Intrusion Detection & Prevention Systems - Sourcefire Snort

Rajesh Vuppala, Mohammed Farik

Abstract: Information security is a challenging issue for all business organizations today amidst increasing cyber threats. While there are many alternative intrusion detection & prevention systems available to choose from, selecting the best solution to implement to detect & prevent cyber-attacks is a difficult task. The best solution is of the one that gets the best reviews, and suits the organization's needs & budget. In this review paper, we summarize various classes of intrusion detection and prevention systems, compare features of alternative solutions and make recommendation for implementation of one as the best solution for business organization in Fiji.

Index Terms: Information Security, Cyber threats, Cyber-attacks, Viruses, IDPS

1 Introduction

Risks and chances of malicious and dedicated attacks towards the networks are very high because of limit possibilities and opportunities in the field of intrusion detection and prevention system. It is very important to design security mechanisms that prevent unauthorized access to system resources and confidential data of the company. However at present the complete control of security breaches looks to be impossible. Somehow we can try to detect these attempts and actions may be take to mitigate them. This is called as Intrusion detection prevention. I will provide a overview on IDPS in this paper. According Prof M A Peer, 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 [7]:

- Information Availability
- Information Usage
- Render a system unrealistic or unusable

Intrusion detection provides the following:

- Monitoring and analysis of user and system activity
- Checking and comparing vulnerabilities
- Availability of critical data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal behaviour analysis
- Operating system analysis and comparison with stable state.

2 IDPS (IDS & IPS)

Intrusion Detection Systems (IDS) passively monitor traffic on a network and perform more advanced checks, including protocol and content inspection, to determine indications of possible attacks [8].

- *Rajesh Vuppala is an IT Manager and is currently pursuing master's degree program in Information Technology in the School of Science and Technology at The University of Fiji. Email: vuppalaraj@gmail.com*
- *Mohammed Farik is a Lecturer in Information Technology in the School of Science and Technology at The University of Fiji. Email: mohammedf@unifiji.ac.fj*

Intrusion Prevention Systems (IPS) combines the functionality of IDS and firewalls, performing in-depth inspection and using this information to block possible attacks. Thus together known as Intrusion Detection and Prevention Systems (IDPs) which is a passive system that scans the traffic and block reports on threats, actively analyzing and taking an automated action on all traffic flows that enter the network. These actions specifically include [8]:

- Sending an alarm to the administrator.
- Dropping the malicious packets.
- Blocking traffic from the source address.
- Resetting the connections.

3 Issues and Challenges in IDS

As demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap. Today intrusion detection system is still in infancy and need lot of research work to be done to make the intrusion detection even more successful. There are a huge number of issues and challenges in current intrusion detection system which needs the immediate and strong research attention. In this paper, I have identified some important issues and challenges which need to be addressed by research communities. The issues and challenges are:

- Deficiency or incomplete Data set
- Detection Algorithms
- Integration of multiple formats of data
- Platform dependencies
- Poor Design
- Testing/Evaluation of IDS

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. Few examples of what an Intrusion Detection Systems are capable of, every network environment varies and each system needs to be tailored to meet enterprise environment needs.

Advantages:

- Consummate for infrastructure
- Tracing of user activity
- Checking on alterations of data
- Searching for latest attacks

- Detecting system is under attack
- Find out configuration errors
- Guiding administrator to make policies
- Making security management

Disadvantages:

- No compensate for a weak identification and authentication mechanisms
- No investigation for attacks without human
- No compensate for weaknesses in network protocols
- No compensate for quality or integrity of information
- No analysis on busy network
- No dealing with problems in packet-level attacks
- No dealing with some of the modern network hardware and features

4 CLASSIFICATION OF IDS

They are 2 patters to classify IDS systems. 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. The ID system has been classified in three groups.

- Host Based Intrusion Detection System
- Network Based Intrusion Detection System
- Hybrid Based Intrusion Detection System

4.1 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. In fact there are also some application-based IDS which a part of this category. One good example is OSSEC which is open source IDS [7].

4.2 Network Intrusion Detection Systems

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

4.3 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. In the second classification scheme, 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 divided into three groups:

- Misuse Based Intrusion Detection System
- Signature Based Intrusion Detection System
- Anomaly Based Intrusion Detection System

4.4 Misuse 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

4.5 Signature-Based IDS

A signature based IDS monitor 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. To reduce further lag, security software using such signatures should be updated as frequently as feasible. The different types which come under this category are:

- Expert system
- Signature Analysis
- Petri Nets
- State Transition

4.6 Anomaly-Based Intrusion Detection System:

Anomaly-based IDSs detect incidents, which show atypical behaviour profiles or violate thresholds based on statistical analysis. Examples for this are possible masquerade attacks, which are detected in this 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. Therefore, statistical anomaly-based IDSs determine 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). This could include comparing certain traffic indicator value against a threshold, based on their historically determined standard deviation. Table 1 shows different type of IDPS classifications and also explanation about that system.

TABLE 1

DIFFERENT TYPES OF IDPS CLASSIFICATIONS

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.

