International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM: A COMPARATIVE STUDY

Nilotpal Chakraborty

School of Future Studies & Planning, Devi Ahilya University, Indore, India

ABSTRACT : *Intrusions in computing environment are a very common undesired malicious activity that is going on since the inception of computing resources. A number of security measures have taken place for the last three decades, but as Technology has grown up, so as the security threats. With the whole world depending on computers, being directly or indirectly, it is a very important issue to prevent the malicious activities and threats that can hamper the computing infrastructures. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are the standard measures to secure computing resources mostly in a network. They are deployed in a network for assuring an intrusion free computing environment. In this paper, we shall discuss the two technologies in details, their functionality, their performances and their effectiveness to stop the malicious activity over a computer network.*

Keywords- *IDS, IPS, Intrusion, Intrusion Detection, Intrusion Prevention, Firewall, Security*

1. INTRODUCTION

An intrusion can be termed as an unauthorized entry to another's property or area, but in terms of computer science, it is the activities to compromise the basic computer network security goals viz. confidentiality, integrity, and privacy. Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents of threats and violations of computer security practices, acceptable use policies or standard security policies.

Intrusion Detection System (IDS) is a software or hardware component that automates the intrusion detection process. It is designed to monitor the events occurring in a computer system and network and responds to events with signs of possible incidents of violations of security policies.

Intrusion Prevention System (IPS), on the other hand, is the technology of both detecting of intrusion or threat activities and taking preventive actions to seize them. It combines the knowledge of IDS in an automated manner.

2. HISTORY & DEVELOPMENT

Securing data has been a prominent issue ever since the inception of computers and their enormous applications. The studies of Intrusion detection has been active field of research for about more than three decades now. It started with the publication of John Anderson's Computer Security threat monitoring and surveillance in 1980, which is one of the earliest research papers on this field. Dorothy Denning's seminal paper, "An Intrusion Detection Model" published in 1987 provided a methodological framework that inspired a number of researchers. After that, for the past two decades, despite of substantial research and huge commercial investments, Intrusion Detection technology is immature and ineffective.

In the early days of computers, hackers rarely used automated tools to break into systems. They were intelligent with high level of expertise and followed their own methodology to perform such actions. The recent scenario is quite different now. A wide number of intrusion tools and applications are available now that can be used to exploit scripts that capitalize on widely known vulnerabilities. Figure-1 depicts the relationship between the relative sophistication of attackers and attackers from 1980 to present days.

Before the development of modern IDS, intrusion detection consisted of a manual search for anomalies. Due to the availability of adequate processing speed it now became possible not only to look for attack patterns after the event had occurred, but also to monitor in ‘‘real-time’’ and trigger alerts if intrusions were detected.

Due to the financial losses from computer downtime, loss of image, or even confidential data being affected, in recent years the demand for not only being alerted in the event of an attack, but also to prevent the attack altogether has become an absolute necessity. Especially with the introduction of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, the market demands have grown stronger for Intrusion Prevention Systems (IPS) rather than mere intrusion detection.

3. INTRUSION DETECTION SYSTEM

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An Intrusion Detection System (IDS) can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. The key functionalities of IDS can be pointed out as follows—

- Recording information related to observed events.
- Notifying administrators of important observed events.
- Producing reports.

4. INTRUSION DETECTION METHODOLOGY

Several types of intrusion detection methodologies are available due to the variance of network configuration. Each of them is having their own advantages and disadvantages in detection, configuration and cost.

4.1 SINATURE BASED DETECTION

A signature is a pattern that corresponds to a known threat. In signature based detection, observed events are compared against the pre-defined signatures in order to identify possible unwanted traffic. This type of detection technique is very fast and easy to configure.

Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats. An attacker can slightly modify an attack to render it undetectable by a signature based IDS. Still, IDS using signature based methodology, though having limited capability, can be very accurate.

4.2 ANOMALY BASED DETECTION

Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDS using anomaly-based detection has *profiles* that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time.

The major benefit of Anomaly based detection technique is that they can be very useful for detecting unwanted traffic that is not specifically known. For instance, anomaly-based IDS will detect that an Internet protocol (IP) packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.

4.2 STATEFUL PROTOCOL ANALYSIS

Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Stateful protocol inspection is similar to anomaly based detection, but it can also analyze traffic at the network and transport layer and vender-specific traffic at the application layer, which anomaly-based detection cannot do.

5. TYPES OF INTRUSION DETECTION SYSTEM

There are many types of IDS technologies based on the type of events that they monitor and the ways in which they are deployed. Here in this document we discuss the following four types—

- Network Based IDS
- Wireless IDS
- Network Behavior Anomaly Detection
- Host Based IDS

5.1 NETWORK BASED IDS

Network based IDS (NIDS) monitors' network traffic for a particular network segment and analyzes the network and application protocol activity to identify suspicious activity. It is most commonly deployed at a boundary between networks such as in routers, firewalls, virtual private networks etc.

