Intrusion Detection System- Types and Prevention

B.Santos Kumar, T.Chandra Sekhara Phani Raju, M.Ratnakar, Sk.Dawood Baba, N.Sudhakar

Wellfare Institute of Science, Technology & Management
Dept of CSE
Vishakhapatnam, A.P

Abstract: Intrusion detection is the act of detecting unwanted traffic on a network or a device. An 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. This article aims at providing (i) a general presentation of the techniques and types of the intrusion detection and prevention systems, (ii) an in-depth description of the evaluation, comparison and classification features of the IDS and the IPS.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. An IPS is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and related information.

Keywords: IDS, IPS, DIDS, NIDS, OSI.

I. INTRODUCTION

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) 1 are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization. IDPSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack’s content. This publication describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them. The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed. Therefore, it is important for them to value the improvements brought by these new devices. In the same way, for the network and systems administrators, it would be interesting to assess the IDS/IPS to be able to choose the best before installing it on their networks or systems, but also to continue to evaluate its efficiency in operational method. Unfortunately, many false positives and false negatives persist in the new versions of the IDS/IPS, then, they brought improvements are not worthy of the continuous efforts of research and development in the domain of the detection and the prevention of intrusion. In general, it is essentially due to the absence of efficient methods of assessment of the security tools, and of the IDS/IPS in particular.

II. TYPES OF IDS’S

Several types of IDS technologies exist due to the variance of network configurations. Each type has advantages and disadvantage in detection, configuration, and cost. Mainly, there are three important distinct families of IDS: The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed.

Network-Based

A Network Intrusion Detection System (NIDS) is one common type of IDS that analyzes network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for suspicious activity. Most NIDSs are easy to deploy on a network and can often view traffic from many systems at once. A term becoming more widely used by vendors is “Wireless Intrusion Prevention System” (WIPS) to describe a network device that monitors and analyzes the wireless radio spectrum in a network for intrusions and performs countermeasures which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks. The NIDS are also called passive IDS since this kind of systems inform the administrator system that an attack has or had taken place, and it takes the adequate measures to assure the security of the system. The aim is to inform about an intrusion in order to look for the IDS capable to react in the post. Report of the damages is not sufficient. It is necessary that the IDS react and to be able to block the detected doubtful traffics. These reaction techniques imply the active IDS.

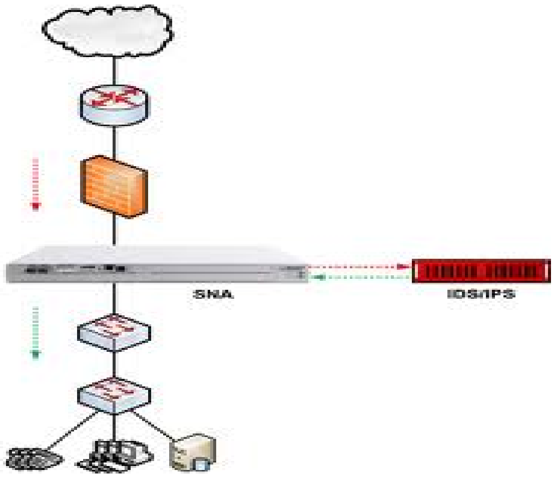

Fig: Location of IDS/IPS

The Host Intrusion Detection System

According to the source of the data to examine, the Host Based Intrusion Detection System can be classified in two categories:

- The HIDS Based Application. The IDS of this type receive the data in application, for example, the logs files generated by the management software of the database, the server web or the firewalls. The vulnerability of this technique lies in the layer application.
- The HIDS Based Host. The IDS of this type receive the information of the activity of the supervised system. This information is sometimes in the form of audit traces of the operating system. It can also include the logs system of other logs generated by the processes of the operating system and the contents of the object system not reflected in the standard audit of the operating system and the mechanisms of logging. These types of IDS can also use the results returned by another IDS of the Based Application type.

Host-based intrusion detection systems (HIDS) analyze network traffic and system-specific settings such as software calls, local security policy, local log audits, and more. A HIDS must be installed on each machine and requires configuration specific to that operating system and software. Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

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 baselining to determine the nominal amount of a segment's traffic. The NIDS-HIDS combination or the so called hybrid gathers the features of several different IDS. It allows, in only one single tool, to supervise the network and the terminals. The probes are placed in strategic points, and act like NIDS and/or HIDS according to their sites. All these probes carry up the alerts then to a machine which centralize them all, and aggregate the information of multiple origins.

