ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Defence Architecture for Various Networks Attacks

Prerna U. Randive

Student, Dept. of Computer, AISSMS COE, Savitribai Phule Pune University, Pune, India

ABSTRACT: now a day almost all the work is done with the help of Internet. So, Internet is relevant and crucial part of daily life, such as social networking, online banking, online shopping, to make able communication and managing the personal and corporate data. Due to raise in web services and data complexity, the web services now have moved to multi-tier design. With this high use of web application networks attacks grown with hazardous purpose. DoubleGuard, Intrusion Detection System helps to detect and prevent networks attacks. The IDS system, which is stipulate the networks behavior of user sessions around the front-end web server and back-end database. The existing system DoubleGuard, it is able to discover attacks after examining web requests and database requests. In this paper, adding one more level that is admin, it is cause for the training to the system, log generation, blacklist. So such IDS system causes to be present security to prevent both the web and database server.

KEYWORDS*:* DoubleGuard; Web Application; Multitier; IDS; Attacks

I. INTRODUCTION

On account of vast growth of internet, utility of internet is grown day by day. So web service's popularity and complexity have been growing around the world. Internet is helped in different daily requirement such as online banking, social networking, online reading newspaper, online shopping, and can manage personal and corporate data and to make able communication. Such kind of web services are accessed on web to run the application user interface logic at front-end side and at the back-end side, database server provides to place database or files [13]. Due to high use of web services, it used to place personal and corporate data. Because of this, it has been targeted for the hazardous purpose. By moving attention from attacking to front-end to take benefit of vulnerabilities of the web application to violet the back-end database system by the help of SQL injection attack. So, security of web application can achieved through the good design of web application. To build system more secure, make use of many anticipating system such as Intrusion Detection System and Firewall.

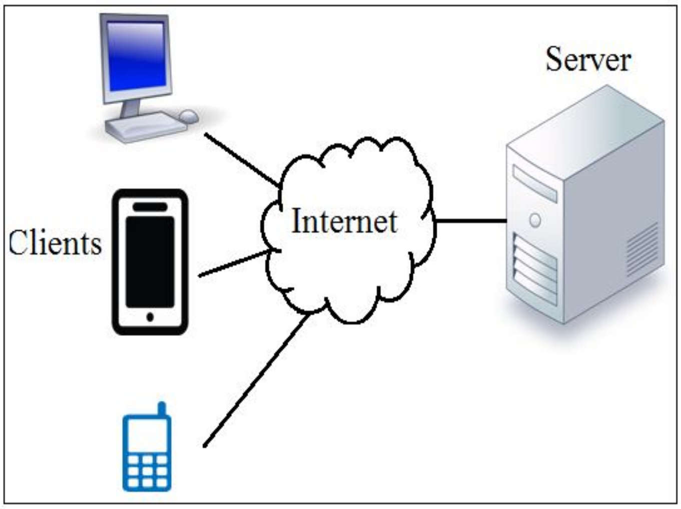

Fig.1. Client Server Architecture

In above figure, it shows client server communication. Client sends request for obtaining response from server. After receiving request, server generates responses and make responses relies on request. So, Attacker targets the front-end and the back-end for harmful purpose.

A. *Intrusion Detection System*

Intrusion Detection System (IDS) is a system created to search out attacks against computer networks and information system. It also awakes to the web application for any type of harmful activity.

IDS uses as a software / hardware device to prevent from harmful activity.[12] It helps to search known attacks by observing matching misused traffic patterns or signatures. By using some machine learning algorithms, IDS can detect unknown attacks. Within given interval training phase abnormal network traffic can be discovered. Such kind of intrusion detection system can find out only known attack when attacker makes use of abnormal traffic. IDS cannot detect attack when attacker makes use of normal traffic. The purpose of the web IDS is to see typical user login traffic and the database IDS see normal traffic of a authenticate user. When database IDS can search that a privileged request from the web server is not connected with user privileged access, then such kind of attack can be easily discovered by IDS. Following are some of the advantages to effectiveness in IDS.

