Scientific Journal Impact Factor (SJIF): 3.518
International Journal of Modern Trends in Engineering and Research
IJMTER
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Web Based Security: - Using Honeypots

Aditya Kulankar[1],Amar Shirgavi[2],Shardul Shewale[3], Jeet Ahluwalia[4], Prof.Neha Jain[5]

[1,2,3,4]Aditya Kulankar,Amar Shirgavi,Shardul Shewale, Jeet Ahluwalia Student, Dept. of Computer Engineering Shree L.R.Tiwari College of Engineering Mumbai, India

[5]Prof.Neha Jain Dept. of Computer Engineering Shree L.R.Tiwari College of Engineering Mumbai, India

Abstract-Honeypots are closely monitored decoys that are employed in a network to study and analyze the trail of hackers and to alert network administrators of a possible intrusion. Honeypots 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, DoS attacks, etc.

I. Introduction

The design of 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 for designing projects for web application security courses. 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. Our project acts as a service provider for Honeypot Security to various websites. It acts as a framework to implement honeypot which can be used by any organization to test their website applications / portals.

We plan to trace characteristics of hackers like

- The browser they use
- Their IP address from the IP header
- The files accessed
- The loopholes they discover
- Various inputs that are used for various input fields.

II. Existing Systems

We have discussed the currently existing systems that are similar to our project.

The following are some famous honeypots available in the market:

A. Back Officer Friendly (BOF):

BackOfficer 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. BackOfficer 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.

B. Specter:

Specter is a commercial honeypot supported by NetSec, a network security company. Specter is a smart honeypot or deception system. It simulates a complete machine, providing an interesting target to lure hackers away from the real machines.

C. Honeyd:

Honeyd is a prepackaged OpenSource honeypot designed for the UNIX platform by Neils Provos. Since it is an OpenSource solution and highly customizable, the user may configure it to listen on any port he/she wants and to adjust the level of emulation to meet his/her specifications.

D. Current System & their drawbacks:

The current honey pot tools available are moreover network specific and don't focus more on 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. All the above mentioned solutions are low-interaction system & server level honeypots.

III. Drawbacks

Honeypots has been focused on research area, in recent years against evading attacks. Centralized control, manages all the control center of the network. Agents can be virtual honeypot, firewall, and intrusion detection system. Control center manages the different agent in a network. It handles the messages and performs sample matching. Another function of control center is it generates the alarm for and identifies intrusion. Honeypot cannot protect a network which is not covered in its network range. It can detect attacks which are directed towards it.

IV. Methodology

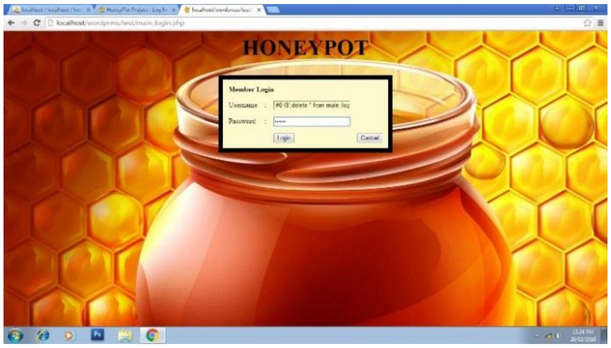
Honey tokens: Honey tokens are fake records that are inserted in the database. These fake records are not expected to be used by normal users. If any of these honey tokens are used, they alert us of the database having been compromised. An example of honey tokens are fake username/passwords in the user database. These users do not exist in the real world, and hence are not expected to be logging in to the application. If the application sees these credentials being used, it immediately recognizes that the user database has been compromised.

Honey pages: These are obscure web pages sprinkled in the web site. They have no legitimate purpose, they are not even linked from any valid page. Normal users would never reach these pages. However, we drop hints about these pages by embedding their urn 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 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.
We plan to inject certain scripts into the code of the webpages which will act as our Honeypot sniffer. These scripts could be JavaScript's 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.

V. Results and Analysis

Our project will help administrator improve the current status of the system application and help provide an overview of the number of logins, attack pattern being used.Automactially scans for known patterns of attacks and generates numerous statistics on the basis of it.