Wireless

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. Some forms of IDPS are more mature than others because they have been in use much longer. Network-based IDPS and some forms of host-based IDPS have been commercially available for over ten years. Network behavior analysis software is a somewhat newer form of IDPS that evolved in part from products created primarily to detect DDoS attacks, and in part from products developed to monitor traffic flows on internal networks. Wireless technologies are a relatively new type of IDPS, developed in response to the popularity of wireless local area networks (WLAN) and the growing threats against WLANs and WLAN clients.

III. DETECTION TYPES

Signature-Based Detection

An IDS can use signature-based detection, relying on known traffic data to analyze potentially unwanted traffic. This type of detection is very fast and easy to configure. However, an attacker can slightly modify an attack to render it undetectable by a signature based IDS. Still, signature-based detection, although limited in its detection capability, can be very accurate.

Anomaly-Based Detection

An IDS that looks at network traffic and detects data that is incorrect, not valid, or generally abnormal is called anomaly-based detection. This method is 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.

Stateful Protocol Inspection

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.

False Positives and Negatives

It is impossible for an IDS to be perfect, primarily because network traffic is so complicated. The erroneous results in an IDS are divided into two types: false positives and false negatives. False positives occur when the IDS erroneously detects a problem with benign traffic. False negatives occur when unwanted traffic is undetected by the IDS. Both create problems for security administrators and may require that the system be calibrated. A greater number of false positives are generally more acceptable but can burden a security administrator with cumbersome amounts of data to sift through.

However, because it is undetected, false negatives do not afford a security administrator an opportunity to review the data.

IDPSs cannot provide completely accurate detection; they all generate false positives (incorrectly identifying benign activity as malicious) and false negatives (failing to identify malicious activity). Many organizations choose to tune IDPSs so that false negatives are decreased and false positives increased, which necessitates additional analysis resources to differentiate false positives from true malicious events. Most IDPSs also offer features that compensate for the use of common evasion techniques, which modify the format or timing of malicious activity to alter its appearance but not its effect, to attempt to avoid detection by IDPSs.Most IDPSs use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection. The primary classes of detection methodologies are as follows:

Signature-based, which compares known threat signatures to observed events to identify incidents. This is very effective at detecting known threats but largely ineffective at detecting unknown threats and many variants on known threats. Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

Anomaly-based detection, which compares definitions of what activity, is considered normal against observed events to identify significant deviations. This method uses profiles that are developed by monitoring the characteristics of typical activity over a period of time. The IDPS then compares the characteristics of current activity to thresholds related to the profile. Anomaly-based detection methods can be very effective at detecting previously unknown threats. Common problems with anomaly-based detection are inadvertently including malicious activity within a profile, establishing profiles that are not sufficiently complex to reflect real-world computing activity, and generating many false positives.

Stateful protocol analysis, which compares predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. It is capable of understanding and tracking the state of protocols that have a notion of state, which allows it to detect many attacks that other methods cannot. Problems with stateful protocol analysis include that it is often very difficult or impossible to develop completely accurate models of protocols, it is very resource-intensive, and it cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior.

IV. INTRUSIONS PREVENTION SYSTEM

The intrusion prevention is an amalgam of security technologies. Its goal is to anticipate and to stop the attacks [2]. The intrusion prevention is applied by some recent IDS. Instead of analyzing the traffic logs, which lies in discovering the attacks after they took place, the intrusion prevention tries to warn against such attacks. While the systems of intrusion detection try to give the alert, the intrusion prevention systems block the traffic rated dangerous. Over many years, the philosophy of the intrusions detection on the network amounted to detect as many as possible of attacks and possible intrusions and to consign them so that others take the necessary measures. On the contrary, the systems of prevention of the intrusions on the network have been developed in a new philosophy "taking the necessary measures to counter attacks or detectable intrusions with precision ".In general terms, the IPS are always online on the network to supervise the traffic and intervene actively by limiting or deleting the traffic judged hostile by

interrupting the suspected sessions or by taking other reaction measures to an attack or an intrusion. The IPS functions symmetrically to the IDS; in addition to that, they analyze the connection contexts, automatize the logs analysis and suspend the suspected connections. Contrary to the classic IDS, the signature is not used to detect the attacks. Before taking action, The IDS must make a decision about an action in an appropriate time. If the action is in conformity with the rules, the permission to execute it will be granted and the action will be executed.

