Honeypot: a tool to track hackers

Yogita M. Mali
maliyogita93@gmail.com

Roshni Mary J. V.
Mohan Raj
mary.roshni@gmail.com

Akshay T. Gaykar
gaykar.akshay@gmail.com

ABSTRACT

Honeypots is a trap set to detect, deflect or counteract attempts at unauthorised intrusion. Honeypots 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. Its system are setup to gather information regarding an attacker or intruder into your system. It does not replace other traditional internet security systems, they are additional level or system. It is being extensively used by the research community to study disputes in network security, such as Internet worms, spam control, DoS attacks, etc. In this paper, we favor the use of low-interaction honeypots as an effective instructing tool to study disputes in network security. We serve as a foundation for this claim by demonstrating a set of projects that we have carried out in a Website, which we have deployed specifically for running various web applications under supervision. The design of our projects acts as a service provider for Honeypot security to various websites. Our project tackles the challenges in installing a honeypot 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 honeypots, we present a framework to implement honeypot which can be used by any organization to test their website applications/portals and trace characteristics of hackers.

General Terms

Security and Protection

Keywords

Honeytokens, Honeypages, Remote File Inclusion(RFI), SQL injection

1.INTRODUCTION

Honeypots are closely supervised decoys that are employed in a network to read the track of hackers and to alert network administrators of a possible intrusion. Using honeypots provides a cost-effective solution to increase the security structure of an organization. Even though it is not a panacea for security breaches, it is useful as a tool for network adaption and intrusion detection.
Honeypots can be classified[16] based on their arrangement and based on their level of Interaction, Based on Implementation and base on purpose:

By level of interaction:
1.Low Interaction

- Simulates some aspects of the system
- Easy to deploy, minimal risk
- Limited Information
- eg.Honeyd

2.High Interaction

- Simulates all aspects of the OS: real systems
- Can be compromised completely, higher risk More Information
- eg.Honey-net

By Implementation:
Physical

- Real machines
- Own IP Addresses
- Often high-interactive

Virtual

- Simulated by other machines that: Respond to the traffic sent to the honeypots May simulate a lot of (different) virtual honeypots at the same time

By purpose:

Production :
Production honeypots are easy to use, capture only restricted information, and are used primarily by companies or corporations; They are placed inside the production network with other production servers by an organization to improve their overall attribute of security. Normally, production honeypots are low-interaction honeypots, which are easier to arrange. They give less information about the attacks or attackers than research honeypots do.

Research:
Research honeypots are run to gather information about the motives and tactics of the Blackhat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats that organizations face and to learn how to better protect against those threats.[1] Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

2.EXISTING SYSTEM

1.BACKOffiCER FRIENDLY(BOF):

BackOfficer[16] Friendly is a spoofing server application that runs on your Windows or UNIX system, and notifies you whenever someone attempts to remote control your system using Back Orifice. Basically, it pretends to be a Back Orifice server. Back Officer Friendly gives the attacker false

answers that look like they came from Back Orifice,while logging the attackers IP address and the operations they attempted to perform.

2.Specter :

Specter is a commercial honeypot supported by NetSec, a network security company.Specter is a smart honeypot or deception system simulates a complete machine, providing an interesting target to lure hackers away from the real machines. Specter offers common Internet services such as SMTP and FTP which appear perfectly normal to the attackers but in fact are traps for them to mess around and leave traces without even knowing that they are connected to a fake system which does none of the things it appears to do it Instead logs everything and notifies the appropriate people. Further more, Specter automatically investigates the attackers while they are still trying to break-in.

3.HONEYD:
Honeyd is a prepackaged OpenSource honeypot designed for the UNIX platform by Neils Provos. It is a low interaction honeypot; therefore, there is no operating system to interact with and it is designed primarily to detect attacks or unauthor-ized activity. Since it is an OpenSource solution and highly customizable, theuser may configure it to listen on any port he/she wants and to adjust the level of emulation to meet his/her specifications.

2.1 Disadvantages Of Existing System

The current honey pot tools available are moreover network specific and don't focus more on attacks the Web based attacks. None of the present honey pot tools are designed to work with website & determine the attacks performed on the web based applications.

