International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 1 (February '2017)
Special Issue on 1st National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

A STUDY ON NETWORK SECURITY AND INTRUSION DETECTION SYSTEM

P.Kanagavalli,
Research Scholar,
Periyar University,
Salem, Tamilnadu,India.

Dr.V.Karthikeyani,
Assistant Professor,
Department of Computer Science,
NKR Government Arts College for Women,
Namakkal ,Tamilnadu,India.

Abstract : In the era of information and communication technology, Security is an important issue. A lot of effort and finance are being invested in this sector. Intrusion detection is one of the most prominent fields in this area. Data mining in network intrusion detection can automate the network intrusion detection field with a greater efficiency. Intrusion detection is the problem of identifying unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators. The proliferation of heterogeneous computer networks provides additional implications for the intrusion detection problem. The fast propagation of computer networks has changed the viewpoint of network security. A boundlessness of methods for misuse detection as well as anomaly detection has been applied. IDS's are based on the belief that an intruder's behavior will be noticeably different from that of a legitimate user. We are designing and implementing a prototype Distributed Intrusion Detection System (DIDS) that combines distributed monitoring and data reduction (through individual host and LAN monitors) with centralized data analysis (through the DIDS director) to monitor a heterogeneous network of computers. Many of the technologies proposed are complementary to each other, since for different kind of environments some approaches perform better than others. This paper presents a review of intrusion detection systems that is then used to survey and classify them. The taxonomy consists of the detection principle, and second of certain operational aspects of the intrusion detection system.

Keywords: **Intrusion Detection System,** ***Network Security, Local Area Network, Host Based Attacks***

I.INTRODUCTION

An **intrusion detection system** (IDS) monitors network traffic and monitors for suspicious activity and alerts the **system** or network administrator. In some cases, the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. A network **intrusion detection system** (NIDS) is crucial for network security because it enables you to **detect** and respond to malicious traffic. The primary purpose of an **intrusion detection system** is to ensure IT personnel is notified when an attack or network **intrusion** might be taking place. Intrusion detection is defined to be the problem of identifying individuals who are using a computer system without authorization (i.e., crackers) and those who have legitimate access to the system but are exceeding their privileges (i.e., the insider threat). Work is being done elsewhere on Intrusion Detection Systems (IDS's) for a single host [10118] and for several hosts connected by a network [7612]. Our own earlier work on the Network Security Monitor (NSM) concentrated on monitoring a broadcast Local Area Network (LAN) [3].

Network intrusion detection is becoming an increasingly important tool to detect and analyze security threats on an organization's network. It complements other network security techniques, such as firewalls, by providing information about the frequency and nature of attacks. A network intrusion detection system (NIDS) often consists of a sensor that analyzes every network packet on the segment under observation, and forwards packets deemed interesting together with an alert message to a backend system that stores them for further analysis and correlation with other events. The sensor is often implemented as a general-purpose computer system running network intrusion detection software. A separate system may host a database or similar software to provide long-term storage and additional analysis capabilities [2][3]. By relying on off-the-shelf hardware and software, this approach produces a cost-effective and flexible network intrusion detection system.

II.INTRUSION DETECTION SYSTEMS AND RELATED RESEARCH

Identifying unauthorized use, misuse and attacks on information systems is defined as intrusion detection [4]. The most popular way to detect intrusions has been done by using audit data generated by operating systems and by networks. Since almost all activities are logged on a system, it is possible that a manual inspection of these logs would allow intrusions to be detected. It is important to analyze the audit data even after an attack has occurred, for determining the extent of damage occurred, this analysis helps in attack trace back and also helps in recording the attack patterns for future prevention of such attacks. An intrusion detection system can be used to analyze audit data for such insights. This makes intrusion detection system a valuable real-time detection and prevention

tool as well as a forensic analysis tool. Soft computing techniques are being widely used by the IDS community due to their generalization capabilities that help in detecting know intrusions and unknown intrusions or the attacks that have no previously described patterns. Earlier studies have utilized a rule based approach for intrusion detection, but had a difficulty in identifying new attacks or attacks that had no previously describe patterns [5]. Lately the emphasis is being shifted to learning by examples and data mining paradigms. Neural networks have been extensively used to identify both misuse and anomalous patterns. Recently support vector machines and their variants are being proposed to detect intrusions. Several researchers proposed data mining techniques to identify key patterns that help in detecting intrusions. Distributed agent technology is being proposed by a few researchers to overcome the inherent limitations of the client-server paradigm and to detect intrusions in real time.

2.1 Misuse Detection

The idea of misuse detection is to represent attacks in the form of a pattern or a signature so that the same attack can be detected and prevented in future. These systems can detect many or all known attack patterns, but they are of little use for detecting naive attack methods. The main issues of misuse detection is how to build signatures that include possible signatures of attacks build a signature that includes all possible variations of the pertinent attack to avoid false negatives, and how to build signatures that do not match non-intrusive activities to avoid false positives.

2.2 Anomaly Detection

The idea here is that if we can establish a normal activity profile for a system, in theory we can flag all system states varying from the established profile as intrusion attempts. However, if the set of intrusive activities is not identical to the set of anomalous activities, the situation becomes more interesting instead of being exactly the same, we find few interesting possibilities. Anomalous activities that are not intrusive are flagged as intrusive, though they are false positives. Actual intrusive activities that go undetected are called false negatives. This is a serious issue, and is far more serious than the problem of false positives. One of the main issues of anomaly detection systems is the selection of threshold levels so that neither of the above problems is unreasonably magnified. Anomaly detection is usually computationally expensive because of the overhead of keeping track of and possibly updating several system profiles. Recent proposed system LEARD (Learning Rules for Anomaly Detection) discovers relationships among attributes in order to model application protocols.

