IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 1, January 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001040|

Intrusion Detection and Prevention System for Multitier Web Application

Pulate Kirti Sudhir

Pravra Rural Engineering College, Loni, India

ABSTRACT*:* Internet and online applications have become an unavoidable part of daily life, enabling communication and the management of personal information from anywhere. To accommodate this increase in application and data complexity, web services have moved to a multitier design. Where, the web server runs the application's front-end logic and data is outsourced to the database or file server. We present an Intrusion Detection and Prevention System that models the network behavior of user sessions across both the front-end webserver and the back-end database. By monitoring both web and subsequent database requests, the proposed system is able to search out attacks that any other application may not be able to identify. The IDPS application will be implemented using Apache web server and MySQL. The IDPS system is executed to expose a wide range of attacks with maximum accuracy while maintaining minimal flaws.

KEYWORDS: Intrusion Detection System, Apache web server, MySQL.

I. INTRODUCTION

Multitier Web Application: In computing, a web application or web app is a client server software application in which the client (or user interface) runs in a web browser. A multi-tier application is any application developed and distributed among more than one layer. It logically separates the different application-specific, operational layers. The number of layers vary by business and application requirements, but two-tier is the most commonly used application. A multi-tier application is also known as n-tier application.

Intrusion: Intrusion is an attempt to compromise the confidentiality, integrity, availability or to bypass the security mechanisms of a computer system or network. An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system. This person attempts to violate Security by interfering with system Availability, data Integrity or data Confidentiality.

Intrusion Detection and Prevention System: Intrusion Detection and Prevention System is primarily focused on identifying possible incidents, logging information about intruders, attempting to stop them, and reporting to security administrators. Intrusion-detection systems aim at detecting attacks against computer systems and networks or, in general, against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization.

Need of IDPS:

History and Development: Data Security has been a most prior issue ever since the assessment of computers and their applications. According to study, intrusion detection has been live field of research and development about more than four decades now. It begins from 1980 with the publication of John Anderson's "Computer Security threat monitoring and surveillance". It is the starting research paper on this area. Dorothy Denning's seminal paper, "An Intrusion Detection Model" published in 1987 provided the information about rules framework. After that, for the past three decades, improvement in this research and huge commercial investments, intrusion detection technology is not under developed and ineffective. In the beginning days of computers, hackers rarely used automated tools to attack into system. It needed high level of expert and they followed their own new techniques to perform malicious actions. A number of intrusion tools and software are present today those can be used to exploit scripts according to known vulnerabilities. Figure-1 describes the relation between the relative experience of attack and attackers from 1980 to present. Before the development of new intrusion detection systems, intrusion detection consisted of a manual detection of anomalies. Due to the availability of huge processing speed, "real-time" detection has now become possible and gives trigger alerts to the administrator if intrusions were detected. Due to the huge amount of financial losses, problem of the computer downtime, reputation damage or even personal data being affected, now-a-days the demand for not

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001040 |

only being alerted in the occurred event of an attack but also to prevent the attack has become an absolute necessity. Especially with the begin of Probing, User to Root Attacks, Remote to User Attacks and Denial of Service attacks, the market needs have grown stronger and stronger for Intrusion Detection and Prevention Systems (IDPS) rather than mere intrusion detection.

Comparison with Firewalls: Though they both relate to network security, an IDS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators. A system that terminates connections is called an intrusion prevention system, and is another form of an application layer firewall.

IDPS Features
Lower Cost of Ownership

- Easy to deploy.
- Efficient use of Pattern Matching Algorithm.

Lower Cost of Ownership: The proposed based IDPS is network based. An IDPS 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 software at the host level.

Easy to deploy: Network based IDPS are easier to deploy as it does not affect existing systems or infrastructure.
The network-based IDPS systems are Operating system independent. A network based IDPS sensor will listen for all the attacks on a network segment regardless of the type of the operating system the target host is running. Server on which Application resides is a separate one from the server where IDPS resides, hence it won't affect the speed of the application. The control logic in the host controller selects the web server to satisfy the web requests. Hence selection of a web server with minimal pending requests can be made and hence processing of the system speeds up. A separate log file is maintained with the intrusion details, the type of attack, culprit's IP address, date and time of the attack for future references.

Efficient Use of Pattern Matching Algorithm: String matching algorithms in software applications like virus scanners or intrusion detection systems are commonly used for improving data security over the internet. String matching is a technique to find out a pattern from given text. String-matching techniques are used for sequence analysis. Let P = p1, p2, ..., pm be a set of patterns, which are strings of characters from affixed alphabet. Let T =t1, t2, ..., tn be a large text, again consisting of characters from the above alphabet. The problem is to find all occurrences of all the patterns of P in T. Given a pattern set P and a text T, report all occurrences of all the patterns in the text. The text T is a string of n characters drawn from the alphabet. The pattern set P is a set of m patterns each of which is a string of characters over the alphabet. For simplicity we assume that all patterns have the same length m.