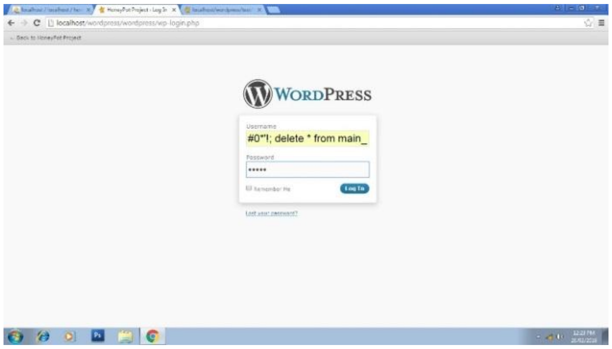
HONEYPOT

Member Login

Username : #0 !$';delete * from main_log

Password : ••••••

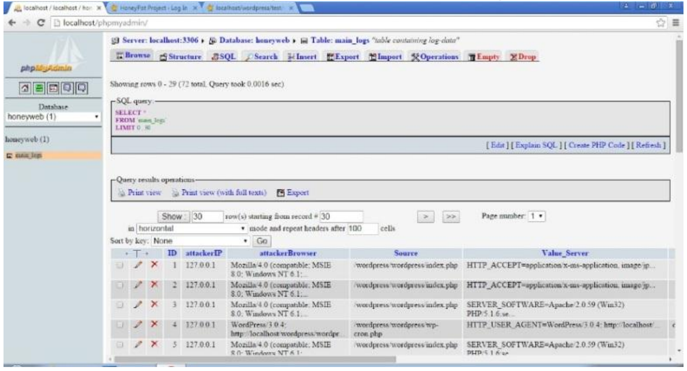
Figure. 1: Honeypot main login page.



Username: #0"'!; delete * from main_

Password: •••••

Figure 2: Second login page, an alternative to the initial login page providing the similar purpose in tracking all the movements of the user whoever logs in.



Server: localhost:3306 ▸ Database: honeyweb ▸ Table: main_logs "table containing log-data"

Showing rows 0 - 29 (72 total, Query took 0.0016 sec)

SQL query:

```
SELECT *
FROM `main_logs`
LIMIT 0 , 30
```

Show : 30 row(s) starting from record # 30

in horizontal mode and repeat headers after 100 cells

Sort by key: None

Page number: 1

ID	attackerIP	attackerBrowser	Source	Value_Server
1	127.0.0.1	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;...	/wordpress/wordpress/index.php	HTTP_ACCEPT=application/x-ms-application, image/jp...
2	127.0.0.1	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;...	/wordpress/wordpress/index.php	HTTP_ACCEPT=application/x-ms-application, image/jp...
3	127.0.0.1	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;...	/wordpress/wordpress/index.php	SERVER_SOFTWARE=Apache/2.0.59 (Win32) PHP/5.1.6.se...
4	127.0.0.1	WordPress/3.0.4; http://localhost/wordpress/wordpr...	/wordpress/wordpress/wp-cron.php	HTTP_USER_AGENT=WordPress/3.0.4; http://localhost/...
5	127.0.0.1	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;	/wordpress/wordpress/index.php	SERVER_SOFTWARE=Apache/2.0.59 (Win32) PHP/5.1.6.se

Figure 3: Administrator receives the detailed log and analysis.

VI. Conclusion

In this paper, our application will focus on analysis, monitoring as well as creating log files etc. In the database that will help our administrator to determine and help him to improve the protection of the website as a general.

VI. References

[1] Glasvezel Networks Nederland Fiber to the Home Project (FTTH),2009.Honeypot Software, Honeypot Products, Deception Software

[2] Lakhani A.D., A dissertation on deception techniques using honeypots. Information Security Group Royal Holloway, University of London, UK.

[3] http://www.mecs-press.org/ijcnis/ijcnis-v4-n10/IJCNIS-V4-N10-7.pdf

[4] http://www.cs.ucf.edu/~czou/research/honeypotDetect-IJICS.pdf

[5] http://www.lib.iup.edu/comscisec/SANSpapers/msink.htm

[6] http://sumnerk.tripod.com/mywebsite/courses/secarch/honeypotpaper.pdf .