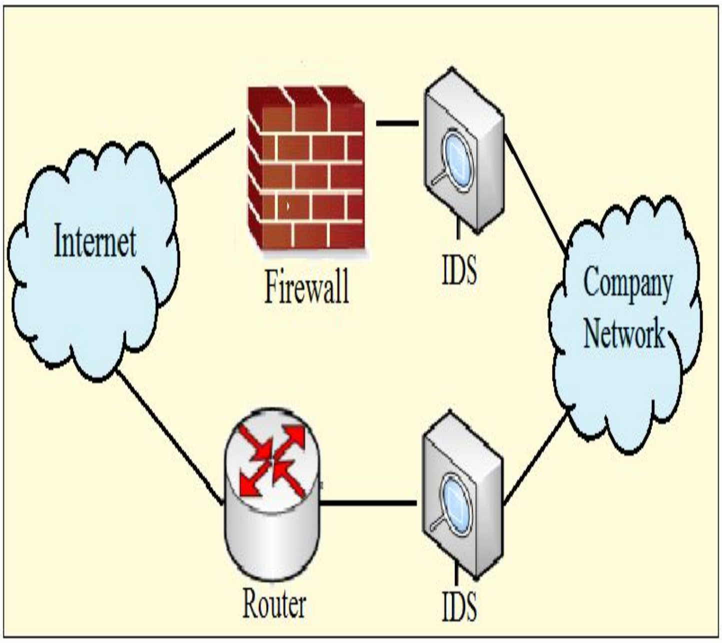

Fig.2. Simple Intrusion Detection System

1. Benefits of Intrusion Detection System:
   - Accuracy of attack detection: Accuracy of intrusion detection system is depending on identification of attack and it is based on mismatch types and signature. In multi-tier web application, it uses IDS and database IDS to find out such attacks.
   - It is easy to deploy: Intrusion Detection System is easier to deploy due to it does not affect existing system or infrasture.
   - Timeliness of attack detection: IDS performs its analysis of server as early as possible, so that security officer can take action before more damage has been happened. It can be also prevent attacker from defeating the audit source and IDS itself.
   - Performance of IDS: The performance of IDS is depends upon the rate at which audit events are processed. If performance is well then it can also be used to find out real-time attacks.

B. *Attack Scenarios*

There are several kinds of attacks on web and database server; this approach can detect the following attacks.

- SQL Injection Attacks: Such kinds of attack only happened on the database server. attacker make use of weak points in web server to inject the database. SQL injection attacks can allows unauthorized access to back-end database. Attacker makes SQL query with the malicious contents. Further that query is treated like input, by this attack attacker can change information from database, or he can extract information from the database.

- Direct DB Attack: It does possible for the attacker to bypass the web server as well as firewalls and make connection directly with database. In this kind of attack, without making any kind of web request, an attacker can taken control over web server and submit harmful query from web server without matching the web requests. For such query, web server IDS and database IDS cannot detect such kind of attack.
- Denial of Service Attacks: The denial of service attacks, which is predetermined attempts to halt or make barrier for legitimate users from using a specific network resource.

II. LITERATURE SURVEY

There are various techniques, which helps to find and protect from vulnerabilities and hazardous activity. From such techniques, web application program can improve them to reduce vulnerability and malicious actions. Some techniques are mentioned below.

DoubleGuard [1], is one kind of intrusion detection system which is used to build models of normal behaviour for the multi-tiered web applications from front-end web (HTTP) request and back-end database (SQL) query. DoubleGuard composes container-based IDS with the multiple input streams for alert creation and generation. It is happened by monitoring web and consequent database requests, it can find out attacks. Using DoubleGuard, it can be expose and detect wide range of multiple attacks with 100 percent accuracy.

A.S. Gadgikar has mentioned negative tainting approach [2]. It is helped to prevention from SQL injection attacks without change in existing code. It can used to reduce time and space complexity. Negative tainting approach has advantages like it does not require any type of expensive hardware and it can work with any kind of database like oracle, SQL etc. This technique includes detection of weak spot from web application, further it inserts the newly identified SQL injection attacks to improve the accuracy of the system.