II. SYSTEM ARCHITECTURE

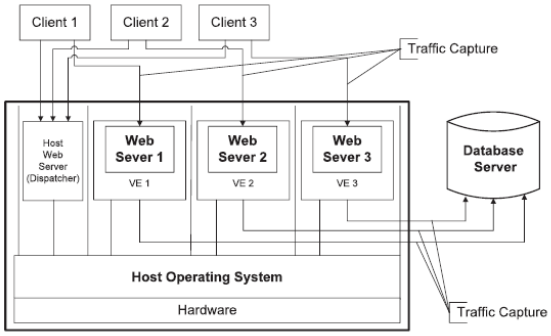
Basic Component of System:

- Web Server
- Dispatcher
- Database Server
- Host Operating System

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001040 |



Basic Component of System

- Web Server
- Dispatcher
- Database Server
- Host Operating System

Web Server: A web server is a program that use HTTP (Hyper Text Transfer Protocol) to server the _les that form web pages to user, in response to their requests, which are forwarded by their computer's HTTP client. Dedicated computers and application may be referred as a web server as well.
Dispatcher: A Dispatcher enables client processes to share a limited number of server processes .It is possible to create multiple dispatcher processes for a single database instance. The optimum number of dispatcher depending on the operating system limitation and the number of connections for each process.
Database Server: Database server is a computer program that provides database services to the computer programs or to computers, as defined by the client server model .User access a database server either through a "front end" running on the user's computer or through the "back end" which runs on server.
Host Operating System: A host operating system is the software installed on a computer that interacts with the underlying hardware and is usually used to describe an operating system used in a virtualized server to differentiate it from the guest operating system.

ATTACK SCENARIO

Provide a secure way to implement web application to prevent below attacks:

- Privilege Escalation Attack.
- Session Hijack Attack.
- SQL Injection Attack.
- Session Hijack Attack.
- Denial of Service Attack.

[A] Privilege Escalation Attack:

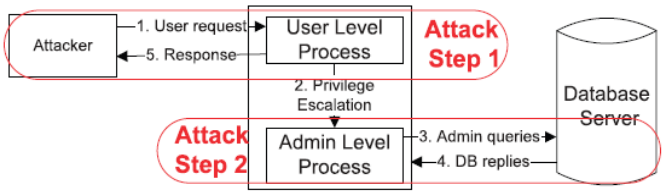
The attacker logs into the web server as a normal user, upgrades his/her privileges, and triggers admin queries so as to obtain unprivileged access.

This attack can never be detected by either the web server or the database server since both requested user and triggered query are legitimate requests and queries. Let us assume that the website serves both regular users and administrators. For a regular user, the web request ru will trigger the set of SQL queries Qu for an administrator, the request ra will trigger the set of admin level queries Qa. Now suppose that an attacker logs into the web server as a normal user, upgrades his/her privileges, and triggers admin queries so as to obtain an administrators data. This attack can never be detected by either the web server IDS or the database IDS since both ru and Qa are legitimate requests and queries. Our approach, however, can detect this type of attack since the DB query Qa does not match the request ru, according to our mapping model.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

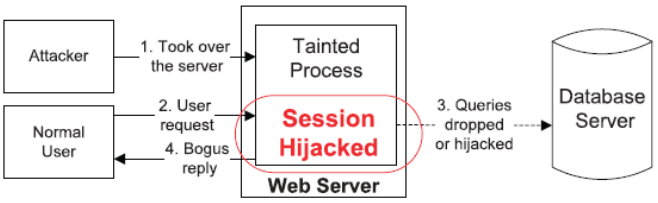
|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001040 |



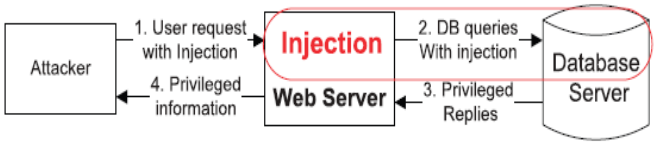
[B] Session Hijack Attack:

The attacker usually takes over the web server and therefore hijacks all subsequent legitimate user sessions to launch attacks. This attack is launched by making fake access point. Attacker can eavesdrop, send spoofed replies, and/or drop user requests. Session-hijacking attack can be further categorized as a Spoofing/Man- in-the-Middle attack, a Denial-of-Service/Packet Drop attack, or a Replay attack .This class of attacks is mainly aimed at the web server side. An attacker usually takes over the web server and therefore hijacks all subsequent legitimate user sessions to launch attacks. For instance, by hijacking other user sessions, the attacker can eavesdrop, send spoofed replies, and/or drop user requests. A session-hijacking attack can be further categorized as a Spoofing/Man-in-the-Middle attack a Denial-of-Service/Packet Drop attack or a Replay attack.



