System.

a. Mis-Use Based Intrusion Detection System:

Most commercial IDS look for attack signatures: specific patterns of network traffic or activity in log files that indicate suspicious behavior are known as knowledge-based or misuse detection IDS. Example signatures might include:

- a number of recent failed login attempts on a sensitive host;
- a certain pattern of bits in an IP packet, indicating a buffer overflow attack;
- Certain types of TCP SYN packets, indicating an SYN flood Does attack.

b. Signature-Based IDS

A signature based IDS monitors packets in the network and compares with preconfigured and predetermined attack patterns known as signatures. When a new attack is recognized experts or programs have to identify typical patterns in such attacks, which can be made into signature. Since this process takes time, there will be a lag between the new threat discovered and signature being applied in IDS for detecting the threat. During this lag time your IDS will be unable to identify the threat.[9]To reduce further lag, security software using such signatures should be updated as frequently as feasible. You can see an S-B IDS with an implemented Attack Signature Database in Fig. 3.

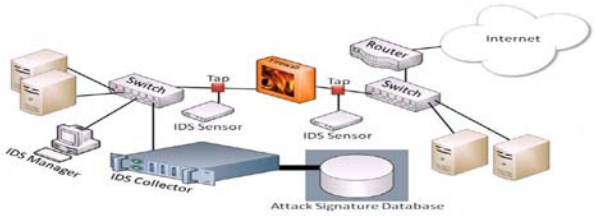

Fig 4: Signature Based Intrusion Detection System.

The different types which comes under thus category are :

i. Expert system
ii. Signature Analysis
iii. Petri Nets
iv. State Transition

i. Expert Systems:

These type of systems works on a previously defined set of rules describing an attack. All security related events incorporated in an audit trail are translated in terms of if-then-else rules. Examples are Wisdom & Sense and Computer Watch (developed at AT&T).

ii. Signature Analysis:

Similarly to expert System approach, this method is based on the attack knowledge. They transform the semantic description of an attack into the appropriate audit trail format. Thus, attack signatures can be found in logs or input data streams in a straightforward way. An attack scenario can be described, for example, as a sequence of audit events that a given attack generates or patterns of searchable data that are captured in the audit trail. This method uses

abstract equivalents of audit trail data. Detection is accomplished by using common text string matching mechanisms. Typically, it is a very powerful technique and as such very often employed in commercial systems (for example Stalker, Real Secure, Net Ranger, Emerald expert-BSM).

iii. Petri Nets:

The Petri Nets approach is often used to generalize attacks from expert knowledge bases and to represent attacks graphically. Purdue University's IDIOT system uses Colored Petri Nets. With this technique, it is easy for system administrators to add new signatures to the system. However, matching a complex signature to the audit trail data may be time-consuming. The technique is not used in commercial systems.

iv. State-transition analysis

Here, an attack is described with a set of goals and transitions that must be achieved by an intruder to compromise a system. Transitions are represented on state-transition diagrams.

c. Anomaly-Based Intrusion Detection System:

Anomaly-based IDSs detect incidents, which show atypical behavior profiles or violate thresholds based on statistical analysis. Examples for this are possible masquerade attacks, which are detected in this way or penetrations of the security control system. Another possible scenarios leakage or denial of service attacks, which are detected by atypical use of system resources. Other problems include malicious use, violations of security constraints, or use of special privileges.[8]Therefore, a statistical anomaly-based IDSs determines normal network activity. It records what sort of bandwidth is generally used, what kind of protocols are used, which ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous (not normal).[8] This could include to compare certain traffic indicator value against a threshold, based on their historically determined standard deviation. The SA-B IDS works with an Network History Database like shown in Fig. 4. This database contains information about previous behavior and events. The System has to consider three main datasets: Statistical information based on historical data, user set thresholds and constraints and finally the data of the current time window which is watched.

