INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# NETWORK INTRUSION DETECTION SYSTEM

**MISS. PRATIKSHA PRAMOD DHOTE**

M.E Student, Department of Computer Science And Engineering, P.R Patil College of Engineering And Technology, Amravati, Maharashtra, India

**Accepted Date: 15/03/2016; Published Date: 01/05/2016**

**Abstract:** The area of intrusion detection is the central concept in overall network and computer security architecture. It is an important technology in business sector as well as in research area. By monitoring the computer and network resources, Intrusion Detection System (IDS) detects any of the misuse or unauthorized access which is basically an attack to these resources. Then it alerts and informs administrator for occurrence of an intrusion. Several methods can be used to detect an intrusion. Ever increasing demand of good quality communication relies heavily on Network Intrusion Detection System (NIDS). Intrusion detection for network security demands high performance. We have discuss here a description of the available approaches for a network intrusion detection system in both software and hardware implementation.

**Keywords:** Misuse Detection, Anomaly Detection, Software based NIDS approach, Hardware based NIDS approach.

**Corresponding Author: MISS. PRATIKSHA PRAMOD DHOTE**

**Access Online On:**

www.ijpret.com

**How to Cite This Article:**

Pratiksha Pramod Dhote, IJPRET, 2016; Volume 4 (9): 1334-1340

***PAPER-QR CODE***

## INTRODUCTION

Network Intrusion detection system can be described as the process of identifying and taking necessary actions against malicious activities targeted to network and computing resources. A network intrusion detection system should continuously monitor the traffic crossing the network and compare with a previously known set of malicious activities or look for statistical deviation of the system under surveillance from its normal behavior. Aim of network security is to protect the device from unauthorized and potentially harmful activities such as denial of service attacks.

### 1.1: Need of NIDS:

Security is an important issue for all the networks of companies and institutions at the present time and all the intrusions are trying in ways that successful access to the data network of these companies and Web services and despite the development of multiple ways to ensure that the infiltration of intrusion to the infrastructure of the network via the Internet, through the use of firewalls, encryption, etc. But IDS is a relatively new technology of the techniques for intrusion detection methods that have emerged in recent years. Intrusion detection system's main role in a network is to help computer systems to prepare and deal with the network attacks [1].

### 1.2: Objectives of NIDS:

- Monitoring and analyzing both user and system activities Analyzing system configurations and vulnerabilities.
- Assessing system and file integrity.
- Ability to recognize patterns typical of attacks.
- Analysis of abnormal activity patterns.
- Tracking user policy violations.

### 1.3: Importance of NIDS:

The purpose of network intrusion detection system is to help computer systems on how to deal with attacks and that network intrusion detection system is collecting information from several different sources within the computer systems and networks and compares this information with pre-existing patterns of discrimination as to whether there are attacks or weaknesses [2].

**1.4: Scope in Computer Science and engineering:**

Intruder's computers, who are spread across the Internet have become a major threat in our world. The researchers proposed a number of techniques such as firewall, encryption to prevent such penetration and protect the infrastructure of computers, but with this, the intruders managed to penetrate the computers. Network intrusion detection system has taken much of the attention of researchers.

Everyone now has no doubt that "Intrusion detection systems have become an essential component of computer security to detect attacks that can occur despite the best preventative measures" [3].Deploying the right tools to defend and protect a perimeter require man-hours, patience and knowledge. Security is more complex than any one organization, business process, or any one person's view or agenda. The IDS research community is developing better techniques for collecting and analyzing. data in order to handle intrusions in large, distributed environments. In order to take advantage of this work, ID systems must be able to quickly adapt to new, improved components, and changes in the environment [3].

**2. Related work:**

During the past five years, security of computer network has become main stream in most of everyone's lives. Today, most discussions on computer security is centered on the tools or techniques used in protecting and defending networks. The aim of network intrusion detection system is to examine the origins of detecting, analyzing and reporting of malicious activity, where it is today and where it appears to be heading in the future. Some of the many techniques and tools presently used in Network defence will be explored as well. There are a variety of tools providing a certain level of comfort with acceptable risks used in the defence and surveillance of computer networks. Defence -in-Depth is a term encompassing comprehensive analyst training, hardware deployed in strategic positions and a strong security policy necessary for achieving this objective. Every day, we have tools at our disposal to reach this goal. The aggregation of data comes from routers, the host itself, firewalls, virus scanners and a tool strictly designed to catch known attacks [3].

Historically, intrusion detection systems have been classified into two broad categories: Host-based systems and Network-based systems. Host-based systems, which are aimed at protecting individual hosts and operate on the basis of information contained in audit logs or other similar sources of data and Network-based systems, which operate by monitoring network traffic. Intrusion detection systems (IDSs) monitor host or network activity to spot

attempted or successful misuse of computers. Such misuses might constitute attacks or simply violations of policy restrictions. While there is a vast literature on network intrusion detection system, we touch on it here only in a limited fashion [4],

**3. Proposed Work:**

One approach to designing a network security system is to define network behavior patterns that indicate intrusive or improper use of the network and look for the occurrence of those patterns .while such an approach may be capable of detecting known varieties of intrusive behavior, it would allow new or undocumented types of attack to go undetected. As a result, our decision was to build a system which monitors and learns normal network behavior and then detects deviations from it.