3. PROBLEM STATEMENT

All the above mentioned solutions are low-interaction system &server level honey pots. Hence there has been always a need for website owners & web development companies for high Interaction website monitoring tools for the attacks. Websites & CMS developed in technologies such as PHP, ASP ,CGI, Javascript , and Ajax have made it much easier for people to build and deploy services on the Internet. Unfortunately, this has opened a wide possibility for new attacks since it is accidentally Introduce new vulnerabilities into it. Therefore, web saites have increasingly been the focus of attackers. Although a lot of web administrator has a lot of choice to choose the more stable and secure open source content management system & websites as their favorite instant deployment medium, they still need to monitor for vulnerabilities and threats that have been occurred on the web servers. For that reason, the web administrator needs an easier way on how to analyze the long and unstructured log file for every server. The best way is to pass on the threat and monitor it on single point like having a proxy within the network to log any [HTTP] hyper text transport protocal request. This project will propose a proper way on how to help the web administrator monitor their entire webserver HTTP request by looking at the log server only instead of having to read every each server log file.

There are kind of attacks on the websites or portals, because of which introduces new vulnerabilities into it.

SQL injection:
SQL injection[[4][9][12] is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input Is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input Is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks

XSS(cross-site scripting):
Cross-site[1][2] scripting is a type of computer security vulnerability typically found in web application .It enables malicious attackers to inject client-side script into web pages viewed by other user.Cross-site[14] scripting carried out on websites were roughly 80% of all security vulnerability documented by Symantec 2007

cURL Attacks:
cURL[2] aka Client URL , a library created by Daniel Sternberg is a predominantly command line based tool, which can be used to force parameter into web request.
Eg. Use of command line like this.
curl-silent –output output_filename
http://example.com/urltofetch.html

Remote file inclusion:
Remote file inclusion[8] is type of vulnerability most often found on websites.
It allows an attackers to include a remote file usually through a script on the web server.
The vulnerability occurs due to the use of user supplied input without proper validation

4. PROPOSED SYSTEM

• Our project acts as a service provider for Honeypot Security to various websites . It acts as a framework to implement honeypot which canbe used by any organization to tes their website applications / portals.
• Our clients would consist of websites of PHP format.
• We plan to trace characteristics of hackers like
1] Their IP address from the IP header
2] The browser they use
3] The files accessed
4] The loopholes they discover
5] Various inputs that are used for various input fields
6] Script Injection
7]the next page navigated
8]Statistic data

5.SYSTEM ARCHITECTURE

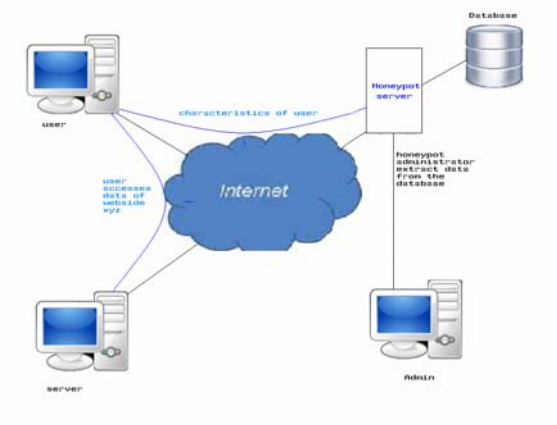

Fig 1:System flow

The above architecture describe the working of honeypot server. user accesses the website xyz's Data through the internet ,the client server communicate with the honeypot through/via internet. Mean while ,the user is accessing the website xyz's data the honeypot server extracts the necessary characteristics of user and stores the data in the database. the admin accesses the honeypot servers database .the admin accesses the honeypot servers database , to extracts data and perform analysis to check whether the user accessing the website xyz's data is a genuine user or malicious attacker.

Assumptions / Dependencies

• We assume that our system will better work with PHP [6][9]based web applications. So we conclude our host Tests are performed on PHP sites

• We assume the client side scripting language on the Host sites is Javascript.

• Injecting scripts and other features on a client website would require Folder Access and FTP rights.

5.1 IMPLEMENTATION

- IP tracing & HTTP packet analysis
- Honeytokens
- Honeypages
- Browser Defect Tracking
- Attacks Tracing [SQL Injection, Cross Side Scripting, etc]

IP tracing & HTTP packet analysis
In our project [15]we inject certain scripts into the code of the web pages which will act as our Honeypot sniffer. These scripts could be JavaScript and SQL injections. These sniffers will then acquire the information and store it in our database. All unauthorized activities would then be tracked and stored in an administrative website for future analysis.
Honeytokens: Honeytokens [15][17][18] are fake records that are inserted in the database. These fake records are not expected to be used by normal users. If any of these honeytokens are used, they alert us of the data-base having been compromised. An example of honeytokens are fake username/passwords in the user database. These users do not exist in the real world, and hence are not expected to be logging into the application. If the application sees these credentials being used, it immediately recognizes that the user database has been compromised.

