Dual-Guarded Intrusions Detection System

[1] Manish Satpute,[2] Swapnil Kotwal,[3] Prashant Kalel,[4] Jayant Gaikwad,[5]R. B. Rathod

[1]Student,[2]Student,[3]Student,[4]Student,[5]Professor

[1]Department of Computer Engineering,

[1] PDEA's College of Engineering, Manjari(Bk), Pune, India

***Abstract*— Internet and its services are most important part as of today. But as we know nothing comes with so ease, similarly all the services which are provided by internet are also vulnerable and need to b secured. There are many mechanisms to protect internet, some of them are firewalls and IDS. The complexity of web is increasing day by day and as of now its has moved to multitier design where web server, application logic and database servers are separated from each other. So it is necessary to provide security to both of front end and back end. But most of IDS present today fail to do so.**

In this paper we present an IDS with DualGuard, an IDS that can provide security to both front end and back end. This IDS will be able to detect intrusions in static as well as dynamic web applications too. Will be able to train this IDS on real life-world traffic for around 15-day period. With this IDS it is possible to detect maximum of attacks both on front end and back end simultaneously while maintaining as much as less false positive rate. We will be implementing this with the help of apache web server, MySQL and lightweight virtualization.

***IndexTerms*— Multitier, intrusions, Intrusion detection system (IDS), Apache web server, MYSQL**

I. INTRODUCTION

Within the last few years some organizations have come to incorporate information technology into their internal operations and business solutions on an enormous scale. This phenomenon is complimented by the increasing need for remote access to system resources due to the growing trend toward telecommuting and the increased utilization of video and voice conferencing. In addition, many local and federal government functions are now conducted over the Internet. As a result, both business and government have become critically dependent on both internal and external computer networks. In many respects, this is an encouraging and positive condition; these networks allow for a more efficient workplace, a more versatile and mobile workforce, and facilitate such things as global communication and electronic commerce. However, in some ways, this leaves the businesses and government organizations in a dangerous position. Crime, for example,that would traditionally be directed at a specific outlet of a store or a strategic federal office, will now likely be directed at the information systems maintained by these bodies. Since these organizations are so dependent on network operation and connectivity, most with mission-critical resources residing on these networks, they leave themselves extremely susceptible to malicious activity that is directed at their networks. Rightly so, awareness about security measures for these systems has increased immensely. It is common for a company to implement a firewall or a security policy, but experience has shown these to be dramatically insufficient. Both industry and government will come to depend on more advanced and integrated security measures to protect their systems from attacks. Though several methods exist for providing network security, arguably the best tool for doing this is the use of intrusion detection systems, these systems are the logical complement of network firewalls and security management. Intrusion detection systems are available in two flavors, host-based and network-based. This paper will first explain what intrusion detection is, then explain and evaluate the two approaches to intrusion detection systems individually, and finally analyze the converging trends of these two methods as well as touch on the evolution of intrusion detection systems. It should be noted that this text is not intended to be a survey or comparison of current intrusion detection systems, for those interested, a partial listing of these systems is available on the Internet

.

II. INTRUSION DETECTION SYSTEM

A. Host-based Systems

Host-based intrusion detection systems are aimed at collecting information about activity on a particular single system, or host. These host-based agents, which are sometimes referred to as sensors, would typically be installed on a machine that is deemed to be susceptible to possible attacks. The term "host" refers to an individual computer, thus a separate sensor would be needed for every machine. Sensors work by collecting data about events taking place on the system being monitored. This data is recorded by operating system mechanisms called audit trails. Other sources from which a host-based sensor can obtain data, "include system logs, other logs generated by operating system processes, and contents of objects not reflected in standard operating system audit and logging mechanisms". These logs are for the most part simple text files, which are written a few lines at a time, as events occur and operations on a system take place.