But if the action is illegal an alarm is issued. In most cases, the other detectors of the network will be informed with the goal to stop the other computers from opening or executing specific files. Unlike the other prevention techniques, the IPS is a relatively new technique. It is based on the principle of integrating the heterogeneous technologies: firebreak, VPN, IDS, anti-virus, anti-Spam, etc. Although the detection portion of an IDS is the most complicated, the IDS goal is to make the network more secure, and the prevention portion of the IDS must accomplish that effort. After malicious or unwanted traffic is identified, using prevention techniques can stop it. When an IDS is placed in an inline configuration, all traffic must travel through an IDS sensor. When traffic is determined to be unwanted, the IDS do not forward the traffic to the remainder of the network. To be effective, however, this effort requires that all traffic pass through the sensor. When an IDS is not configured in an inline configuration, it must end the malicious session by sending a reset packet to the network. Sometimes the attack can happen before the IDS can reset the connection. In addition, the action of ending connections works only on TCP, not on UDP or internet

control message protocol (ICMP) connections. A more sophisticated approach to IPS is to reconfigure network devices (*e.g.*, firewalls, switches, and routers) to react to the traffic. Virtual local area networks (VLAN) can be configured to quarantine traffic and limit its
connections to other resources. The IPS allows the following functionalities [8]:

- ✓ Supervising the behaviour of the application
- ✓ Creating rules for the application
- ✓ Issuing alerts in case of violations
- ✓ Correlating different sensors to guarantee a better Protection against the attacks.
- ✓ Understanding of the IP networks
- ✓ Having mastery over the network probes and the logs analysis
- ✓ Defending the vital functions of the network carrying out an analysis with high velocity.

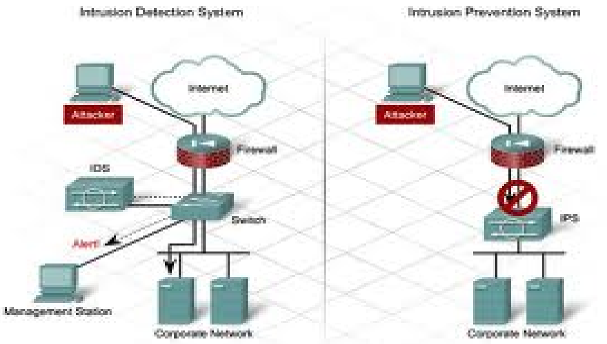

Fig: Intrusion Detection and Prevention System

Network Behavior Anomaly Detection

NBAD is an IDS technology in which the shape or statistics of traffic, not individual packets, determines if the traffic is malicious. NBAD sensors are placed around a network in key places, such as at switches, at demilitarized zones (DMZ), and at locations at which traffic splits to different segments. Sensors then report on what type and amount of traffic is passing through. By viewing the shape of the traffic, an NBAD can detect DoS attacks, scanning across the network, worms, unexpected application services, and policy violations. NIDS and NBAD systems share some of the same components, such as sensors and management consoles; however, unlike NIDS, NBAD systems usually do not have database servers.

The Host Intrusion Prevention System

Nowadays, the attacks evolve quickly and are targeted. Also, it is necessary to have a protection capable to stop the malwares before the publication of an update of the specific detection. An intrusions prevention system based on the Host Intrusion Prevention System or HIPS is destined to stop the malwares before an update of the specific detection is taken by supervising the code behaviour. The majority of the HIPS solutions supervises the code at the time of its execution and intervenes if the code is considered suspected or malevolent [7].

V. IDS TOOLS

AIDE—Advanced Intrusion Detection Environment

AIDE is a free replacement for Tripwire®, which operates in the same manner as the semi-free Tripwire, but provides additional features. AIDE creates a database from the regular expression found in a customizable configuration file. Once this database is initialized, it can be used to verify the integrity of the files. It has several messages digest algorithms (md5, sha1, rmd160, Tiger®, Haval, *etc.*) that are used to check the integrity of the file. More algorithms can be added with relative ease. All the usual file attributes can be checked for inconsistencies, and AIDE can read databases from older or newer versions.

Alert-Plus

Alert-Plus is a rule based system that compares events recorded in a Safeguard audit trail against custom-defined rules and automatically invokes a response when it detects an event of interest. Alert-Plus can detect an intrusion attempt and actually help to block it. Example of Alert Plus Are Builints and Dash Boards.