The main disadvantage of this type of IDS is that it has a single point of failure. Moreover, it is weak against DoS attacks. It monitors the whole network and deployed at the boundary of the network. But it is not suitable for securing each of the hosts within the network. If an intruder can bypass it, all the systems within the network would be in trouble.

Figure-2 depicts the functioning of NIDS.

5.2 WIRELESS IDS

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyze network traffic. However, it will also analyze wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security. Many previous NIDS tools will include enhancements to support wireless traffic analysis.

5.3 NETWORK BEHAVIOR ANOMALY DETECTION

Network behavior anomaly detection (NBAD) views traffic on network segments to determine if anomalies exist in the amount or type of traffic. Segments that usually see very little traffic or segments that see only a particular type of traffic may transform the amount or type of traffic if an unwanted event occurs. NBAD requires several sensors to create a good snapshot of a network and requires benchmarking and base lining to determine the nominal amount of a segment's traffic.

5.3 HOST BASED IDS

In Host-based IDS (HIDS) technology, software agents are installed on each of the computer hosts of the network to monitor the events occurring within that host only. HIDS analyze network traffic and system-specific settings such as software calls, local security policy, local log audits, and more. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. HIDS are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

HIDS overcome the problems incurred in Network based IDS technology of securing individual hosts in the network. But they cause a substantial overhead for the hosts running them.

Figure-3 depicts the functioning of HIDS.

6. INTRUSION PREVENTION SYSTEM

Intrusion prevention system (IPS) is the process of both detecting intrusion activities or threats and managing responsive actions on those detected intrusions and threats throughout the network. IPS are monitoring real time packet traffic with malicious activities or which match specific profiles and will trigger the generation of alerts and it can drop, block that traffic in real time pass through in network. The mainly IPS counter measures is to stop an attack in progress.

IPS can be termed as the extension of IDS with exercises of access control to protect computers from exploitation. IPS is an intelligent device that is capable of not only detecting malicious activities, but also to take preventive actions to secure the host or the network.

In simple terms, IDS may be perfectly suited for network attack monitoring and for alerting administrators of emerging threats. But its speed, performance and passive limitations have opened the door for IPS to challenge it as the proactive defense weapon of choice.

The key functionalities performed by an IPS are as follows—

- IPS detects and takes preventive actions against malicious attacks
- IPS stops the attack itself
- IPS changes the security environment
- IPS changes the attack's contents

7. IDS vs. IPS

Deciding between intrusion detection systems (IDS) and intrusion prevention systems (IPS) is a particularly challenging and time consuming task for most security pros. Both systems provide similar benefits and have markets occupied by the same vendors.

An IPS is best compared to a firewall. Firewalls and IPS are control devices. They sit in line between two networks and control the traffic going through them. But the basic difference between Firewall and IPS is the way they handle network traffic. Whereas a Firewall denies all the requests that do not match its safety definition, IPS accepts all the requests except those whose contents seem to be malicious and threatening to the system.

On the other hand, if an IPS is a control tool, then IDS is a visibility tool. Intrusion Detection Systems sit off to the side of the network, monitoring traffic at many different points, and provide visibility into the security posture of the network. A good analogy is to compare IDS with a protocol analyzer. A protocol analyzer is a tool that a network engineer uses to look deep into the network and see what is happening, in sometimes excruciating detail. An ID is a "protocol analyzer" for the security engineer. The IDS looks deep into the network and sees what is happening from the security point of view.

From their definitions itself, we can infer that IPS starts functioning at the point where IDS stops. IDS can only detect an error, but IPS, along with detecting it, can also rectify the incurred problem.

Figure-4 shows the combined functioning of IDS and IPS.

