ACQUIRING ATTACK VECTOR DATA USING HONEYPOT

Snehal Chandrakant Mahadik[1], Kajal Hiralal Mhatre[2], Harsha GajendrasingPatil[3]

[1,2,3]*I T Department, Datta Meghe College of Engineering, Navi Mumbai.*

***Abstract** –Information security is the main concern now a days, for that honeypot is one of the method which is use for security purpose, In this paper we implement honeypot, to identify attacker and get to know the attackers data. As honeypot is use for the network security so it gathers all the information about attacker who are trying to attack. Basically in these paper we presenting the honeypot. Which identify different attackers like Dos and Ddos.*

Keywords: honeypot, security, attack, DOS, DDOS, data collection, log file

I. INTRODUCTION

Now a days for attackers web application have become the main traget, so for that honeypot is the one of method which is used for security purpose. Honeypot is a network attached setup. Which is use to detect attackers. Honeypot fetches all the data about attackers. Honeypot is information resource it collects all the data then it save it as a log file. For that wehave created a website. which is remotely accessable to everyone. And also we have created some attacks like Dos and DDoS. These attacks will make network resource temporary unavailable to its intended user by sending lots of traffic. So here honeypot will identify that attacker and then it will block that attacker.

II. LITERATURE SURVEY

In the literature survey that we have done, we've checked over the following papers mentioned in the table and examined the concepts if they were suitable for our project. Michele Adams in his papers gives all the information about Honeypot, its concept challenges and approaches.

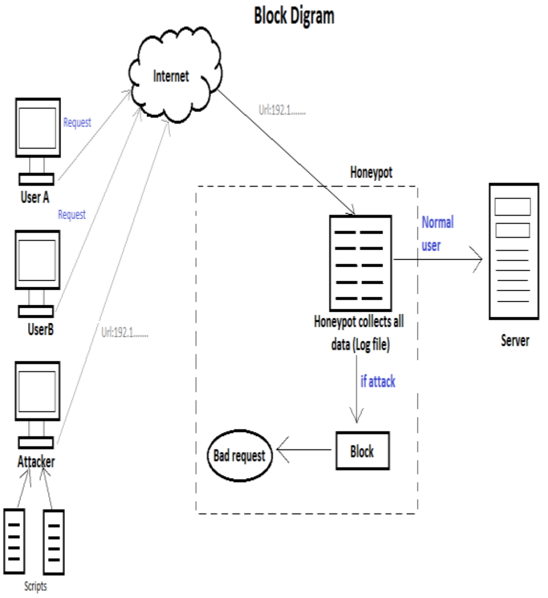
which gets information of each user who visits the system and stores the information also monitor it and detects that the user is not normal user and it is attacker. Honeypot is a system which is nonproduction specially designed to interact with all kind of cyber attacks, and even collect intelligence on which all techniques and behavior of attacker. Honeypots are used to protect company from all the malicious activities done for hacking the company site. They also explained in in their paper Honeyd and Honeynet. Honeyd creates virtual host on network. That host can be allowed to run arbitrary. And In Honeynet to get effective deploy it requires both physical systems and security mechanism.

III. PROBLEM STATEMENT

The attacker can attack whenever and however they want to expose the identity of attacker.

So from the problem statement we got the solution that we can analyse all log files. We can block the user if it has been previously blocked it will not be able to access our website again honeypot will send bad request. We will get various information of the attacker and can store all the information in system. which is collected by honeypot.

IV. METHODOLOGY



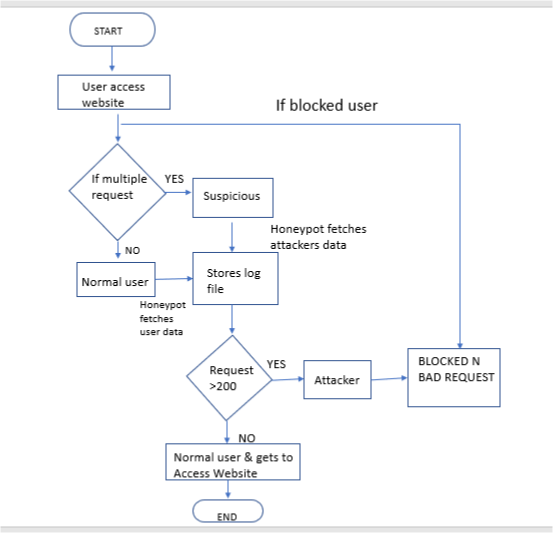
Web applications are often become the main target of attacks. As we are using honeypot which is a computer security mechanism set to detect attack. From the flowchart at the starting multiple users trying to access our website. If multiple request are arrived means that person is suspicious, then honey pot fetches all the data of that suspicious user. If there are normal request like MORE THAN 20 means that person is normal user then honeypot fetches all the data of that normal user. Here after fetching data honeypot collect all the data n store it as a log file. Which is access able to the admin only.

Now honeypot checks whether there are more than 200 request or not. If there are more than 200 request means means that person is attacker. Then honeypot mentioned it as attacker in log file. Then admin block that user after entering ip address of attacker. And list of that attackers is again saved in blocked list user. But If there are less than 200 request means that person is normal user and can access that website.

For that we are taking two attack as dos and ddos attacks. They make machine unavailable to its intended user by temperory hanging that website. For dos attacker it use one machine as a source are trying to send traffic to its targeted user. And in ddos attacker it uses multiple machine as source and send traffic to targeted one. So basically we run this scripts for demo

For that we are taking two attack as dos and ddos attacks. They make machine unavailable to its intended user by temperory hanging that website. For dos attacker it use one machine as a source are trying to send traffic to its targeted user. And in ddos attacker it uses multiple machine as source and send traffic to targeted one. So basically we run this scripts for demo.

