Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.21 – 26

RESEARCH ARTICLE

Testing PHP Website for Possible Attacks Using Honeypot

Nachiket Save, Kunal Yadav, Sonali Pawar, Shamili Kumar, Abhay E. Patil

Department of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai India
nachiketsave92@gmail.com, ku34naly@gmail.com, shonalipawar22@gmail.com, shamili275.sk@gmail.com, abhay.patil@mctrgit.ac.in

***Abstract*: Today security of web based applications is a matter of high concern amongst all enterprises. Here we propose a system based on the concept of intrusion detection which will track the trends of attacks on the system and will serve for development of a system immune to the same.**
Today such systems are very expensive we propose an inexpensive approach to the same which will be very helpful for small website owners who find it a drain on resources to buy the expensive software. The signatures of known attacks are stored. It will attack user activity on the web page on which the proposed system is deployed, it will perform pattern matching and give the result. Also a honeypot system is deployed which will fetch complete details of attacker/user i.e.: I.P address, browser type, details entered.

Keywords: Honeypot, Attacks, Intrusion Detection, Threat, inexpensive, pattern matching.

I. INTRODUCTION

Honey-pots are closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion. Using honey-pots provides a cost-effective solution to increase the security posture of an organization. Even though it is not a panacea for security breaches, it is useful as a tool for network forensics and intrusion detection. Nowadays, they are also being extensively used by the research community to study issues in network security, such as Internet worms, spam control, Denial of Service attacks, etc. In this paper, we advocate the use of honey-pots as an effective educational tool to study issues in network security. We support this claim by demonstrating a set of projects that we have carried out in a Websites, which we have deployed specifically for running various web applications' under supervision . The design of our projects tackles the challenges in installing a honey-pot in organizational website, thus determining various security compromises that are performed on it over the Internet by attackers/hackers. In addition to a classification of honey-pots, we present a framework for designing projects for web application security courses.

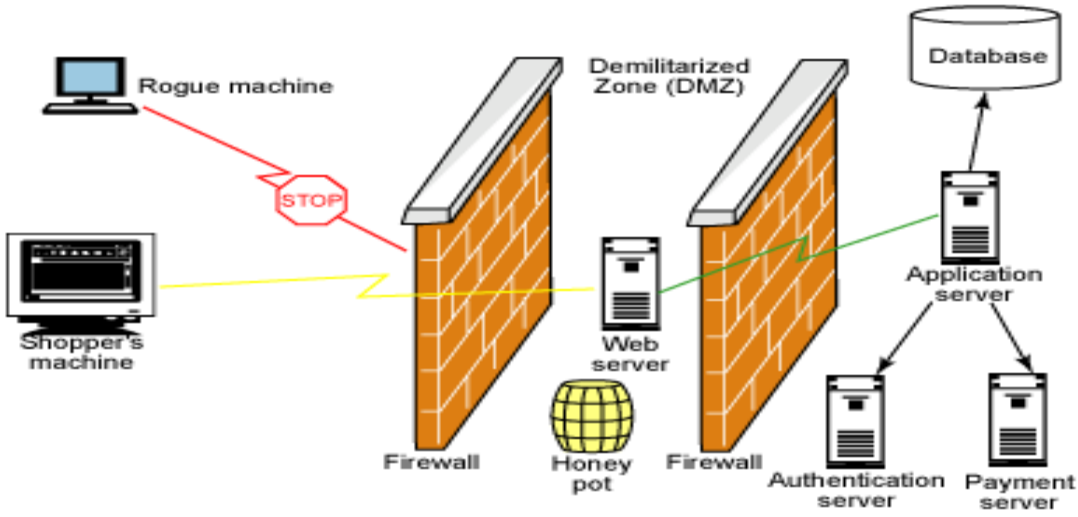

Fig1: Honeypot System

II. ENTERPRISE OBJECTIVES

Our project acts as a service provider for Honey-pot Security to various websites. It acts as a framework to implement honey-pot which can be used by any organization to test their website applications / portals. Our clients would consist of websites of PHP format.

We plan to trace characteristics of hackers like

- The browser they are using
- Their IP address from the IP header
- Files accessed by the user.
- The loopholes they discover
- Various inputs that are used for various input fields.
- Script Injection.

III. SCOPE OF THE SYSTEM

The system will be focussing on the following,

- This system will be focusing on server side programming language specifically PHP which are mainly used for development of CMS – content management systems, e – commerce, social networking site, etc.

- The system acts as a Service Provider for Honey-pot security to various websites.

- The system is proposed to trace the user activities on the client site – demo websites.

- Various attacks performed on the demo sites will be traced within the tool. Thus providing a competitive analytical & statistical data so as to find the loop holes of the demo sites.

- This system can be deployed at on the same server as in where the demo website is located or can also work with remote web server

- This system will be using PHP, JavaScript, & my SQL. Our main aim is to emphasize more on the LAMP framework – LINUX – APACHE-MY SQL-PHP

With a user-friendly environment, it will diminish the problem of reading long and unstructured log files and efficiently captures what has happened inside the virtual honey-pots.