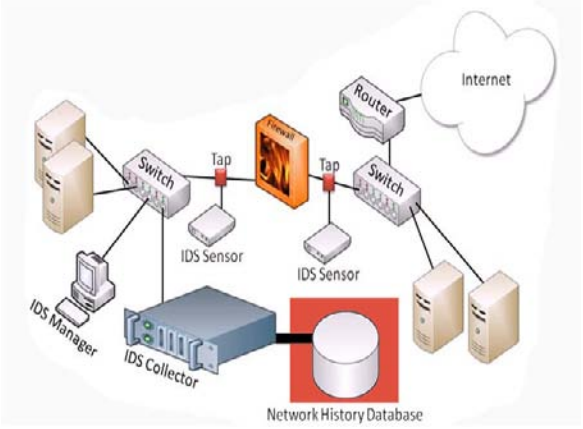

Fig 4: Example for Statistical Anomaly-based IDS

The different type which comes under Anomaly intrusion detection system are as under:

i. Statistical Based Intrusion Detection System.
ii. Expert system Intrusion Detection System.
iii. Neural Networks Intrusion Detection System.
iv. Computer immunology Intrusion Detection System.
v. User Intention Identification System.
vi. Data Mining

i. Statistical Analysis Approach:

This is a frequently used method (for example SECURENET). The user or system behavior (set of attributes) is measured by a number of variables over time. Examples of such variables are: user login, logout, number of files accessed in a period of time, usage of disk space, memory, CPU etc. The frequency of updating can vary from a few minutes to, for example, one month. The system stores mean values for each variable used for detecting exceeds that of a predefined threshold. Yet, this simple approach was unable to match a typical user behavior model. Approaches that relied on matching individual user profiles with aggregated group variables also failed to be efficient. Therefore, a more sophisticated model of user behavior has been developed using short- and long-term user profiles. These profiles are regularly updated to keep up with the changes in user behaviors. Statistical methods are often used in

implementations of normal user behavior profile-based Intrusion Detection Systems.

ii. Neural Networks:

Neural networks use their learning algorithms to learn about the relationship between input and output vectors and to generalize them to extract new input/output relationships. With the neural network approach to intrusion detection, the main purpose is to learn the behavior of actors in the system (e.g., users, daemons). It is known that statistical methods partially equate neural networks. The advantage of using neural networks over statistics resides in having a simple way to express nonlinear relationships between variables, and in learning about relationships automatically. Experiments were carried out with neural network prediction of user behaviors. From the results it has been found that the behavior of UNIX super-users (roots) is predictable (because of very regular functioning of automatic system processes). With few exceptions, behavior of most other users is also predictable. Neural networks are still a computationally intensive technique, and are not widely used in the intrusion detection community.

iii. User intention identification:

This technique (that to our knowledge has only been used in the SECURENET project) models normal behavior of users by the set of high-level tasks they have to perform on the system (in relation to the users' functions). These tasks are taken as series of actions, which in turn are matched to the appropriate audit data. The analyzer keeps a set of tasks that are acceptable for each user. Whenever a mismatch is encountered, an alarm is produced.

iv. Computer immunology:

An analogy with immunology hassled to the development of a technique that constructs a model of normal behavior of UNIX network services, rather than that of individual users. This model consists of short sequences of system calls made by the processes. Attacks that exploit flaws in the application code are very likely to take unusual execution paths. First, a set of reference audit data is collected which represents the appropriate behavior of services, then the knowledge base is added with all the known "good" sequences of system calls. These patterns are then used for continuous monitoring of system calls to check whether the sequence generated is listed in the knowledge base; if not — an alarm is generated. This technique has a potentially very low false alarm rate provided that the knowledge base is fairly complete. Its drawback is the inability to detect errors in the configuration of network services. Whenever an attacker uses legitimate actions on the system to gain unauthorized access, no alarm is generated.

v. Machine learning:

This is an artificial intelligence technique that stores the user-input stream of commands in a Victoria form and is used as a reference of normal user behavior profile. Profiles are then grouped in a library of user commands having certain common characteristics [16].

vi. Data Mining

Generally this refers to a set of techniques that use the process of extracting previously unknown but potentially useful data from large stores of data. Data mining method excels at processing large system logs (audit data). However they are less useful for stream analysis of network traffic. One of the fundamental data mining techniques used in intrusion detection is associated with decision trees [17]. Decision tree models allow one to detect anomalies in large databases. Another technique refers to segmentation, allowing extraction of patterns of unknown attacks [18]. This is done by matching patterns extracted from a simple audit set with those referred to warehoused unknown attacks [18]. A typical data mining technique is associated with finding association rules. It allows one to extract previously unknown knowledge on new attacks [20] or built on normal behavior patterns. Anomaly detection often generates false alarms. With data mining it is easy to correlate data related to alarms with mined audit data, thereby considerably reducing the rate of false alarms [21].

6. INTRUSION PREVENTION SYSTEMS

Intrusion Prevention Systems (IPSs) also known as Intrusion Detection and Prevention Systems (IDPSs),

ARPN Journal of Science and Technology

http://www.ejournalofscience.org

are network security applications, that monitor and change network and system activities if found suspicious. The main functions of IPSs are, as explained to identify malicious activity, log information about it, and attempt to block or stop and report that activity [10]. Since they are not in the focus of this report, it is necessary to note here, that they are important parts of network security and strongly related to intrusion detection. IPSs can be considered extensions of IDSs. The main differences that should be figured out between them are, that IDPs are placed in-line and are able to actively prevent or block intrusions that are detected. [11][12] To be a little bit more precise it can be declared, that IPSs can take such actions as sending an alarm, dropping the malicious packets, resetting the connection or blocking the traffic from the offending IP address. [13] This might also include other actions like changing or reconfiguring firewall rules. Additional tasks of an IPS are correcting "Cyclic Redundancy Check (CRC) errors, un-fragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options" [10] [13]. For that they are using several response techniques, which involve the IDPS stopping the attack itself.

7. CLASSIFICATIONS OF IDPS

Intrusion Prevention Systems can be classified into four different types like shown in table 1 below [11][15]

Table 1: classification of IDPS

Name	Explanation
Network Based Intrusion Prevention System (NIPS)	In this kind of IDPS, it analysis the traffic of entire network by analyzing protocol activities and take appropriate actions.
Wireless Intrusion Prevention System (WIPS)	In this kind of IDPS, it analysis the traffic of Wireless network by analyzing protocol activities and take appropriate actions.
Network Behavior Analysis (NBA)	This type of IDPS examines traffic to identify threats that generate unusual traffic flow, such as DDOS attack, malware and Policy Violation.
Host Based Intrusion Prevention (HIPS)	This type of IDPS monitors single host for suspicious activity by analyzing events occurring within that host

8. FEATURED ANALYSIS OF IDS AND IDPS

This section summarizes pertinent information, providing users a brief description of available IDS and IDPS tools. Here in this paper, we are not going to evaluate the effectiveness of these tools but will analyze them on certain parameters. The written descriptions are drawn from vendors' informationsuch as brochures and Web sites, and are intended only to highlight the capabilities or features of each product. As such there are no guide lines for choosing best IDPS, after understanding the parameter; it will be easy for us to put forth some frame work for choosing guidelines.