Swaddler: An Approach [3] suggested by authors. Swaddler is used to detection of attacks against web applications, which are depend upon the analysis of the internal application state. In web application, Swaddler firstly models values of session variables in association with the critical execution points. Authors also mentioned novel detection model which relies on multi variable invariants to detect web-based attacks. It also developed a prototype of system for the PHP language and calculates it against different real world applications. Attack identification is made by leveraging the internal that is hidden state of a web application.

Mihai Christodorescu Somesh Jha has proposed Static Analysis to Detect Malicious Patterns [4] presents a unique view on malicious code detection. Authors regard malicious code explosion, as obfuscation deobfuscation game between the malicious code writers and researchers evaluating on malicious code detection. Malicious codes writers try to obfuscate the malicious code for the subversion of malicious kind of code identifiers, like as antivirus application software. Authors perform resilience of the three commercial virus scanners against to code-obfuscation malicious activity. Result is the virus scanners can be subverted by a simple obfuscation transformation. It also modelled architecture for identification of malicious patterns in executables that are resilient to common obfuscation transformation.

Nidhi Srivastav Rama Krishna Challa mentioned Novel Intrusion Detection System [5]. In this paper, they have presented layered framework integrated with neural network. This system has evaluated with Knowledge Discovery & Data Mining 1999 dataset. The built system has much high attack detection accuracy and less false alarm rate.

Evaluation of Web Security Mechanisms [6] suggested by José Fonseca, Marco Vieira, Henrique Madeira. Authors suggested a technique and the prototype tool to evaluate web application for security mechanisms. Authors also present implementation of Vulnerability & Attack Injector Tool (VAIT) that permits the automation of whole process. This tool is performed to run the group of experiments that demonstrate the feasibility and effectiveness of the suggested technique. The injection of the vulnerabilities and attacks is the good way to compute the security mechanisms and to point out both their weakness and improvement.

TDFA technique is developed [7]. TDFA is having of three main components that are Detection, Traceback, and Traffic Control. In this method, the purpose is to keep packet filtering as near to the attack source. By doing this, the traffic control component at the victim side aims to put up limit on packet forwarding rate to victim. This kind of technique used to reduce the rate of forwarding the attack packets and thus improves the throughput of legitimate traffic. So TDFA performed to reduce the attack traffic for the prevention the quality of service for the legitimate traffic.

III. PROPOSED ARCHITECTURE

The main aim is efficiently detection of intrusion to protect multi-tier web application. The objective is to prevent and detect attacks by using Artificial Neural Network and adds one more level that maintains log. It consists of blacklist that keep list of attacker system's IP address, which should get block. In this way, some modification will be do in existing DoubleGuard to increase its reliability, performance in case of static and dynamic web sites both.

As shown in figure, firstly client sends request to the server for this purpose it generate request. Further client sends request to the server and wait for the response from server. At the server side server firstly accept the request and process that request. For this request, server arranges particular session for each client request after the arrangement, it process that session. If it consists of malicious content in the request then server deny that request. Such kind of attack is DDoS attack. This generally happened on the web server. Distributed Denial of Service attack (DDoS) occurs when large numbers of compromised systems attack a single machine. Due to the effect of DDoS attack, network resources are being unavailable to its intended users. Further, if the accepted request is safe then it proceed and generate query and process query. If the query is consisting of malicious contents then it denied that query. Because this is SQL injection attacks. Such kind of attack happened on the database server. From this attack, attacker can modify database, can extract information from database. If the query is safe then it connects to the database and generates the result with the help of the database server and gives feedback to the client as the response.