As host-based systems rely heavily on audit trails, they become limited by these audit trails, which are not provided by the manufacturers who design the intrusion detection system itself. As a result, theses trails may not necessarily support the needs of the intrusion detection system, leading some to conclude that having more effective hostbased systems, "may require the developer to amend the operating system kernel code to generate event information. This approach extracts a cost in performance, which might be unacceptable for customers running computationally greedy applications”

B. Net-Based Systems

Network-based intrusion detection systems offer a different approach. “These systems collect information from the network itself,” rather than from each separate host. They operate essentially based on a “wiretapping concept,” information is collected from the network traffic stream, as data travels on the network segment. The intrusion detection system checks for attacks or irregular behavior by inspecting the contents and header information of all the packets moving across the network. The network sensors come equipped with “attack signatures” that are rules on what will constitute an attack, and most network-based systems allow advanced users to define their own signatures. This offers a way to customize the sensors based on an individual network’s needs and types of usage. The sensors then compare these signatures to the traffic that they capture, this method is also known as packet sniffing, and allows the sensor to identify hostile traffic.

Using network data as a primary source if information is desirable in several ways. To start, running network monitors does not degrade the performance of other programs running over the network. This low performance cost is due to the fact that the monitors only read each packet as they come across its network segment. The operation of the monitors will be transparent to system users, and this is also significant for the intrusion detection system itself. The transparency of the monitors, “decreases the likelihood that an adversary will be able to locate it and nullify its capabilities without significant effort”. This decreased vulnerability strengthens the intrusion detection system, and adds another measure of security. From a financial perspective, network based systems are very desirable. The primary resource for these monitors is storage space, so companies could use older and slower equipment to do this work, rather than purchase additional equipment. This could significantly save on deployment costs.

III. SYSTEM ARCHITECTURE

The classic three-tier model. At database side, we arent able to tell which transaction corresponds to which client query. The communication between Front end Server and the database isn’t divided , and we can understand the relationships between clients and server. If Client 2 is malicious and takes over Web Server, all subsequent database transactions become suspect, as well as response to client. By contrast, according to Fig. 1, Client 2 will only compromise VE 2, and the corresponding database transaction set T2 will be the only changed section of data within database.

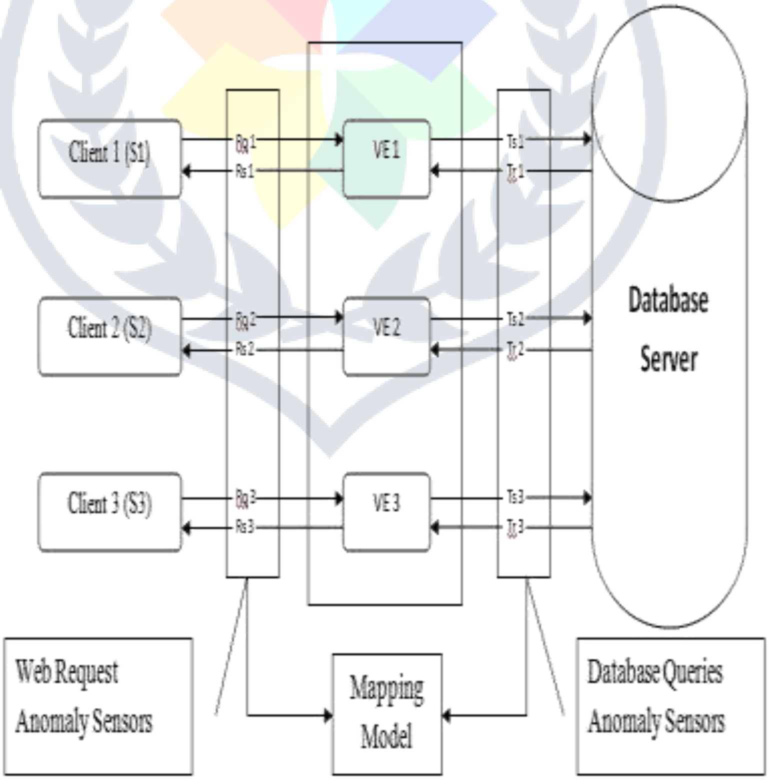

Fig. 1 System Architecture

This container-based and session-altered web servers architecture are not only enhances the security performance but also provides us with an isolated information flows that are seperated in each container session. It allows us to detect the mapping between web server request and the subsequent Database queries, and to utilize such a mapping model to identify non-normal behaviors on a session/client level. In typical three-tiered Web Server Architecture, Web Server receive HTTP query from clients and then issues SQL queries to the database Server to get and update data. These SQL queries are dependent on the web request hitting the Server. We want to model such a causal mapping relationships of all authorised traffic so as to detect non-normal/attack traffic.