[C] SQL Injection Attack:

Attacks such as SQL injection do not require compromising the web server. Attackers can use existing vulnerabilities in the web server logic to inject the SQL query or string content that contains the exploits and then use the web server to relay these exploits to attack the back-end database .Attacks such as SQL injection do not require compromising the web server. Attackers can use existing vulnerabilities in the web server logic to inject the data or string content that contains the exploits and then use the web server to relay these exploits to attack the back-end database. Since our approach provides a two-tier detection, even if the exploits are accepted by the web server, the relayed contents to the DB server would not be able to take on the expected structure for the given web server request. For instance, since the SQL injection attack changes the structure of the SQL queries, even if the injected data were to go through the web server side, it would generate SQL queries in a different structure that could be detected as a deviation from the SQL query structure that would normally follow such a web request.



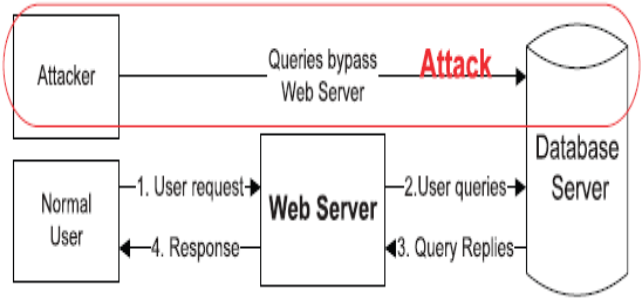
[D] Direct DB Attack:

The attacker is able to bypass the web server or firewalls and connect directly to 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. It is possible for an attacker to bypass the web server or firewalls and connect directly to the database. An attacker could also have already taken over the web server and be submitting such queries from the web server without sending efforts for the attackers to launch successful attacks. In addition, users with non admin permissions can cause minimal (and sometimes zero) damage to the rest of the system and therefore they have limited incentives to launch such attacks.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

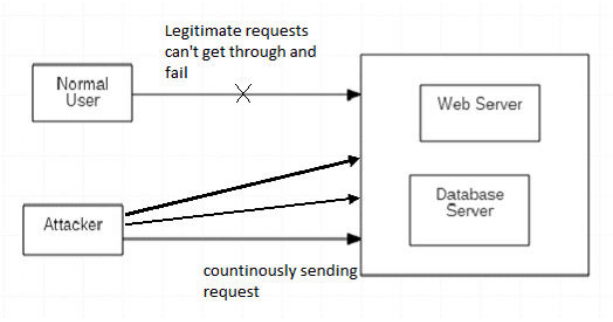
|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001040 |



[E] Denial of Service Attack

It is an attempt to make a machine or network resource unavailable to its intended users .In this case, the attacker gains access to a private resource and sends tremendous requests to it making the resource too busy or crash it in order to make it unavailable to legitimate user .The application is designed in such way that no user will have direct access to database server .It is possible for an attacker to bypass the web server or firewalls and connect directly to 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 matched web requests for such queries, a web server IDS could detect neither. Furthermore, if these DB queries were within the set of allowed queries, then the database IDS it would not detect it either.



III. ATTACK DETECTION

I. Privilege Escalation Attack

This type of attack is actually done by accessing privilege of authorized user by an unauthorized users. Suppose there is an application for the Payment System for Employee's in which Administrator have privilege to update and change the salary of the employee and employee have privilege to see their attendance. If any employee gets the URL to update the salary then he/she gets the access of all the employee salary. In case, the attacker employee will get the privilege of the admin and privilege escalation attack is done.

If the Payment System uses the IDPS application then it will be placed after the IDPS. IDPS will store the admin privilege and employee privilege separately in the IDPS database. Whenever the admin or employee want to use the Payment System application then they has to go from IDPS's privilege authentication where according to the user i.e. admin or employee and its privilege the IDPS application will take to their respective privilege pages according to the user register privileges in the IDPS database. IDPS will never show the URL of the respective application database. In this way, IDPS will prevent privilege attack.

II. Hijack Future Session Attack:

Whenever we use the internet services or application through web browser, it generates a unique session ID and it remains until or task is not completed or web browser is closed. Attacker tries to get this session ID. So that attacker can get the valuable data and it's most common examples are FACEBOOK, GMAIL etc. After getting session ID the attacker can do anything he wants with the user data. But the original user doesn't know that attacker is accessing his/her data which would turn harmful for the user.