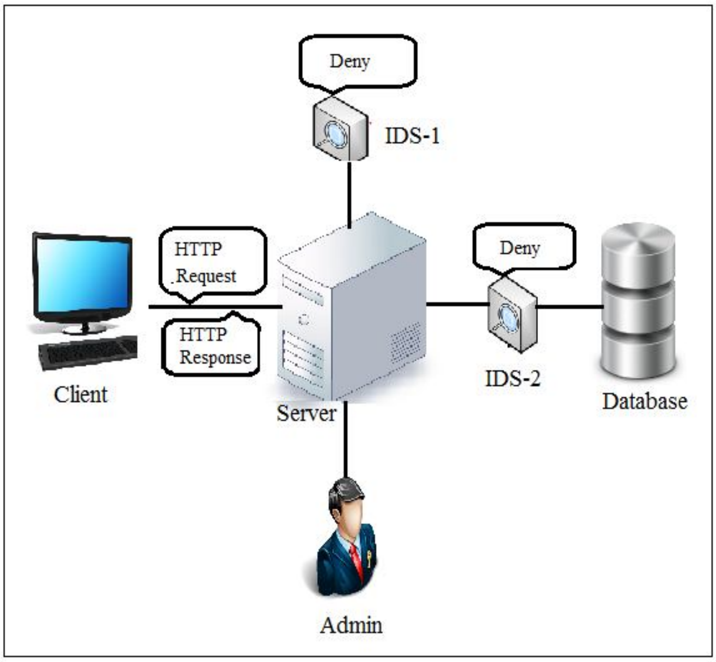

Fig.3. Proposed Architecture

Along with the detection and prevention from attack, proposed system architecture consists of admin log at server side. This log consists of different parameters that keep information regarding attacks, IP address of attacker system, time of the request and difference of request. By keeping this information it can blacklist that particular request and machine also. So this log is very helpful to maintain history. Further, attacker cannot send any type of request with same system to the web server or database server. Finally it will able to expose or detect a wide range of multiple attacks with high accuracy.

For the training of system, Artificial Neural Network algorithm have used. The steps of algorithm is as follows,

- First apply the inputs to network and work-out the output.
- Next, work-out error for neuron B.
  $\text{Error}_B = \text{Output}_B\ (1\text{-Output}_B)\ (\text{Target}_B - \text{Output}_B)$ (1)
- Change the weight and let W^+_{AB} be new weight and W_{AB} be the initial weight.
  $W^+_{AB} = W_{AB} + (\text{Error}_B \text{ x } \text{Output}_A)$ (2)
- Calculate the Errors for the hidden layer neurons.
  $\text{Error}_A\text{=Output}_A(1 - \text{Output}_A)(\text{Error}_B\, W_{AB} + \text{Error}_C\, W_{AC})$ (3)
- By obtained Error for the hidden layer neurons, then proceed as in step 3 to change the hidden layer weights. By repeating this, we can train a network of any number of layers.

IV. Results

Firstly apply different possible attacks on IDS. This is expected that IDS is able to detect front-end attack that is DDos attack and back-end attack that is SQL injection attacks. Along with this, admin is responsible for the training to the system and log generation. The admin log will blacklist the malicious request of the attacker system. Further no any request of attacker will accepted by server.

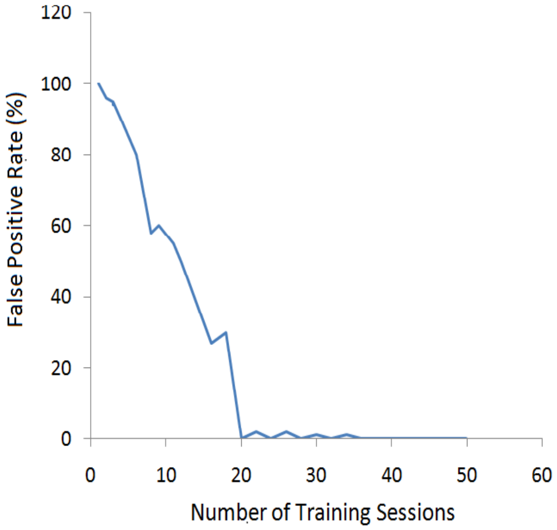

Fig.4 False Positives vs. Training Time in Static Website

As shown in above figure, it shows false positives vs. training time in static website as well as it shows the training process. As the number of training session increased the rate of false positive is decreased. Which means that model became more accurate. After more training session the false positive rate decreased and finally it stayed at 0.