Attack Scenarios

Direct DB Attack:

Direct DB Attack means we can directly attack on the database by using various types of queries, to get all access to the database by using queries. By using various queries we can directly go to database and access that directly without having authentication

Injection Attack:

Attacks such as SQL injection don't need compromising Front end Server. Attackers can use existing vulnerabilities in the web server logic to inject the existing data or string content that contains the exploits and then use the web server to relay these exploits to attack the database. An attacker could also have already taken over the web server and be submitting such queries from the web server without sending web requests.

Without matching web requests for such queries, a web server-side IDS could identify neither. Furthermore, if these database queries were within the set of allowed queries, then the database IDS it-self would not identify it either. However, this type of attack can be caught with Double Armor approach.

Privilege Escalation Attack:

This type of attack show how a normal user may use admin queries to obtain such a privileged-information. The attackers log into the web server as a normal user, upgrades their privileges, and triggers admin queries so as to get the administrator's information. Privilege Escalation attack can never be identified by either Web Server IDS or the database IDS

Hijack Future Session Attack:

These attacks show the scenario where in a compromised web server can damage all the Hijacked Future Sessions by not creating any DB queries for the normal user requests. This attack is mainly focused at Web Server-side. An attacker usually takes over the web server and therefore hijacks all subsequent authorized user sessions to launch attacks. For instance, by hijacking other user's session, the attacker can eavesdrop, send spoofed replies, and/or delete user requests

IV. ADVANTAGES

Detects attacks that a network based IDS fail to detect:

Host based systems can detect attacks that network based IDS sensors fail to detect. For example, if an unauthorized user makes changes to system files from the system console, this kind of attack goes unnoticed by the network sensors. So, host based sensors can be very useful in protecting hosts from malicious internal users in addition to protecting systems from external users.

Near real time detection and response:

Although host based IDS does not offer true real-time response, it can come extremely close if implemented correctly. Unlike older systems, which use a process to check the status and content of log files at predefined intervals, many current host-based systems receive an interrupt from the operating system when there is a new log file entry. This new entry can be processed immediately, significantly reducing the time between attack recognition and response.

Does not require additional hardware:

Host based Intrusion detection sensors reside on the host systems. So they do not require any additional hardware for deployment, thus reducing cost of deployment.

Lower entry cost:

Host based IDS sensors are far more cheaper than the network based IDS sensors.

Lower Cost of Ownership:

Network based IDS can be deployed for each network segment. An IDS monitors network traffic destined for all the systems in a network segment. This nullifies the requirement of loading software at different hosts in the network segment. This reduces management overhead, as there is no need to maintain sensor software at the host level.

Easier to deploy:

Network based IDS are easier to deploy as it does not affect existing systems or infrastructure. The network-based IDS systems are Operating system independent. A network based IDS sensor will listen for all the attacks on a network segment regardless of the type of the operating system the target host is running.

REFERENCES

[1] Bace, Rebecca: *An Introduction to Intrusion Detection & Assessment*. Infidel Inc., prepared for ICSA Inc. Copyright 1998

[2] .B. I. A. Barry and H. A. Chan. Syntax, and semantics-based signature database for hybrid intrusion detection systems. *Security and Communication Networks*, 2(6), 2009.

[3] D. Bates, A. Barth, and C. Jackson. Regular expressions considered harmful in client-side xss filters. In *Proceedings of the 19th international conference on World Wide Web*, 2010.

[4] M. Christodorescu and S. Jha. Static analysis of executables to detect malicious patterns.

[5] M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna. Swaddler: An Approach for the Anomaly-based Detection of State Violations in Web Applications. In *RAID 2007*.

[6] H. Debar, M. Dacier, and A. Wespi. Towards a taxonomy of intrusiondetection systems. *Computer Networks*, 31(8), 1999.

[7] V. Felmetsger, L. Cavedon, C. Kruegel, and G. Vigna. Toward Automated Detection of Logic Vulnerabilities in Web Applications. In *Proceedings of the USENIX Security Symposium*, 2010.

[8] Y. Hu and B. Panda. A data mining approach for database intrusion detection. In H. Haddad, A. Omicini, R. L. Wainwright, and L. M. Liebrock, editors, *SAC*. ACM, 2004.