If the user uses the IDPS application he will be prevented from such kind of attack. In our application, we are making the Mapping Model for the session ID and IP address. If the attacker will be able to get the session ID then also it will not possible to him/her to attack the user data because the IP address of the attacker will not match with our

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001040 |

IDPS's Mapping Model. IDPS will allow the access if the session ID and IP address are match according to the mapping model of application database. Depending upon the result of the IDPS it will decide the user is legal or not and allow him/her access the database or not.

III. Injection Attack

Now-a-days the attackers are using the SQL queries to get the data or change the data of another user by sending queries like INSERT, UPDATE, DELETE, etc. In this kind of attack, the attacker communicate with the database by sending queries. But whiles ending the SQL queries by an attacker the structure of the queries are changed and which are never detected by the IDS. But, the IDPS application is able to prevent the injection attack because the IDPS will generate its own structure queries and which are different from the attacker SQL queries structure. IDPS will allows to access, update the database if structure of the SQL queries are matched with the structure of the IDPS application query structure.

IV. Direct DB Attack

Most of the attackers directly attack the database server besides going to the web server. In this kind of attacking, the attacker uses the IP address of the database server. It is very easy and less time requirement attack. In this attacker sends the SQL queries directly to the database server by bypassing the web server. If the IDPS is used then the attack will be detected and attacker will not be allowed to the database server. If IDPS is used then it will be placed before the web server and the database server. So that, IDPS will be able to hide the IP address and location where the database server is located and IDPS doesn't match the web request with the SQL queries. Thus IDPS can avoid such kind of attacks.

IV. SYSTEM DESIGN

Application is designed in such way no user will have direct access to database server as well as application server on which web application is hosted. All request will be processed from Server 1s Servlet Filter, it will take care of session validation and session tracking. Then control goes to dispatcher Servlet which will take care of dispatching re appropriate service. Database server will be accessible only to Server 2 and Server 3 where actual web application is hosted

Hardware

We will be using 3 workstations with the control logic residing on one of them. These workstations will form a will be connected with the help of a router.

Software

Multiple Web servers are required to speed up provision of. An application dependent database server and a separate Web server that will execute the control logic of the system.

V.PERFORMANCE

Server on which Application resides is a separate one from the server where IDPS resides; hence it won't affect the speed of the application. The control logic in the host controller selects the web server to satisfy the web requests. Hence selection of a web server with minimal pending requests can be made and hence processing of the system speeds up.

VI. SECUIRITY

In our System, we are storing the vital information about the application (for which the system will work) in encrypted and secure format. Also the admin details will be safely stored. And as the system itself works for the security this information will not be easily accessible according to our architecture.

VII. CONCLUSION

We conclude that an Intrusion Detection and Prevention System represents the normal behavior of multitier web applications from both front-end web (HTTP) requests and back-end database (SQL) queries. Unlike previous approaches that correlated or summarized alerts generated by independent IDPSs, This system forms a container-based IDPS with multiple input streams to produce alerts.

We have shown that such correlation of input streams provides a better characterization of the system for anomaly detection because the intrusion sensor has a more precise normality model that detects a wider range of

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001040 |

threats. We achieved this by isolating the flow of information from each web server session with a lightweight virtualization. Furthermore, we quantified the detection accuracy of our approach when

We attempted to model static and dynamic web requests with the back-end file system and database queries.

REFERENCES

1. Willaim Stallings, "Computer Security: Principles and Practices", Pearson Ed. ISBN: 978-81-317-3351-6
2. F. Valeur, G. Vigna, C. Kru gel, and R. A. Kemmerer, "A Comprehensive Approach to Intrusion Detection Alert Correlation" IEEE Trans. Dependable and Secure Computing, vol. 1, no. 3, pp. 146-169, July-Sept. 2004.
3. Http://www.dummies.com/how-to/content/examining-dierenttypes-of-intrusion-detections.html
4. M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna, "An Approach for the Anomaly-Based Detection of State Violations in Web Applications", Recent Advances in IDS, 2007.
5. Karen scarfone, Petermell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", NIST
6. http://www.omnisecu.com/security/infrastructure-and-email-security/types-of-intrusion- detection-systems.php
7. J. P. Anderson. Computer Security Threat Monitoring and Surveillance. Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980
8. Kai Hwang, Min Cai, Ying Chen, and Min Qin, Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes, IEEE transactions on dependable and secure computing, vol.4, no.1, Jan-Mar 2007.
9. Swaddler: An Approach for the Anomaly-based Detection of State Violations in Web Applications Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni Vigna Department of Computer Science, University of California Santa Barbara Santa Barbara, CA 93106-5110, USA marco,balzarot,rusvika,vigna@cs.ucsb.edu

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details