8. FIGURES

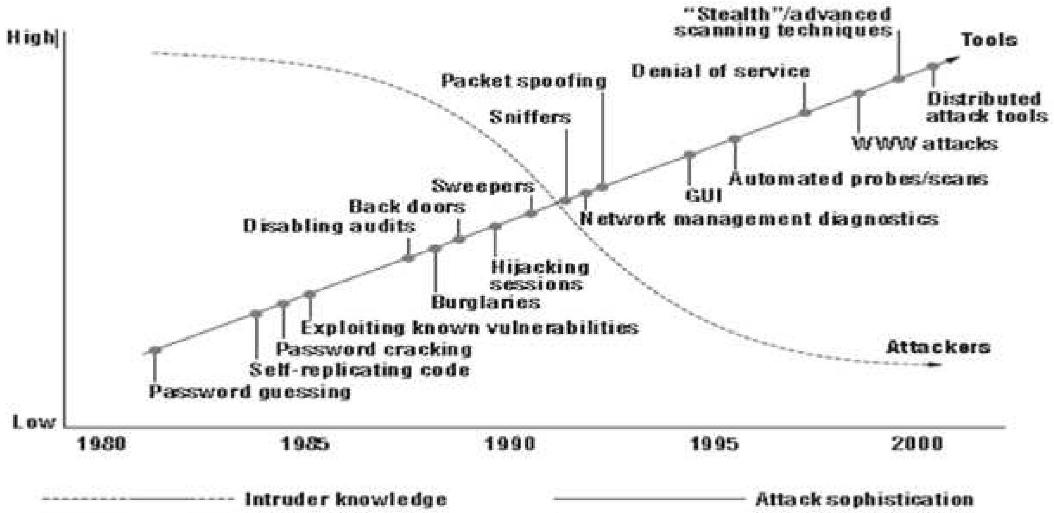

Figure-1: Attack sophistication vs. Intruder technical knowledge

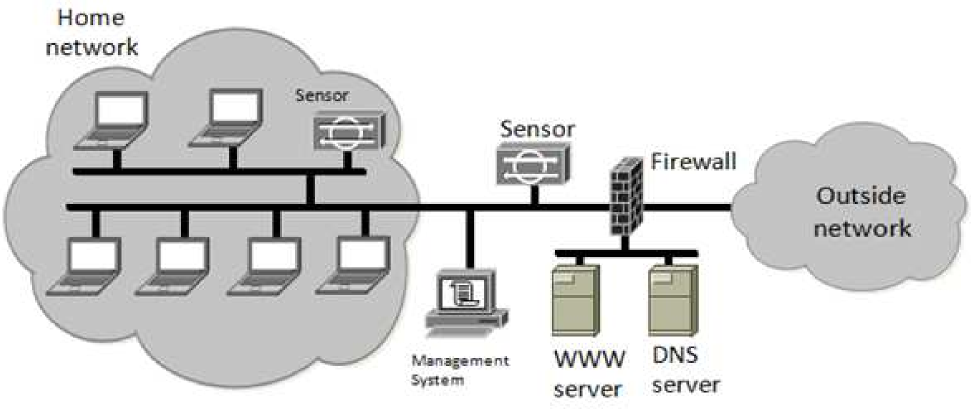

Figure-2: Network based Intrusion detection System (NIDS)

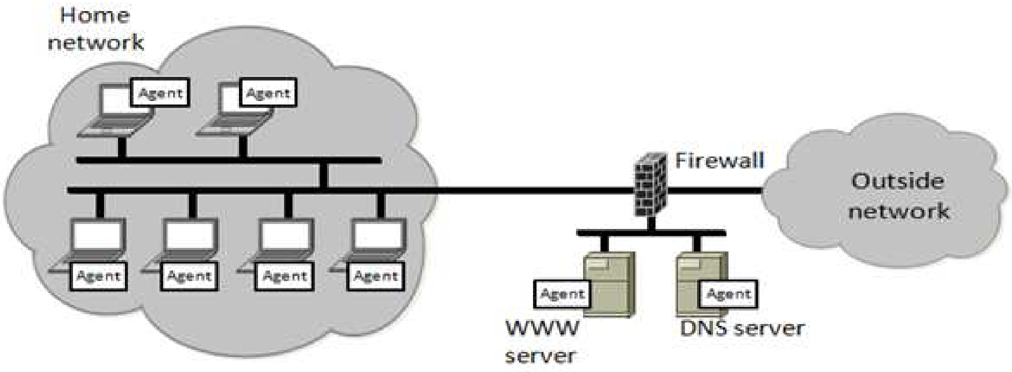

Figure- 3: Host based Intrusion detection System (HIDS)