ARPN Journal of Science and Technology

http://www.ejournalofscience.org

Table 2: List of parameters with explanation for comparative analysis

Type	The type of tool, or category in which this tool belongs, e.g., "Web Application Scanning"
Operating System	The operating system(s) on which the tool runs. If the tool is an appliance, this field will contain a "not applicable" symbol (N/A) because the operating system is embedded in the tool.
Hardware	The third-party hardware platform(s) on which the tool runs, plus any significant additional hardware requirements, such as minimum amount of random-access memory or free disk space. If the tool is an appliance, this field will contain a "not applicable "symbol (N/A) because the hardware is incorporated into the tool.
License	The type of license under which the tool is distributed, e.g., Commercial, Freeware, GNU Public License
NIAP Validated	An indication of whether the product has received validation by the National Information Assurance Partnership (NIAP) under the Common Criteria, Federal Information Processing Standard 140, or another certification standard for which NIAP performs validations. If no such validation has been performed, this field will be blank or put N/A
Common Criteria .	If the tool has received a Common Criteria certification, the Evaluation Assurance Level and date of that certification. If no such certification has-been performed, this field will be blanker N/A
Developer	The individual or organization responsible for creating and/or distributing the tool
URL	The Uniform Resource Locator (URL) of the Webpage from which the tool can be obtained (downloaded or purchased), or in some cases, the Web page at which the supplier can be notified withal request to obtain the tool

The below table shows the parameterized comparative analysis of different ID and IDPS system, Based on the parameters chosen in table 2, we will compare different IDPS tools .The analysis are as under:

Name	Type	Platform	Hardware Required	License	NIAP Validated	Common Criteria	Based On
AIDE—Advanced Intrusion Detection Environment	HIDS	Linux 2.6, Solaris 10/ Open Solaris, FreeBSD2.2.8,3.4,Unixware 7.0.1,BSDi 4.1, OpenBSD2.6,3.0, AIX 4.2, TRU64 4.0x, HP-UX 11i, Cyg win	Required	Open Source	N/A	N/A	Rule Based
CSP Alert-Plus	HIDS	Windows	Required	Commercial	N/A	N/A	Rule Based
eEye® Retina	HIDS	Windows	Required	Commercial	True	EAL2	Rule Based
eEyeSecureIIS Web Server Protection	HIDS	Windows	Required	Commercial	N/A	N/A	Rule Based
GFI Events Manager	HIDS	Windows	• Processor: 2.5 Gigahertz (GHz) or	Commercial	N/A	N/A	Rule Based

			higher • Random access memory (RAM): 1024 Megabyte (MB) • Hard disk: 2 Gigabyte (GB) of available space				
Hewlett Packard®-Unix (HP-UX®) 11i Host Intrusion Detection System (HIDS)	HIDS	Unix	Required	Freeware	N/A	N/A	Rule Based
IBM® Real Secure® Server Sensor	HIDS	Windows, Sun Solaris, IBM AIX, HP-UX, VMware® ESX	Required	Commercial	N/A	N/A	Rule Based
McAfee® Host Intrusion Prevention	HIDS	Linux, OS/400 and i5/OS V5R2 or later, Unix, Windows, OS/390	• Dual processor dual-core (AMD®/Intel® Recommended). Quad processors Recommended for large environments. • 2 GB RAM (minimum); 4 GB RAM (recommended) • Windows Server 2003 • Microsoft SQL Server 2005 SP2 for the Database and Reporting Servers. Enterprise Edition is recommended for Reporting Server. Reporting Server also requires Microsoft SQL Server 2005 Analysis Services with Service Pack 2, Microsoft SQL Server 2005 Integration Services (SSIS) • IIS 5.0, IE 6.0, Office 2003 Web Components and more are required for	Commercial	True	EAL2	Rule Based