III. EFFICIENCY OF INTRUSION-DETECTION SYSTEMS

To evaluate the efficiency of an intrusion-detection system, Porras and Valdes have proposed the following three parameters: Accuracy.

Accuracy: deals with the proper detection of attacks and the absence of false alarms. Inaccuracy occurs when an intrusion-detection system flags a legitimate action in the environment as anomalous or intrusive.

Performance: The performance of an intrusion-detection system is the rate at which audit events are processed. If the performance of the intrusion-detection system is poor, then real-time detection is not possible.

Completeness: Completeness is the property of an intrusion-detection system to detect all attacks. Incompleteness occurs when the intrusion-detection system fails to detect an attack. This measure is much more difficult to evaluate than the others because it is impossible to have a global knowledge about attacks or abuses of privileges. Let us introduce two additional properties:

Fault tolerance: An intrusion-detection system should itself be resistant to attacks, especially denial-of service-type attacks, and should be designed with this goal in mind. This is particularly important because most intrusion-detection systems run above commercially available operating systems or hardware, which are known to be vulnerable to attacks.

Timeliness: An intrusion-detection system has to perform and propagate its analysis as quickly as possible to enable the security officer to react before much damage has been done, and also to prevent the attacker from subverting the audit source or the intrusion-detection system it. This implies more than the measure of performance because it not only encompasses the intrinsic processing speed of the intrusion-detection system, but also the time required to propagate the information and react to it.

IV.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.

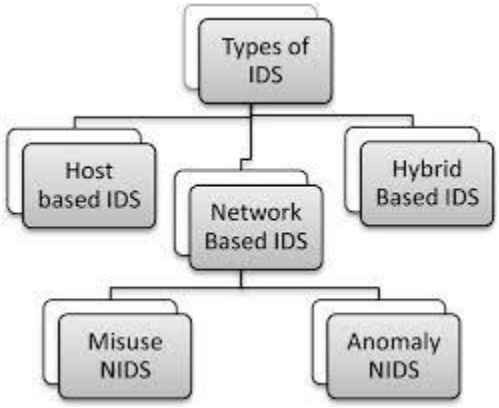

Figure 1: Types of IDs

1. 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.

2. Host -Based

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 base lining 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.

3. Hybrid –Based

The **hybrid** IDS is obtained by combining packet header anomaly **detection** (PHAD) and network traffic anomaly **detection** (NETAD) which are anomaly-based IDSs with the misuse-based IDS Snort which is an open-source project.

V.ISSUES AND CHALLENGES IN IDS

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 [5]. In this paper, we have identified some important issues and challenges which need to be addressed by research communities.

The issues and challenges are as:

- ✓ Deficiency or incomplete Data set
- ✓ Algorithms for Detection
- ✓ Integration of multiple formats of data
- ✓ Platform dependencies
- ✓ Weak Design
- ✓ Evaluation of IDS
- ✓ Let we explain these issues

VI.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 Secure IIS Web Server Protection SecureIIS Web server security delivers integrated multilayered 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 Real Secure Server Sensor IBM Real Secure 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- 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.

VII.CONCLUSION

Our Distributed Intrusion Detection System (DIDS) is being developed to address the shortcomings of current single host IDS's by generalizing the target environment to multiple hosts connected via a network (LAN). Most current IDS's do not consider the impact of the LAN structure when attempting to monitor user behavior for attacks against the system. Intrusion detection systems designed for a network environment will become increasingly important as the number and size of LAN's increase. Our prototype has demonstrated the viability of our distributed architecture in solving the network-user identification problem. We have tested the system on a sub-network of Sun SPARCstation and it has correctly identified network users in a variety of scenarios. Work continues on the design, development, and refinement of rules, particularly those which can take advantage of knowledge about particular kinds of attacks. The initial prototype expert system has been written in Prolog, but it is currently being ported to CLIPS due to the latter's superior performance characteristics and easy integration with the C programming language. We are designing a signature analysis component for the host monitor to detect events and sequences of events that are known to be indicative of an attack, based on a specific context. In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment.

REFERENCES:

[1]. Department of Defense, Trusted Computer System Evaluation Criteria, National Computer Security Center, DOD 5200.28-STD, Dec. 1985. 2
[2]. http://en.wikipedia.org/wiki/Intrusion_detection_system .
[3]. E. Lundin, E. Jonsson, Survey of research in the intrusion detection area, Technical report 02-04, Department of Computer Engineering, Chalmers University of Technology, Goteborg January 2002,
[4]. R. Base, P. Mell, "Special publication on intrusion detection systems", NIST Infidel, Inc., National Institute of Standards and Technology, Scotts Valley, CA, 2001.
[5]. https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799.
[6]. Kendall K. (1998) "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems", Master's Thesis, Massachusetts Institute of Technology.
[7]. Hertz J., Krogh A., Palmer R. G. (1991) "Introduction to the Theory of Neural Computation," Addison – Wesley.
[8]. Joachims T. (1998) "Making Large-Scale SVM Learning Practical," LS8-Report, University of Dortmund, LS VIII-Report.
[9]. Friedman J. H. (1991) "Multivariate Adaptive Regression Splines", Analysis of Statistics, Vol 19, pp. 1-141.
[10]. J. Coit, S. Staniford, J. McAlerney, "Towards Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort," Proc. DARPA Information Survivability Conference and Exposition (DISCEX II '02), IEEE CS Press, Los Alamitos, Calif., 2001, pp. 367-373.
[11]. R. Danyliw, "ACID: Analysis Console for Intrusion Databases," http://acidlab.sourceforge.net, 2001. [6] S. Edwards, "Vulnerabilities of Network Intrusion Detection Systems: Realizing and Overcoming the Risks. The Case for Flow Mirroring," whitepaper, Top Layer Networks, Inc., 2002.