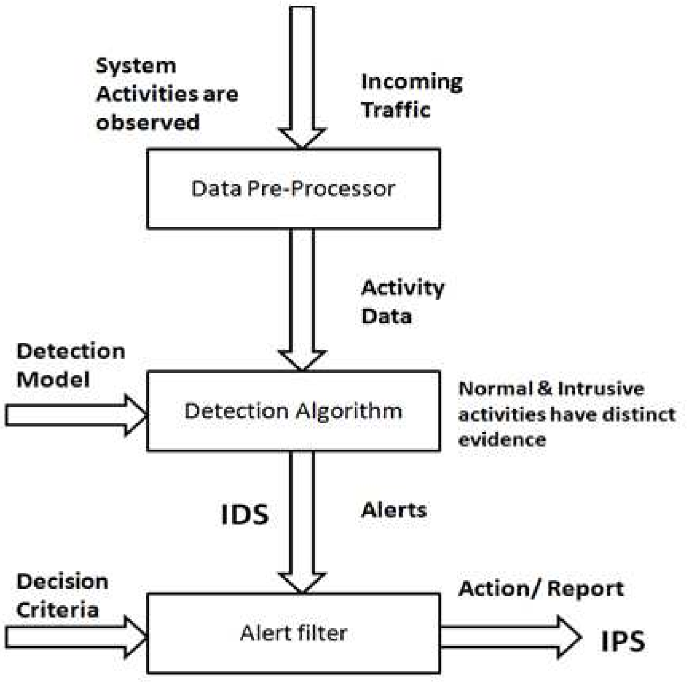

Figure-4: Functioning of IDS & IPS in network security

9. CONCLUSION

There are many technologies in the market today to help companies fight the inevitable network and system attack. Having IPS and IDS technologies are only two of many resources that can be deployed to increase visibility and control within a corporate computing environment. IDS and IPS are to provide a foundation of technology that meets the requirement of tracking, identifying network attacks to which detect through logs of IDS systems and prevent an action through IPS systems. If the host is with critical systems, confidential data and strict compliance regulations, then it's a great to use IDS, IPS or both in network environments.

10. ACKNOWLEDGEMENT

It is my greatest pleasure to present sincere thanks to Dr. V. B. Gupta, Head, School of Future Studies & Planning, Devi Ahilya University, Indore and Dr. D. S. Bhilare, Head, IT Center, Devi Ahilya University, Indore, for their constant support and encouragement for my academics and while writing this paper. I would like to present my sincere thanks to Mr. Alok Malviya and Mr. Nandkishore Bhuwade of IT Centre, Devi Ahilya University, Indore, for being my mentors. I am also very thankful to all of my friends and my family members for their valuable presence in my life.

REFERENCES

[1] J.P. Anderson, *Computer Security Threat Monitoring and Surveillance*, tech. report; James P. Anderson Co., Fort Washington, Pa., 1980.

[2] D.E. Denning, "An Intrusion Detection Model," *IEEE Trans. Software Eng.*, Vol. SE- 13, No. 2, Feb. 1987, pp. 222–232.

[3] 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] J. Allen et al., *State of the Practice of Intrusion Detection Technologies*, Tech Report CMU/ SEI-99-TR-028, Carnegie Mellon Univ., Software Engineering Inst., Pittsburgh, 2000

[5] Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth, SANS Institute, 2004.

[6] Karen Scarfone , Peter Mell, " Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology,2007.

[7] Debar, H., An Introduction to Intrusion Detection Systems, IBM Research, Zurich Research Laboratory

[8] Kent, Karen & Warnock, Matthew (2004). *Intrusion Detection Tools Report, 4th Edition.* Herndon, VA: Information Assurance Technology Analysis Center (IATAC).

[9] Jennifer Jabbusch , "IDS vs. IPS: How to know when you need the technology", 22 November 2010

[10] Pete Lindstrom, "Intrusion prevention systems (IPS): Next generation firewalls", A Spire Research Report – March 2004 by, Spire Security

[11]Paul Helman, Gunar Liepins, and Wynette Richards; Foundations of intrusion detection, in Proceedings of the Fifth Computer Security Foundations Workshop, Franconic, NH, June 1992

[12] Teresa Lunt and R. Jagannathan; A prototype real-time intrusion-detection expert system; in Proceedings of the 1988 Symposium on Security and Privacy, Oakland, CA, April 1988

[13] Jan Vykopal, "Security Analysis of a Computer Network", Masaryk University Brno, master thesis, 2008.

[14] B. Mukherjee, L.T. Heberlein, and K.N. Levitt, "Network Intrusion Detection," *IEEE Network*, Vol.8, No. 3, May-June 1994

[15] Charlie Kaufman, Radia Perlmon and Mike Speciner; Network Security; Private Communication in a Public World, 2nd Edition, Prentice Hall of India

[16] William Stallings, Cryptography and Network Security: Principles and Practices, Pearson Education, 4th Edition, 2011.

[17]https://supportforums.cisco.com/community/netpro/security/intrusion-prevention

[18]http://www.cisco.com/en/US/products/ps5729/Products_Sub_Category_Home.html

[19]http://www.windowsecurity.com/articles/intrusion-detection-systems-faq.html

[20]www.networkworld.com/topics/ids-ips.html

[21]http://www.pcsecurityworld.com/79/intrusion-detection-systems-for-enterprise-security.html

[22] http://www.gslis.utexas.edu/~netsec/ids.htm

[23]http://www.airtightnetworks.com/home/solutions/wireless-intrusion-prevention.html

AUTHOR'S PROFILE

Nilotpal Chakraborty is a student of Masters of Technology in Systems Management, Devi Ahliya University, Indore, Madhya Pradesh, India. He earned his Bachelor degree from Assam University, Silchar, Assam, India in Information Technology. He is a prolific researcher and has published a number of international research journals. His area of interest includes Computer and Network Security, Cloud Computing, e-Governance, Design and Analysis of Algorithms, Databases and Web Development.