Table 2 explains about list of parameters and explanation about that parameter how it works for the IDPS classification analysis.

TABLE 2

LIST OF PARAMETERS WITH EXPLANATION FOR COMPARATIVE ANALYSIS

Parameter	Description
Name	The name of the intrusion detection system
Type	The type of tool, or category in which this tool belongs, e.g.Web Application Scanning
Platform	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.
License	The type of license under which the tool is distributed, e.g., Commercial, Freeware, GNU Public License
Based on	The technology on which IDS is based on i.e, Rule based , pattern matching etc.
Suitability	On what kind of networks or systems it will be best implemented.
Attacks Detected	What kind of attacks is detected by the system?

Table 3 shows some examples of IDPS systems and their type and suitability and functions of those IDPS systems. For eg sourcefire is SNORT and network based intrusion and detection system and it suitable for large and small organizations

TABLE 3

COMPARATIVE ANALYSIS OF DIFFERENT INTRUSION DETECTION TECHNIQUES AVAILABLE ON SOME SELECTED PARAMETERS

Name	Type	Platform	License	Based on	Suitability	Attacks Detected
AIDE	HIDS	Linux	Open Source	Rule Based	Checking integrity of file & directory, mainly useful for security purposes and can be used in small, medium, large scale organizations	
CSP Alert-Plus (Checker)	HIDS	Windows	Commercial	Rule Based	Checking integrity of file & directory. Mainly useful for security purpose and can be used in large scale organizations	intrusion, file and integrity checker
Sourcefire-Snort (Scans)	NIDS	Linux	Open Source	Rule Based	Suitable for checking intrusion or attacks for large or small organizations	DOS & CGI Attacks, Intrusion Attacks, port Scans, SMB probes layer3 and above attacks.
Bro (inspection)	NIDS	LINUX	Open source	Pattern matching	Suitable for checking intrusion in the system for known attacks	Signature inspection method.
AAFID (filling)	NIDS	Windows NT, Linux,	Open source	Statistical based	Suitable for checking intrusion or attacks for large or small organizations	DOS, File System Attacks
DTK (Scanning)	HISD	Free BSD, Open BSD Linux, MAC OS	Open source	Statistical based	Works as a deception to attackers and is suitable in Linux and Unix based systems. It suits in single user environment.	Resources Exhaust, Port Scanning
ImSafe	NIDS	Free BSD, Open BSD Linux, MAC OS	Open source	Statistical based	Suitable for buffer overflow attacks and react in real time, for monitoring sequences of system calls, in Linux and Unix based platforms. It suits in small scale organization.	Buffer Overflow Attack
Host -S entry	HIDS	Linux, Free BSD	Open Source	Statistical based	Suitable for detecting login anomaly detection, trace suspicious user activity, monitors interactive login sessions, and reports or reacts in real time in Linux. It suits in environment where authentication and authorization is main concern.	Unknown user Logins, Suspicious User Activity, Suspicious login Domain

5 CONCLUSION

This paper explained different groups of intrusion detection and prevention system to support the security of an organization against threats and attacks. It also explained about classification scheme of these intrusion detection and prevention systems, to get a better idea about each and every class of intrusion detection and preventions system. Moreover, we made a parameterized comparative analysis for some IDPS tool. We recommend Sourcefire's IPS the best option for my organization as it having highest ratings for intrusion detection and prevention in the market. It can be noted from many articles and review papers that the product works accurately and effectively, with solid alerting and reporting features. I also noticed about cost that Sourcefire IPS gives a

good return for the money we spend. This system also won gold winner in 2011 [9]. Sourcefire IPS has its roots in Snort, an open source intrusion detection and prevention tool created by the founders of Sourcefire. The product itself is not open source, but it can receive alerts from Snort. Sourcefire IPS sensors operate in either inline or passive mode. Sourcefire IPS provides intrusion detection and blocking, dashboard and reporting, policy management and Snort rule editing. It is backed by Sourcefire's Vulnerability Research Team (VRT), which aims to proactively discover and respond to various attacks and intrusion activities. The VRT uses this information to populate the official Snort rules. In 2013 Juniper Network IDP series won gold winner award [10]. There are some others IDP series won, silver and brown awards every year. Sourcefire IPS is one component in Sourcefire's 3D System, an integrated suite that also includes optional endpoint protection, SSL inspection and antimalware. With all these features we recommend Sourcefire is the best option for our organization and also it suits for our server which we are using in LINUX environment.

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" 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.

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

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

[6] Classification for IDPS at ARPN Journal of Science and Technology::Intrusion Detection and Prevention System: classification and Quick Review - vol2no7_17.pdf

[7] Comparative analysis at : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.4979&rep=rep1&type=pdf

[8] Best IDS system : http://searchsecurity.techtarget.com/guide/Best-Intrusion-Detection-and-Prevention-Products-2011

[9] Best IPS system: http://searchsecurity.techtarget.com/feature/Best-of-intrusion-detection-and-prevention-2013

[10] Basic information about IDPS at : https://en.wikipedia.org/wiki/Intrusion_detection_system

[11] Top free network based IDPS systems at: https://www.upguard.com/articles/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise