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. 4, Issue 6, June 2016

Web Security Using Software Based Honeypot Architecture

Maitri Shukla[1], Pranav Verma[2], Shyamal Pandya[3]

ME Research Scholar, Department of Computer Engineering, SOCET, Ahmedabad, India[1]

Assistant Professor, Department of Information Technology, SOCET, Ahmedabad, India[2]

ABSTRACT: In couple of decades number of attacks on IT organization has increased. Among them small and medium sized organization's risk is higher because of lower security architecture in their system. Attackers use SQL injection and XSS type of attacks to exploit the vulnerability of the system or the organization. A mechanism which is created to learn about the attackers' method of attack and pattern and also used to get useful information about the intrusive activity is Honeypot. Honeypots can be classified according to the level of interaction as low-interaction, medium-interaction, high interaction and the purposed for which it is used as research honeypot and production honeypot. Detailed study about the types of honeypot is included in this paper. Various honeypot results are enlisted in this paper to show that how honeypot works in real-time environment and how it responds when any unwanted activity occurs in the network.

KEY WORDS: Network security, Honeypot, Intrusion-detection, Types of Honeypot, Honeynet

I. INTRODUCTION

Attacks on websites and databases are increasing day by day rapidly. Among all of them sophisticated attacks are being increased drastically, which affects small and medium sized companies also. There are few features of these sophisticated attacks which involve high skilled attackers, also knowledge about the targets etc. So there must be some system to detect those attacks on the databases. From the basis on this idea we have formed this architecture which is useful to detect attacks and also create logs for all entries in the database, from which we can find if there is any suspicious entry is occurred with wrong purpose.[1]

According to the Lance Spitzner, Founder of Honeypot Technology, "A honeypot is an information system resources whose value lies in unauthorized of illicit use of that resources".[2]

A honeypot can detect the behaviour of the attacker or the intrusion information to observe and record the details of the attacker and create a log of malicious entries and examines level, purpose, tools and methods used by the attacker so that evidence can be obtained and further actions can be taken. [3] Honeypot technology and traditional security system combined can build an active network security protection system.[4]

There are several types of Honeypot based on the level of interaction and the purpose of Honeypot.

A. Based on level of interaction Honeypots can be classified based on the level of interaction between intruder and system. These are Low-interaction, high interaction and medium-interaction honeypot

i) Low-interaction honeypot: These types of honeypots have the limited extend of interaction with external system. Main advantage of this type of honeypot is that, it is very easy to deploy and maintain and it does not involve any complex architecture. With this advantage there is also some drawback of this system. That is, it will not respond accurately to exploits. This creates the limitation in ability to aid in discovering new vulnerabilities or new attack patterns. Low-interactive honeypots are a safer and easy way to gather info about the frequently occurred attacks and their sources. [2][5][6][7]

ii) High-interaction honeypot: This is the most advanced honeypot.[7] This type of honeypot have very higher level of interaction with the intrusive system. It gives more realistic experience to the attackers and gathers more information about intended attacks; this also involves very high risk of capturing of whole honeypot. High-interaction honeypot are most complex and time consuming to design and manage.

DOI: 10.15680/IJIRCCE.2016. 0406016

iii) Medium-interaction honeypot: These are also known as mixed-interactive honeypots.[3] Medium-interaction honeypots are slightly more sophisticated than low-interaction honeypots, but are less sophisticated than high-interaction honeypots. It provides the attacker with a batter illusion of the operation system so that more complex attacks can be logged and analysed.

B. Based on the purpose Honeypots can be classified based on the purpose as Research honeypot and Production honeypot.

i) Research honeypot: Research honeypots are basically used for learning new methods and tools of attacks.[8] Research honeypots are used to gather intelligence on the general threats organizations may face, which gives the organization a better protection against those threats. Its main goal is to gain info about the way in which the attackers progress and performs lines of attacks. Research honeypots are complex to build, deploy and manage. They are basically used by organizations like universities, governments, the military and intelligence systems to learn more about threats. Research honeypots provides a strong platform to study cyber-threats and forensic skills. [7]

ii) Production honeypot: production honeypots are simply aimed to protect the network.[8] Production honeypots are easy to build and deploy, as they require very less functionalities. They protect the system by detecting attacks and giving alerts to administrators. It is typically used within an organization environment to protect the organization. [7][8]

Mainly Honeypots can be of two types Hardware based Honeypots and Software based Honeypots.Though hardware based honeypots involves highly configured servers and computer machines, they are very expensive and complex to install for medium and small sized companies, software based low-interaction honeypot are more suitable for that.

II. RELATED WORK

According to OWASP survey of 2013[9] SQL injection and XSS(Cross site scripting) are the most frequently performed attacks to hack the database. There are various solutions for this security attacks like IDS(Intrusion Detection System) but it does not create any logs for intrusive activities occurred in the system. The logs give more information about the attacker which might help to track the attacker and find the attacker. This problem can be solved by using a new generation security mechanism called Honeypot.

In this research software based, low-interaction honeypot is designed to detect the various attacks on the system. Here for experiment the system is designed for XSS and SQL Injection, so that the Honeypot will detect these two attacks and will respond accordingly.

Following figure shows the system block diagram of the designed Honeypot.

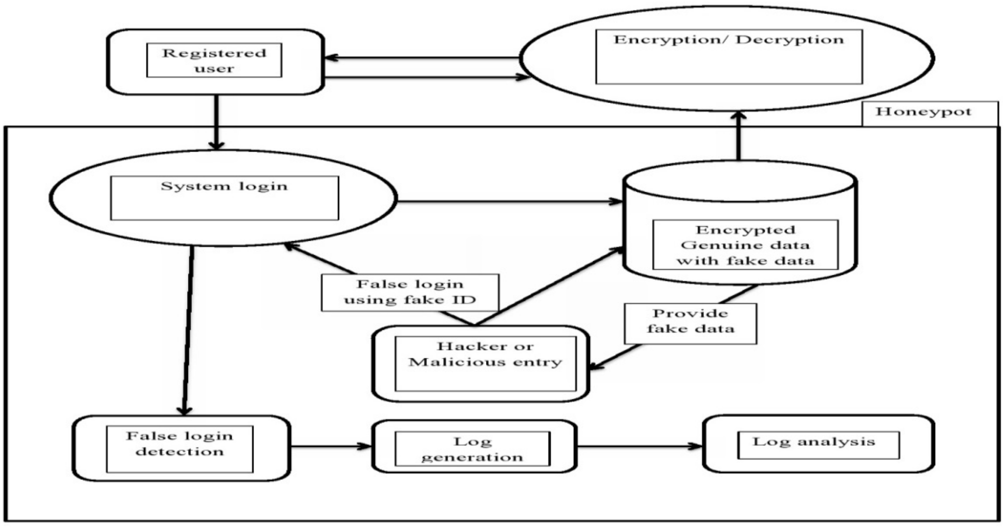


Fig. 1 System Block Diagram

To test the security of any web site, first of all a non-secure web-site is formed. Then the effect of SQL Injection and XSS can be monitored over that.

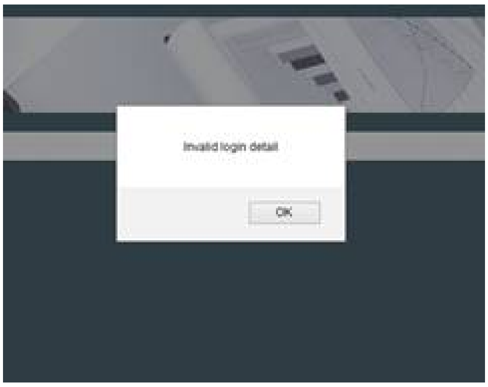
Honeypot is implemented over the website and again the effects of various attacks are checked. Efficiency of the Honeypot is monitored. Log for the suspicious entries is generated to get information about the attacks and attacker like IP address, attack method, intruder identification if any followed etc. Same database is used to store the data so that it will not require separate database for encrypted original data and false data. As the original data is encrypted no one can read it directly so attacker will not able to read it or use it. Another thing is we have designed a mechanism of read on accessibility for the random fake logins. So in worst case scenario if the attacker is successful to read the original data it will not be able to delete or modify it so that no change will resemble to the main website. MAC address and Cookies are used to get information about the attacker. MAC address is the system's physical address which will be registered at IT databases so that we can get information about the person having the system with a particular address. Another is cookies, which will give us information like browser details, OS details, attacker's system details and IP address, which will be helpful to track back the attacker in the detection process. Following details are gathers about the attacker.

http_user_agent	http_accept	http_accept_language
http_accept_encode	http_referer	http_cookie
http_connection	http_cache_control	http_path
Systemroot	Comspec	Pathext
Windir	remote_addr	server_admin
script_filname	remote_port	gateway_interface
server_protocol	request_method	query_string
request_url	script_name	request_time

III. SIMULATION & RESULTS

In this section how actual system works is shown.

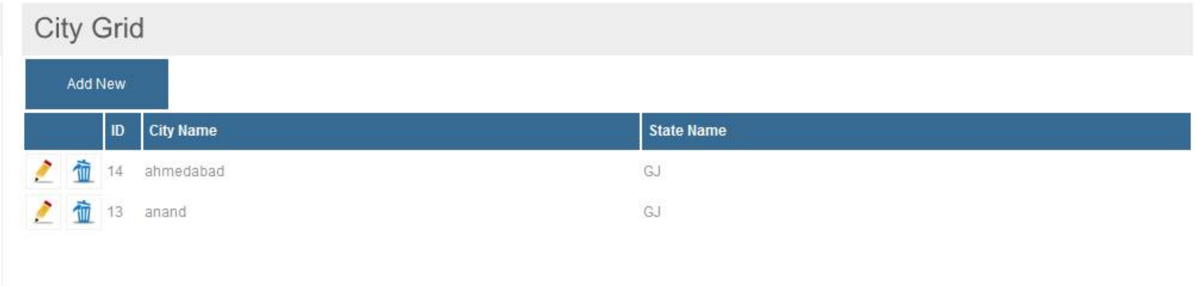
Figure 2 shows the invalid login block in the system, so that if someone tries to enter in the system with false login detail it will be blocked.



Invalid login detail

Fig. 2 Invalid Login

Figure 3 shows the details shown when login is done with valid login details.

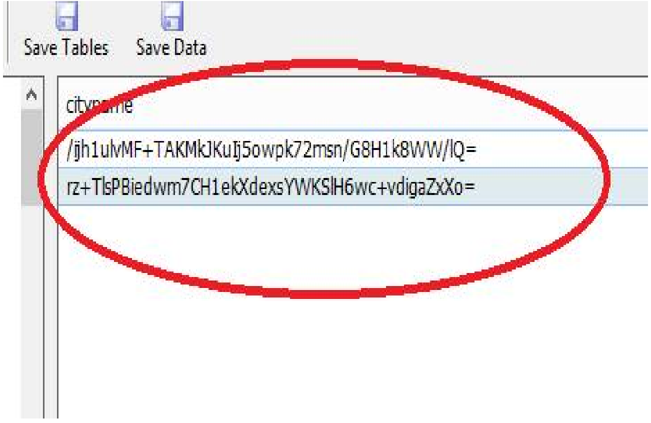


City Grid

		ID	City Name	State Name
		14	ahmedabad	GJ
		13	anand	GJ

Fig. 3 Decrypted Data on Valid Login

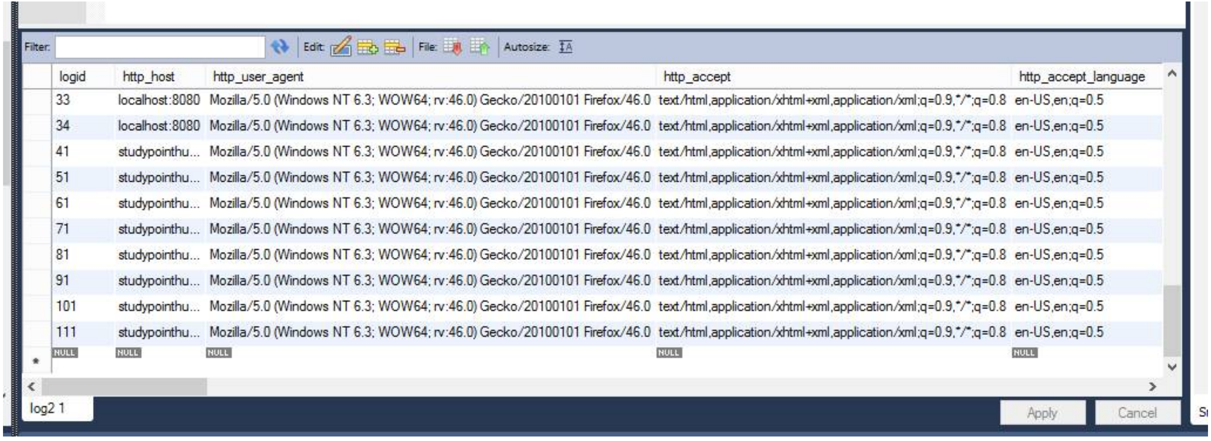
Figure 4 shows the encrypted data. Data in the whole site is encrypted so that if someone tries to hack threw any SQL Injection tools then only encrypted data will be displayed so that no one can get the original data.



cityname
/jjh1ulvMF+TAKMkJKuIj5owpk72msn/G8H1k8WW/lQ=
rz+TlsPBiedwm7CH1ekXdexsYWKSlH6wc+vdigaZxXo=

Fig. 4 Encrypted Data

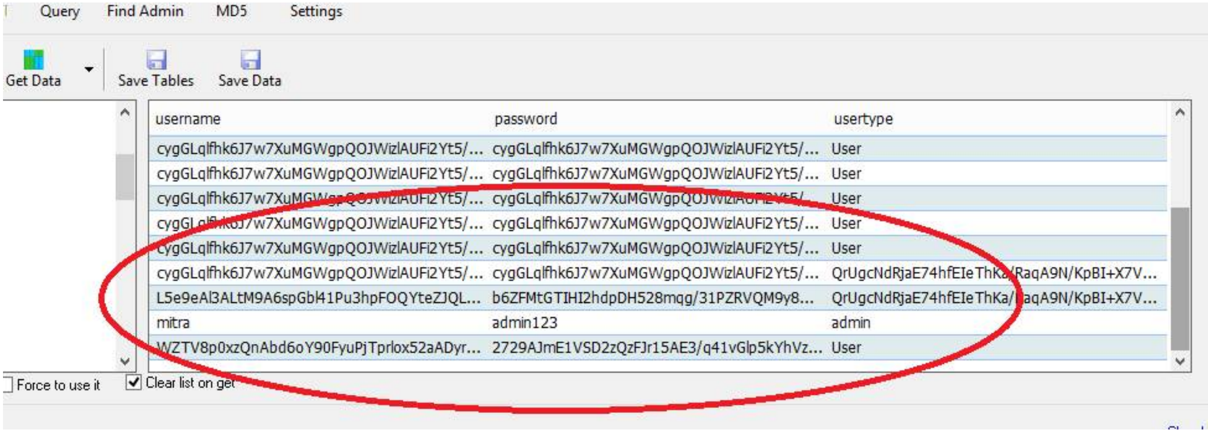
Figure 5 shows the log which will be generated with each entry in the system.



logid	http_host	http_user_agent	http_accept	http_accept_language
33	localhost:8080	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
34	localhost:8080	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
41	studypointhu...	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
51	studypointhu...	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
61	studypointhu...	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
71	studypointhu...	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
81	studypointhu...	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
91	studypointhu...	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
101	studypointhu...	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
111	studypointhu...	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	en-US,en;q=0.5
NULL	NULL	NULL	NULL	NULL

Fig. 5 Log Generation

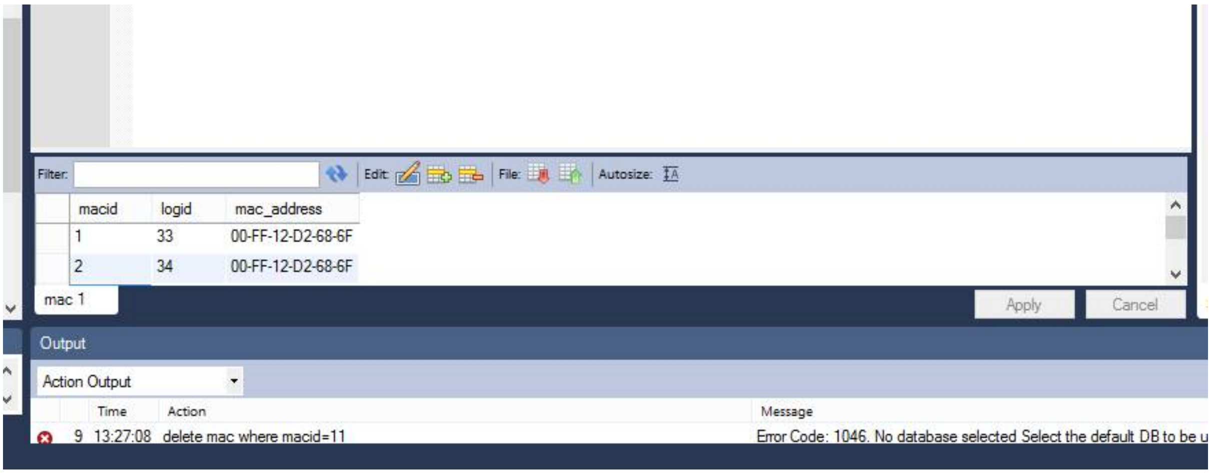
Figure 6 shows the false entries in the random tables so that using that we can fool the intruder.



username	password	usertype
cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	User
cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	User
cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	User
cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	User
cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	User
cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	cygGLqlfhk6J7w7XuMGWgpQOJWizlAUFi2Yt5/...	QrUgcNdRjaE74hfEIeThKa/RaqA9N/KpBI+X7V...
L5e9eAl3ALtM9A6spGbl41Pu3hpFOQYteZJQL...	b6ZFMtGTIHI2hdpDH528mqg/31PZRVQM9y8...	QrUgcNdRjaE74hfEIeThKa/RaqA9N/KpBI+X7V...
mitra	admin123	admin
WZTV8p0xzQnAbd6oY90FyuPjTprlox52aADyr...	2729AJmE1VSD2zQzFJr15AE3/q41vGlp5kYhVz...	User

Fig. 6 False data

Figure 7 shows the MAC address of every entry in the system, so that if we find any suspicious entry we can detect the intruder.