Eye Retina

Retina Network Security Scanner provides vulnerability management and identifies known and zero day vulnerabilities, plus provides security risk assessment, enabling security best practices, policy enforcement, and regulatory audits.

eEye SecureIIS Web Server Protection

SecureIIS Web server security delivers integrated multi-layered Windows server protection. It provides application layer protection *via* integration with the IIS platform as an Internet Server Application Programming Interface (ISAPI) filter, protecting against known and unknown exploits, zero day attacks and unauthorized Web access.

GFI Events Manager

GFI Events Manager is a software-based events management solution that delivers automated collection and processing of events from diverse networks, from the small, single-domain network to extended, mixed environment networks, on multiple forests and in diverse geographical locations. It offers a scalable design that enables you to deploy multiple instances of the front-end application, while at the same time, maintaining the same database backend. This decentralizes and distributes the event collection process while centralizing the monitoring and reporting aspects of events monitoring.

11i Host Intrusion Detection System (HIDS)

HP-UX HIDS continuously examines ongoing activity on a system, and it seeks out patterns that suggest security breaches or misuses. Security threats or breaches can include attempts to break into a system, subversive activities, or spreading a virus. Once you activate HP-UX HIDS for a given host system and it detects an intrusion attempt, the host sends an alert to the administrative interface where you can immediately investigate the situation, and when necessary, take action against the intrusion.

IBM RealSecure Server Sensor

IBM RealSecure Server Sensor provides automated, real-time intrusion protection and detection by analyzing events, host logs, and inbound and outbound network activity on critical enterprise servers in order to block malicious activity from damaging critical assets.

INTEGRIT

Integrit has a small memory footprint, uses up-to-date cryptographic algorithms, and has other features. The integrit system detects intrusion by detecting when trusted files have been altered. By creating an integrit database (update mode) that is a snapshot of a host system in a known state, the host's files can later be verified as unaltered by running integrit in check mode to compare current state to the recorded known state. integrit can do a check and an update simultaneously.

Lumension Sanctuary Application Control

Lumension Application Control (formerly Secure Wave Sanctuary® Application Control) is a three-tiered client/server application that provides the capability to centrally control the programs and applications users are able to execute on their client computers. Three tiers of a Sanctuary Application Control Desktop (SACD) deployment comprise:

An SQL database

- ***One or more servers***
- ***Client kernel driver (SXD)***
- ***McAfee Host Intrusion Prevention***

McAfee Host Intrusion Prevention (HIP) is a host based intrusion prevention system designed to protect system resources and applications. Host Intrusion Prevention is part of McAfee Total Protection for Endpoint, which integrates with McAfee ePolicy Orchestrator® for centralized reporting and management that's accurate, scalable, and easy to use and works with other McAfee and non-McAfee products.

Osiris

Osiris is a host integrity monitoring system that can be used to monitor changes to a network of hosts over time and report those changes back to the administrator(s). Currently, this includes monitoring any changes to the file systems. Osiris takes periodic snapshots of the file system and stores them in a database. These databases, as well as the configurations and logs, are all stored on a central management host. When changes are detected, Osiris will log these events to the system log and optionally send email to an administrator.

CLASSIFICATION OF THE IPS/IDS:

The following criteria will be adopted in the classification of the IPS/IDS:

Reliability: The generated alerts must be justified and no intrusion to escape

Reactivity: An IDS/IPS must be capable to detect and to prevent the new types of attacks as quickly as possible. Thus, it must constantly self-update. Capacities of automatic update are so indispensable.

Facility of implementation and adaptability: An IDS/IPS must be easy to function and especially to adapt to the context in which it must operate. It is useless to have an IDS/IPS giving out some alerts in less than 10 seconds if the resources necessary to a reaction are not available to act in the same constraints of time.

Performance: the setting up of an IDS/IPS must not affect the performance of the supervised systems. Besides, it is necessary to have the certainty that the IDS/IPS has the capacity to treat all the information in its disposition because in the reverse case it becomes trivial to conceal the attacks while increasing the quantity of information. These criteria must be taken into consideration while classifying an IDS/IPS, as well:

- The sources of the data to analyze, *network*, *system* or *application*
- The behaviour of the product after intrusion *passive* or *active*
- The frequency of use, *periodic* or *continuous*
- The operating system in which operate the tools, *Linux*, *Windows*, *etc*.
- The source of the tools, *open* or *private.*

VI. CONCLUSION

This study has proved that both the intrusion detection systems and the intrusion prevention systems still need to be improved to ensure an unfailing security for a network. They are not reliable enough (especially in regard to false positives and false negatives) and they are difficult to administer. Yet, it is obvious that these systems are now essential for companies to ensure their security. To assure an effective computerized security, it is strongly recommended to combine several types of detection

system. The IPS, which attempt to compensate in part for these problems, is not yet effective enough for use in a production context. They are currently mainly used in test environments in order to evaluate their reliability. They also lack a normalized operating principle like for the IDS. However, these technologies require to be developed in the coming years due to the increasing security needs of businesses and changes in technology that allows more efficient operation detection systems and intrusion prevention. We are working on the implementation of a screening tool of attack and the characterization of test data. We also focus on the collection of exploits and attacks to classify and identify. Further work is under way and many ways remain to be explored. Then it would be interesting to conduct assessments of existing IDS and IPS following the approaches we have proposed and tools developed in this work. This paper provided a new way of looking at network intrusion detection research including intrusion detection types that are necessary, complete, and mutually exclusive to aid in the fair comparison of intrusion detection methods and to aid in focusing research in this area.

ACKNOWLEGMENT

Thanks to management of WISTM Engg College and to my guide Mr. B.Kiran Kumar M.Tech is working as Asst.Prof in the department of CSE in WellFare institute of science, Technology & Management.

REFERENCES

[1] Langin, C. L. A SOM+ Diagnostic System for Network Intrusion Detection. Ph.D. Dissertation, Southern Illinois University Carbondale (2011)

[2] Amoroso, E.: Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Intrusion.Net Books (1999)

[3] Denning, D.: An Intrusion-Detection Model. IEEE Transactions on Software Engineering 13(2), 118-131 (1986)

[4] Young, C.: Taxonomy of Computer Virus Defense Mechanisms. In: The 10th National Computer Security Conference Proceedings (1987)

[5] Lunt, T.: Automated Audit Trail Analysis and Intrusion Detection: A Survey. In: Proceedings of the 11th National Computer Security Conference, Baltimore, pp.65-73 (1988)

[6] Lunt, T.: A Survey of Intrusion Detection Techniques. Computers and Security 12, 405-418 (1993)

[7] Vaccaro, H., Liepins, G.: Detection of Anomalous Computer Session Activity. In: Proceedings of the 1989 IEEE Symposium on Security and Privacy (1989)

[8] Helman, P., Liepins, G., Richards, W.: Foundations of Intrusion Detection. In: Proceedings of the IEEE Computer Security Foundations Workshop V (1992)

[9] Denault, M., Gritzalis, D., Karagiannis, D., Spirakis, and P.: Intrusion Detection: Approach and Performance Issues of the SECURENET System. Computers and Security 13(6), 495-507 (1994)

[10] Crying wolf: False alarms hide Newman attacks, Snyder & Thayer Network World, 24/06/02, http://www.nwfusion.com/techinsider/2002/0624security1.html

[11] F. Cikala, R. Lataix, S. Marmeche", The IDS/IPS. Intrusion Detection/Prevention Systems ", Presentation, 2005.

[12] Hervé Debar and Jouni Viinikka, "Intrusion Detection,: Introduction to Intrusion Detection Security and Information Management", Foundations of Security Analysis and Design III, Reading Notes in to Compute Science, Volume 3655, 2005. pp. 207-236.

[13] Hervé Debar, Marc Dacier and Andreas Wespi, "IN Revised Taxonomy heart Intrusion Detection Systems", Annals of the Telecommunications, Flight. 55, Number,: 7-8, pp. 361-378, 2000.

[14] Herve Schauer Consultants", The detection of intrusion…" Presentation: excerpt of the course TCP/IP security of the Cabinet HSC, March 2000.

[15] ISS Internet Risk Impact Summary - June 2002.

[16] Janne Anttila", Intrusion Detection in Critical Ebusiness Environment ", Presentation, 2004.

[17] D K. Müller", IDS - Systems of intrusion Detection, Left II ", July 2003, http://www.linuxfocus.org/Francais/July2003/article294.shtml

AUTHORS

T.Chandra Sekhar Phaniraju

Sk.Dawood Baba

M.Ratnakar

B.Santos Kumar

N.Sudhakar

Students of WellFare institute of Science technology & Management, pinagadi, Vishakapatnam.