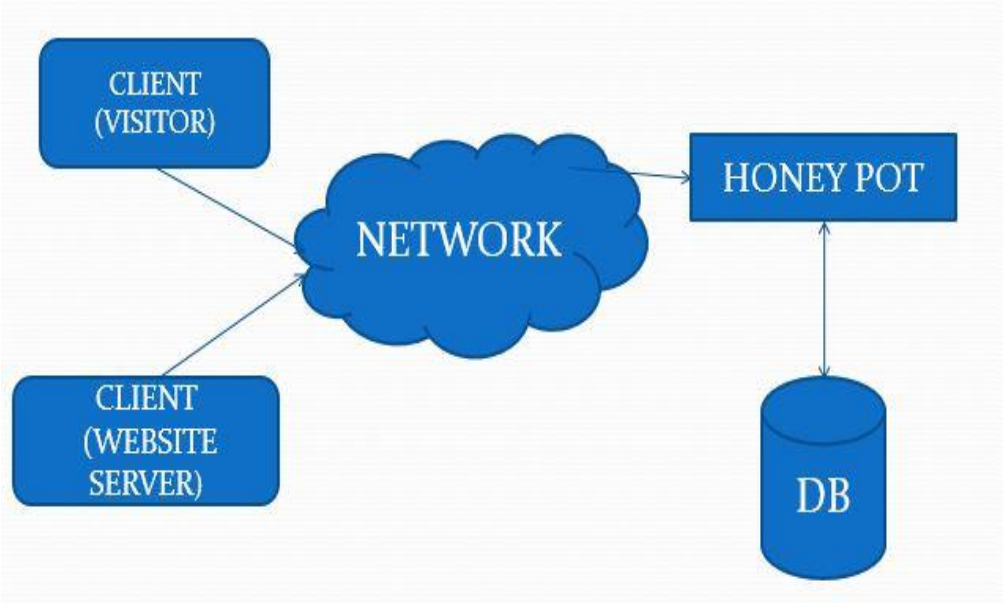

Fig2. Proposed System Architecture

IV. METHODOLOGY

We will be tracing the entire request made by the client to the server from the demo site. All the GET-POST values sent & received from the client will be logged in to the Honey-pot database for analysis purpose.

We will broadly use the G-P-S-C [GET POST SERVER COOKIES] data variables which are sent & received from the client to the server.

There are two ways the browser client can send information to the web server.

- The GET Method
- The POST Method

Before the browser sends the information, it encodes it using a scheme called URL encoding. In this scheme, name/value pairs are joined with equal signs and different pairs are separated by the ampersand.

Example: name1=value1&name2=value2&name3=value3

Spaces are removed and replaced with the + character and any other no alphanumeric characters are replaced with a hexadecimal values. After the information is encoded it is sent to the server.

The GET Method

The GET method sends the encoded user information appended to the page request. The page and the encoded information are separated by the **?** character.

Example : http://www.test.com/index.htm?name1=value1&name2=value2

- The GET method produces a long string that appears in your server logs, in the browser's Location: box.
- The GET method is restricted to send up to 1024 characters only.
- Never use GET method if you have password or other sensitive information to be sent to the server.
- GET can't be used to send binary data, like images or word documents, to the server.
- The data sent by GET method can be accessed using QUERY_STRING environment variable.
- The PHP provides *$_GET* associative array to access all the sent information using GET method.

The POST Method

The POST method transfers information via HTTP headers. The information is encoded as described in case of GET method and put into a header called QUERY_STRING.

- The POST method does not have any restriction on data size to be sent.
- The POST method can be used to send ASCII as well as binary data.
- The data sent by POST method goes through HTTP header so security depends on HTTP protocol. By using Secure HTTP you can make sure that your information is secure.
- The PHP provides **$_POST** associative array to access all the sent information using GET method.

The $_REQUEST variable

The PHP $_REQUEST variable contains the contents of both $_GET, $_POST, and $_COOKIE.

The PHP $_REQUEST variable can be used to get the result from form data sent with both the GET and POST methods.

Cookies

Cookies are text files stored on the client computer and they are kept of use tracking purpose. PHP transparently supports HTTP cookies.

There are three steps involved in identifying returning users:

- Server script sends a set of cookies to the browser. For example name, age, or identification number etc.
- Browser stores this information on local machine for future use.
- When next time browser sends any request to web server then it sends those cookies information to the server and server uses that information to identify the user.

Accessing Cookies with PHP:

PHP provides many ways to access cookies. Simplest way is to use either $_COOKIE or $HTTP_COOKIE_VARS variables.

V. FEASIBILITY STUDY

All projects are feasible, given unlimited resources and infinite time. But the development of software is plagued by the scarcity of resources and difficult delivery rates. It is prudent to evaluate the feasibility of the project at the earliest possible time.

Three key considerations are involved in feasibility analysis.

Technical Feasibility:

Technical feasibility centres on the existing computer system (Hardware, Software etc.,) and to what extent it can support the proposed addition. If the budget is a serious constraint, then the project is judged not feasible.

Economic Feasibility:

This procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. It benefits outweigh costs, and then the decision is made to design and implement the system. Otherwise, further justification or alternations in proposed system will have to be made if it is to have a chance of being approved. This is an ongoing effort that improves in accuracy at each phase of the system lifecycle.

Operational Feasibility:

People are inherently resistant to change, and computers have been known to facilitate change. It is understandable that the introduction of a candidate system requires special effort to educate, sell, and train the staff on new ways of conducting business.

VI. CONCLUSION

In this research paper we have proposed a system which provides an inexpensive solution for detecting threats and attacks on a PHP website. It will be an effective tool to detect threat based on common patterns of attacks using signature matching. The user/attacker details will also be fetched using this system.

REFERENCES

[1] Lance Spitzner. Honeypots: Tracking Hackers. Addison Wesley, Boston. 2002.

[2] Honeynet Research Alliance. Project Honeynet Website. Retrieved May 16th

[3] http://www.honeynet.org/papers/honeynet/tools/snort.co nf.

[4] TANUSHA A Firefox Extension for Detecting Stored Cross Site Scripting Attack MARCH 23, 2011