Honeypages: These are [8][15]obscure web pages sprinkled in the web site. They have no legitimate purpose, nay they are not even linked from any valid page. Normal users would never reach these pages. However, we drop hints about these pages by em bedding their url as comments or hidden fields in valid pages. While normal users would never see this, an attacker who analyzes the source code, or a vulnerability scanner that spiders the site would see these and follow the link. When the page is accessed, it points us to the intruder.

Browser Defect Tracking :

All browsers[15] have various configurations and accessibility. Hackers usually attack a website through loopholes in the browser.We intend to track the loopholes used by the hacker and change the settings of the website.

SQL injection : SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks. we have proposed a scheme for detection and the prevention of SQL injection attack. It is done using pattern matching technique.[6][7] The proposed system is evaluated using sample of well-known attack signatures.

5.2 TECHNOLOGY AND CONCEPTS

The following depicts the concepts and technology used in the proposed system.

We will be tracing all the request made by the client to the server from the demo site. All the GET-POST value s sent & received from the client will be logged in to the Honeypot 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.
Eg: 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.

Conclusion

In this paper, we have proposed honeypot who focus more on web based attacks. This honeypot tool basically aim to work with website and determine the attacks performed on the web based applications. In this honeypot it collect and log data with small amounts of false positives value and negatives value , as it logged data only from the target web page. The data has high value.hence, we have implemented the database for storing user log data ,GUI designing of the overview,log and Attack Signatures.

REFERENCES

[1] K. Fernandez and D. Pagkalos. Xssed.com - xss (cross-site scripting) information and vulnerabile websites archive. [online], http://xssed.com (03/20/08).

[2] Automatic Creation of SQL Injection and Cross-Site Scripting Attack**s** BY Adam Kie, Philip J**.** Guo Karthick ,Jayaraman Michael D. Ernst

[3] S. Christey and R. A. Marti**n.** Vulnerability type distributionsincve,version1.1[online],http://cwe.mitre.org/documents/vuln-trends/index.html,(09/11/07), May 2007.

[4]S.Bandhakavi, P. Bisht, P. Madhusudan, and V. N.Venkatakrishnan. CANDID: preventing SQL injection attacks using dynamic candidate evaluations. In CCS, 2007

[5] T. Holz, F. Raynal, "Detecting Honeypots and othersuspicious environments", In Proceedings of the 6thIEEE Workshop on Information Assurance and Security,pp.29-36, 2005.

[6]Alias-aware propagation of simple pattern-based properties in PHP applications,2012 IEEE 12th International Working Conference on Source Code Analysis and Manipulation

[7]AN EFFICIENT TECHNIQUE FOR PREVENTINGSQL INJECTION ATTACK USING PATTERN MATCHING ALGORITHM,2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)

[8] Intrusion Detection System", International Journal of Web Information Systems, volume 4, pp. 97-120, 2007

[9]https://www.acunetix.com/websitesecurity/sql-injection/

[10]http://www.w3schools.com/php/

[11]http://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php

[12]Halfond, W. G. and Orso, A , "AMNESIA: Analysis and Monitoring for Neutralizing SQL-Injection Attacks", in Proceedings of the 20th IEEE/ACM international Conference on Automated Software Engineering, 2005

[13]C.J. Ezeife, J. Dong, A.K. Aggarwal, "Sensor WebIDS: A Web Mining Intrusion Detection System", International Journal of Web Information Systems, volume 4, pp. 97-120, 2007

[14]D.Ross.IE8 XSS filterarchitecture/implementation.[online],http://blogs.technet.com/swi/archive/2008 /08/18/ie-8-xss-filter-architecture-implementation.aspx (09/09/08), August 2008

[15]E VIL S EED: A Guided Approach to Finding Malicious Web Pages2012 IEEE Symposium on Security and Privacy

[16]Lance Spitzner. Honeypots: Tracking Hackers. Addison-Wesley,2003.

[17] L. Spitzner, "Honeyt okens: The other honeypot," Security Focus, vol.21,2003.

[18] D. Storey, "Catching flies with honey tokens," Network Security,vol.2009,no. ,pp. 15-18,2009.