DOI: 10.15680/ijircce.2015. 0307109

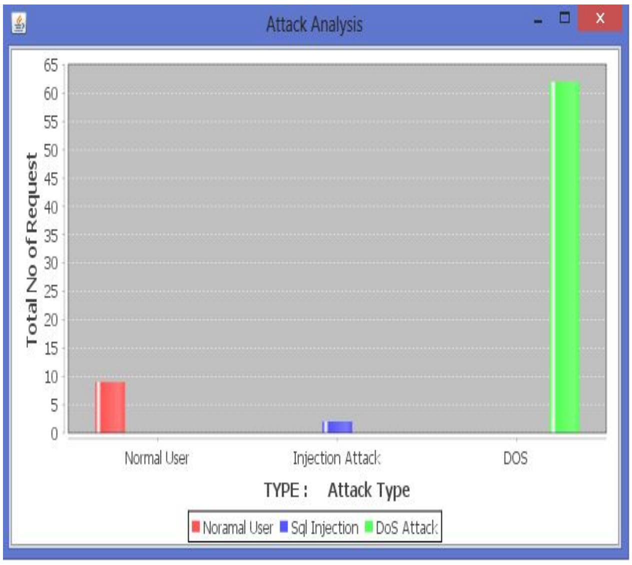

Fig.5. Attack Analysis

The above figure it shows attack analysis. In this it consist of number of request and attack types. The graph shows number of attacks happens till now, it shows normal user, SQL injection attack and DDoS attack attacks happened on the system.

V. CONCLUSION

The presented IDS have presented models of normal behaviour for the multi-tier web applications from front-end and back-end requests. Unlike prior techniques, this correlated alerts produce by independent IDS. So this approach produces a container based IDS by the help of multiple input streams for making alerts. For this reason wider range of attacks can be discovered by intrusion sensor. This happens because of separating flow of information from each web server session with a light weighted virtualization. Along with this admin log used to blacklist the malicious request. Due to such blacklist the upcoming request from attacker system get stopped. So, such Intrusion Detection System is able to detect the wide range of various networks attacks with minimal false positive. The number of false positives relies on size and coverage of training sessions took place.

REFERENCES

1. Meixing Le, Angelos Stavrou, and Brent ByungHoon Kang, "DoubleGuard: Detecting Intrusions in Multitier Web Applications," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 4, July/August 2012.
2. A.S. Gadgikar, "Preventing SQL Injection Attacks Using Negative Tainting Approach," 2013 IEEE International Conference on Computational Intelligence and Computing Research, 978-1-4799-1597-2/13/$31.00 ©2013 IEEE.
3. Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni Vigna, "Swaddler: An Approach for the Anomaly-based Detection of State Violations in Web Applications".
4. Nidhi Srivastav, Rama Krishna Challa, "Novel Intrusion Detection System integrating Layered Framework with Neural Network," 2013 3rd IEEE International Advance Computing Conference (IACC), 978-1-4673-4529-3/12/$31.00_c 2012 IEEE.
5. Jose Fonseca, Marco Vieira, Henrique Madeira, "Evaluation of Web Security Mechanisms using Vulnerability & Attack Injection," IEEE Transactions on Dependable and Secure Computing.
6. Vahid Aghaei Foroushani A. Nur Zincir-Heywood, "TDFA: Traceback-based Defense against DDoS Flooding Attacks," 2014 IEEE 28th International Conference on Advanced Information Networking and Applications.
7. H. Debar, M. Dacier, and A. Wespi, "Towards Taxonomy of Intrusion-Detection Systems," Computer Networks, vol. 31, no. 9, pp. 805-822, 1999.
8. Muthu Kumara Raja, Bala Sujitha.T.V, "Intrusion Detection System in Web Services," International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 2, February 2013.

9. Lwin Khin Shar, Hee Beng Kuan Tan, “Defeating SQL Injection,” Published by the IEEE Computer Society.

10. Narmadha.S, Deepak Lakshmi Narashima, “Multilayer Intrusion Detection System in Web Application Based Services,” Narmadha.S et al. / International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013.

11. K.Karthika, K.Sripriyadevi, “To Detect Intrusions in Multitier Web Applications by using Double Guard Approach,” International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013 ISSN 2229-5518.

12. Bogadhi Swetha, A .Kalyan Kumar, “Detection of Intrusion in Multitier Web Application: A Perspective View,” International Journal of Computers Electrical and Advanced Communications Engineering Vol.1 (3), ISSN: 2250-3129..