ARPN Journal of Science and Technology

			Trend Analysis reports.				
OSSEC HIDS	HIDS	FreeBSD, Linux, Open BSD, Solaris, AIX, HP-UX, Mac OSX, VMW are ESX, Windows	Required	Open Source	N/A	N/A	Rule Based
Samhain	HIDS	Cygwin/Windows, Linux, Unix	Required	Open Source	N/A	N/A	Rule Based
Tripwire® Enterprise	HIDS	Linux, Unix, Windows	Windows and Linux • 3.0 GHz x86 processor or compatible • 2 GB RAM • 2 SATA or SCSI hard drives • 3.2 GB free disk space • 4 GB Data storage space • 256-color display 900 MHz Ultras ARC III processor • 2 GB RAM • 2 SATA or SCSI hard drives • 3.2 GB free disk space • 4 GB Data storage space • X-Windows capable display • 256-color display	Commercial	True	EAL3	audit assessment
Arbor Networks Peak flow® X	NIDS	N/A	N/A	Commercial	True	EAL3	Behavior Based
Arc Sight®	NIDS	N/A	N/A	Commercial	True	EAL3	Anomaly Based
Bro	NIDS	Unix	Processor • 1 GHz CPU (for 100 BT Ethernet with average packet rate <= 5,000 packets/second) • 2 GHz CPU (for 1000 BT Ethernet with average packet rate <= 10,000 packets/second) • 3 GHz CPU (for 1000 BT Ethernet with	Open Source	N/A	N/A	Pattern Based

			average packet rate <= 20,000 packets/second) • 4 GHz CPU (for 1000 BT Ethernet with average packet rate <= 50,000 packets/second) (Note: these are very rough estimates, and much depends on the types of traffic on your network [e.g., HTTP, FTP, email, etc.].) Operating System • FreeBSD 4.10 (http://www.freebsd.org/) Bro works with Linux and Solaris as well, but the performance is best under FreeBSD. In particular, there are some performance issues with packet capture under Linux. Memory • 1 GB RAM is the minimum needed, but 2–3 GB is recommended Hard disk • 10 G Byte minimum, 50 G Byte or more for log files recommended Network Interfaces • 3 interfaces are required: 2 for packet capture (1 for each direction), and 1 for host management. Capture interfaces should be identical.				
Check Point IPS Software Blade	NIDS	N/A	N/A	Commercial	N/A	N/A	Anomaly Based
Cisco	NIDS	N/A	N/A	Comme	True	EAL2	Rule

Intrusion Detection System Appliance IDS-4200				rcial			Based
Cisco Security Agent	NIDS	N/A	N/A	Commercial	True	EAL2	signature-based
Intrusion Secure Net IDS/IPS	NIDS	N/A	N/A	Commercial	True	EAL2	Deep-packet analysis
Hardware Defense Pro®	NIDS	N/A	N/A	Commercial	N/A	N/A	behavioral-based
Snort®	NIDS	Linux	N/A	Open Source	False	N/A	signature, protocol, and anomaly-based inspection methods.
Source fire® Intrusion Prevention System	NIDS	N/A	N/A	Commercial	True	EAL2	combination of vulnerability and anomaly based inspection methods
Kismet	Wireless	Linux	N/A	Open Source			passively collecting packets and detecting standard named networks

9. CONCLUSION AND FUTURE SCOPE

Intrusion detection is still a fledging field of research. This field is still in infancy mode. Here in this paper, we have discussed different groups of intrusion detection and prevention system to support the security of an organization against threats and attacks. Accordingly we have purpose a classification scheme of these intrusion detection and prevention systems, so that we will get a better idea about each and every class of intrusion detection and preventions system also we have made a parameterized comparative analysis for some IDPS tool.

The main future scope behind this survey pattern is that to put forth some prime concepts in for research community i.e. guidelines for choosing intrusion detection and prevention system for its organization. In upcoming research work, we will try to highlight prime design attributes (via guidelines) for choosing a particular type of Intrusion detection and prevention system for your organization.

REFERENCES

[1] J.P.Anderson. Computer Security Threat Monitoring and Surveillance. Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980.

[2] J MJ. McHugh, A. Christie, J. Allen, “Defending Yourself: The Role of Intrusion Detection Systems,” In IEEE Software September/October 2000 Focus Malicious IT, pages 42 – 51.