**3.1 Types of intrusion detection system:**

**3.1.1: Misuse Detection:**

Misuse detection systems essentially define what's wrong. They contain attack descriptions and match them against the audit data stream, looking for evidence of known attacks. One such attacks, for example, would occurs if someone created a symbolic link to a Unix system's password file and executed a privileged application that accesses the symbolic link. In this example, the attack exploits the symbolic link. In this example, the attack exploits the lack of file access checks. The main advantage of misuse detection system is that they focus analysis on the audit data and the typically produce few false positives [5].

**3.1.2: Anomaly Detection:**

Anomaly detection uses models of the intended behavior of users and applications, interpreting deviations from this 'normal' behavior as a problem. A basic assumption of anomaly detection is that attacks differ from normal behavior. For example, we can model certain user's daily activity quite precisely. Suppose a particular user typically logs in around 10 a.m., reads mail, performs database transactions, takes a break between noon and 1 p.m., has very few files access errors, and so on. If the System notices that this same user logs in at 3 p.m., starts using compilers and debugging tools, and has numerous file access errors, it will flag this activity as suspicious. The main advantage of anomaly detection systems is that they can detect previously unknown attacks. By defining what's normal, they can identify any violation, whether it is part of the threat model or not [5].

There are two approaches of NIDS:

1. Software based NIDS approach,

2. Hardware based NIDS approach.

**3.2 Software based NIDS approach:**

Software based NIDS relies heavily on Snort Rules. Snort is a network intrusion prevention and detection system developed by Sourcefire. Snort is the most popular intrusion detection and prevention technology and has world -wide industry usage [6]. Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use [7].

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified [7].

**3.3 Hardware based NIDS approach**

Intrusion detection systems are highly dependent on their hardware architecture. Therefore, some researchers have focused on ways to improve IDS performance by analyzing various aspects of the hardware implementation. Most researchers use field programmable gate arrays (FPGA) as a preferred hardware platform. Sidhu and Prasanna in 2001 provided an efficient method for intrusion detection using FPGAs and regular expressions. They showed that performing matches using regular expressions can be more efficiently done on FPGA implementations than on standard PC implementations. They ran their experiment using both the Intel Pentium III processor and a Virtex FPGA. Their study found that using regular expression matching will result in situations where not enough memory is available on the PC. In this case, an FPGA can be more suitable [6]. Baker and Prasanna in 2004, proposed a

methodology for building an efficient IDS using an FPGA as the hardware platform and optimizing the design of the system. They applied optimization processes in order to have efficient parallel multi-byte comparisons and partial matches for high performance calculations using FPGA.They showed that this methodology results in faster computing times. As a down side, their approach also increased the amount of false-positive alerts issued by the system be more suitable. Baker and Prasanna in 2004, proposed a methodology for building an efficient IDS using an FPGA as the hardware platform and optimizing the design of the system. They applied optimization processes in order to have efficient parallel multi-byte comparisons and partial matches for high performance calculations using FPGA. They showed that this methodology results in faster Computing times. As a down side, their approach also increased the amount of false-positive alerts issued by the system [7].

**CONCLUSION:**

In this paper, we have discussed that an intrusion detection system is the important part of the defensive system of computer and network resources. This system detects attacks and intrusions more accurately than any other security system and raises fewer false positive alarms. As it is an important security measure, so it becomes the need for organizations to implement this to detect the attacks and other malicious activities at preliminary stage.

**4. REFERENCES:**

1. D. E. Denning, "An intrusion detection model." IEEE Transactions on Software Engineering, Vol. SE-13 No. 2:222-232, Feb. 1987.
2. Heberlein, L. etal. "A Network Security Monitor." Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, May 1990, pp. 296-303
3. Lippman, Richard et al. 'The 1999 DARPA off-line intrusion detection evaluation",Volume 34, Number 4, October 2000.
4. V. Paxson. Bro: A system for detecting network intruders in real-time. Computer Networks (Amsterdam, Netherlands:1999), 31(23–24):2435–2463, 1999.
5. J.saltzr and m.schroeceder,"The protection of information in computer system"proc. IEEE,vol.63,no.9,1975,pp.1278-1308.
6. Zachary K. Baker, Student Member, IEEE, and Viktor K. Prasanna, Fellow, IEEE. Automatic Synthesis of Efficient Intrusion Detection Systems on FPGAs. IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, October-December 2006.
7. Baker, Z. K., & Prasanna, V. K. 2004. A methodology for synthesis of efficient intrusion detection systems on FPGAs.

8. In Field-Programmable Custom Computing Machines, 2004. FCCM 2004, 12th Annual IEEE Symposium on (pp. 135-144).