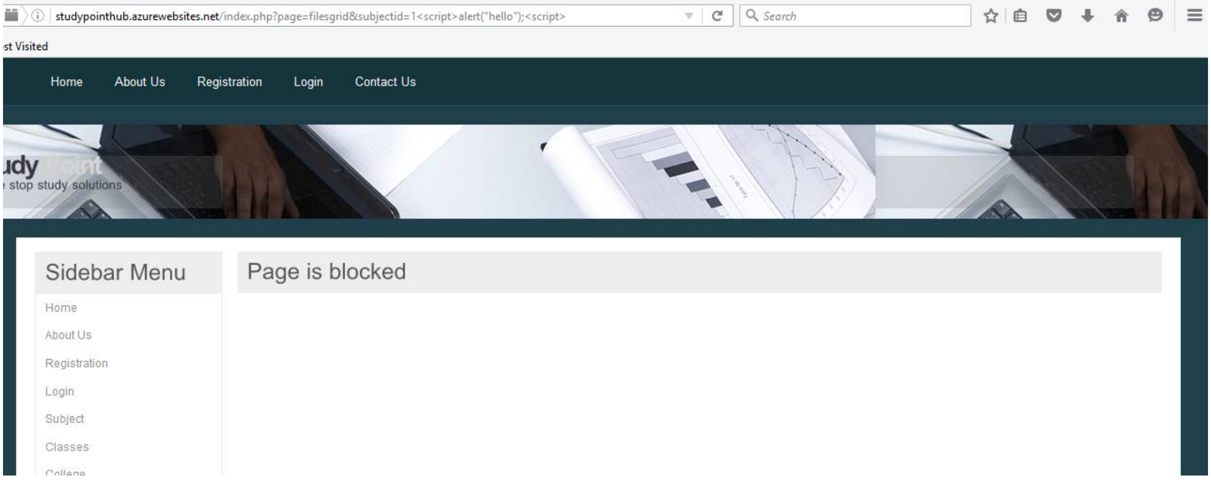


	macid	logid	mac_address
	1	33	00-FF-12-D2-68-6F
	2	34	00-FF-12-D2-68-6F

```
    Time      Action                          Message
9   13:27:08  delete mac where macid=11       Error Code: 1046. No database selected Select the default DB to be u
```

Fig. 7 MAC address

Figure 8 shows that the system is capable of providing security against XSS. So that if someone tries to enter in the system using scripts the entry will be blocked immediately.



studypointhub.azurewebsites.net/index.php?page=filesgrid&subjectid=1<script>alert("hello");<script>

Page is blocked

Fig. 8 XSS Security

IV. CONCLUSION

Honeypot is a security mechanism which works by luring the attacker by giving false information and gathering details about the attacker. Here a lowinteraction software based Honeypot is designed which will detect the SQL Injection and XSS attacks performed over the site and will provide data security against it. The tool will fool the attacker by giving false login information to the attacker stored in the user_details table. This Honeypot architecture gives extra level of security for data, as encryption-decryption mechanism is used for the database. Moreover a detailed log is generated which will give the basic information about the attacker including time and the page visited by the unauthorised user. It will provide more précised information related to the IP and physical address and the browser details about the attacker.

V. FUTURE SCOPE

The work can be extended by adding security against more attacks. Furthermore extra information about the attacker can be generated by designing a high interactive Honeypot.

REFERENCES

[1] MaitriShukla, PranavVerma,“Honeypot: Concepts, Types and Working”, © 2015 IJEDR Volume 3, Issue 4.

[2] SupenoDjanali, FX Arunanto, BaskoroAdiPratomo, AbdurrazakBaihaqHudanStudiawan, AryMazharuddinShiddiqi, “Aggressive Web Application Honeypot for Exposing Attacker's Identity” , 2014 1st International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE).

[3] IyadKuwatly, MalekSraj, Zaid AI Masri, and Hassan Artail, “A Dynamic Honeypot Design for Intrusion Detection”, ©2004 IEEE.

[4] Song LI, QianZou, Wei Huang, “A New Type of Intrusion Prevention System”, ©2014 IEEE.

[5] JianBao,Chang-pengJi and Mo Gao,“Research on network security of defense based on Honeypot”, 2010 international Conference on Computer Application and System Modeling (ICCASM 2010).

[6] Mr.KartikChawda ,Mr.Ankit D. Patel ,“Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring”, ©2014 IEEE.

[7] Robert McGrew, Rayford B. Vaughn, JR, PhD,” Experiences With Honeypot Systems: Development, Deployment, and Analysis”, Proceedings of the 39th Hawaii International Conference on System Sciences – 2006.

[9] https://www.owasp.org/index.php/Top_10_2013-Top_10