[3] SANS Institute Info Sec Reading Room” Understanding Intrusion detection systems”

[4] E. Amoroso and R. Kwapniewski, “A Selection Criteria for Intrusion Detection Systems,” Proc. 14th Ann. Computer Security Applications Conf., IEEE Computer Soc. Press, Los Alamitos, Calif., 1998, pp. 280–288.

[5] Andreas Fuchsberger,”Intrusion Detection Systems and Intrusion Prevention Systems “Information Security Technical Report Elsevier (2005) 10, 134-139.

[6] OSSEC (Observing System Science Executive Council) OSS. Homepage of ossec, 2011. http://www.ossec.net/. Online; accessed: 28.4.2012

[7] Peter Scarf one, Karen; Mell. Guide to intrusion detection and prevention systems (idps). Computer Security Resource Center (National Institute of Standards and Technology), January 2010.

[8] Joseph Migga Kizza. Computer Network Security. Springer, 2005, Part III, 315-346. DOI: 10.1007/0-387-25228-2 12.

[9] Vermanitin.; Mattord. Principles of Information Security. Course Technology, 2008. ISBN 9781423901778.

[10] Peter Scarf one, Karen; Mell. Guide to intrusion detection and prevention systems (idps).Computer Security Resource Center (National Institute of Standards and Technology), January 2010.

[11] Robert C. Newman. Computer Security: Protecting Digital Resources. Jones and Bartlett Learning. 2009. ISBN 9780763759940.

[12] Michael E. Whitman; Herbert J. Mattord. Principles of Information Security. Engage Learning EMEA, 2009. ISBN 9781423901778.

[13] Tim Boyles. CCNA Security Study Guide: Exam 640-553. John Wiley and Sons, 2010. ISBN 9780470527672.

[14] Harold F. Tipton; Micki Krause. Information Security Management Handbook.CRC Press, 2007. ISBN 9781420013580.

[15] John R. Vacca. Managing Information Security. Syngress, 2010. ISBN 9781597495332.

[16] Marin J., Ragsdale D, Surdu J: A Hybrid Approach to the Profile Creation and Intrusion Detection. Proceedings of the DARPA Information Survivability Conference and Exposition –DISCEX 2001, June 2001, http://www.itoc.usma.edu/Documents/Hybrid_DISCEX_AcceptedCopy.pdf.

[17] Fan W., Miller M., Stolfo S., Lee W., Chan P.: Using Artificial Anomalies to Detect Unknown and Known Network Intrusions. In Proceedings of the First IEEE International Conference on Data Mining, San Jose, CA, November 2001, http://www.cc.gatech.edu/~wenke/papers/artificial_anomalies.ps.

[18] Lee W., Stolfo S, Mok K.: Adaptive Intrusion Detection: a Data Mining Approach. Artificial Intelligence Review, 14(6), December 2000, pp. 533-567, http://www.cc.gatech.edu/~wenke/papers/ai_review.ps.

[19] Lee W. i inni: A data mining and CIDF based approach for detecting novel and distributed intrusions. Recent Advances in Intrusion Detection, Third International Workshop, RAID 2000, Toulouse, France, October 2-4, 2000, Proceedings.

ARPN Journal of Science and Technology

Lecture Notes in Computer Science 1907 Springer, 2000, pp. 49-65. http://www.cc.gatech.edu/~wenke/papers/lee_raid_00.ps

[20] Bass T.: Intrusion Detection Systems Multisensor Data Fusion: Creating Cyberspace Situational Awareness. Communication of the ACM, Vol. 43, Number 1, January 2000, pp. 99-105, http://www.silkroad.com/papers/acm.fusion.ids.ps.

[21] Manganaris S., Christensen M., Zerkle D., Hermiz K.: A data mining analysis of RTID alarms. Computer Networks, 34, 2000, pp. 571-577.

[22] Yogesh Kumar and Swati Dhawan,A REVIEW ON INFORMATION FLOW IN INTRUSION DETECTION SYSTEM, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 1, January 2012ISSN (Online): 2230-7893 p 91-96