V. FLOW CHART



VI. DETAILS OF HARDWARE AND SOFTWARE

Hardware and Software Requirements

Hardware Requirements

1. Server 1: Front-end Web Server
2. Server 2: Application Server
3. SQL Server

Software Requirements

1. Operating System
2. Windows server 2008 R2 (64-bit)
3. SQL server 2012
4. Visual Studio

VII. RESULTS

We created the gym website having two dashboards, user and admin dashboard. Homepage is visible for user as well as admin. in which user can register or log into the website only if the user is genuine user. But if it's attacker who is trying to access website, then record will immediately send to the admin.

Now, admin controls entire website as there are various options available for admin in admin dashboard. Since, this website is for security purpose using honeypot, an additional option is available for admin i.e log file. Where all the data of attacker get recorded by honeypot. And admin will able to check that records.

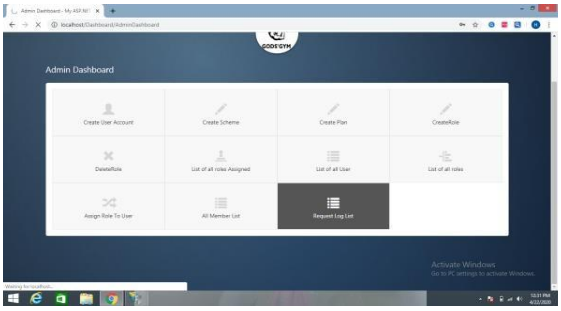


Fig.5.1.1. Request Log List Following is the log file which is connected by honeypot.

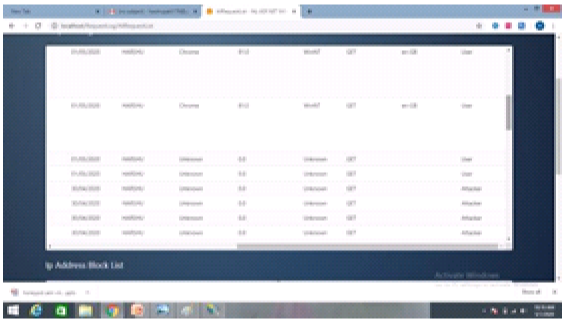
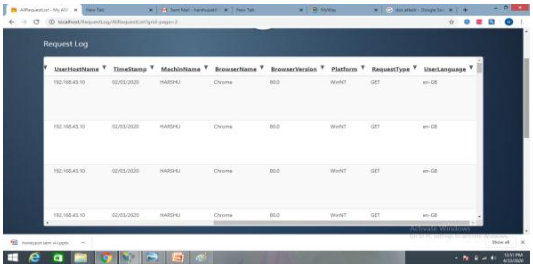


Fig.5.1.2. Logs

As we are using one concept to detect attacker that , If there are more than 200 hundred request then honeypot mentioned it as an attacker.

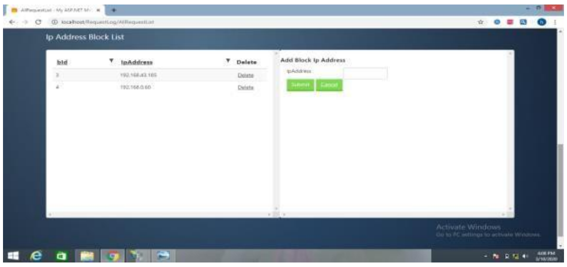


Request Log

UserHostName	TimeStamp	MachinName	BrowserName	BrowserVersion	Platform	RequestType	UserLanguage
192.168.43.10	02/03/2020	HARSHU	Chrome	80.0	WinNT	GET	en-GB
192.168.43.10	02/03/2020	HARSHU	Chrome	80.0	WinNT	GET	en-GB
192.168.43.10	02/03/2020	HARSHU	Chrome	80.0	WinNT	GET	en-GB
192.168.43.10	02/03/2020	HARSHU	Chrome	80.0	WinNT	GET	en-GB

Fig.5.1.3. identify as attacker

Now it's time to block that attacker and all that data is saving in block list.



localhost/RequestLog/AllRequestList
Add Block Ip Address
IpAddress
Submit
Cancel
Activate Windows
Go to PC settings to activate Windows.

Ip Address Block List

bId	IpAddress	Delete
3	192.168.43.105	Delete
4	192.168.0.60	Delete

Fig.5.1.4 Block User List

VIII. CONCLUSION

This framework is to make a website for gym. In which we have implemented honeypot for gym website. Which allows the admin of the website to have a complete record of the Dos and DDos attack done on the website. Here we have discussed about the two types of attack that are Dos and DDos. We have also analyzed various features, functions and uses and role of a honeypot. Basically it secures our system.

IX. REFERENCES

1. Samu, F. (2016).Design and Implementation of a Real-Time Honeypot System Detection and Prevention of systems Attacks.

2. Jain, Y. K., &amp; Singh.S (2011). Honeypot based secu Network system international Journal on Computer Science and Engineering, 3(2), 612-620

3. Kambow N., & Passi, LK.(2014). Honeypots: The need of network security. Internationl Journal of Computer Science and Information Technologies, 5(5), 6098-6101

4. Sadasivam,K, Samudrala B & Yang T.A(2005)Design of network security Projects using honeypots. Journal of computing sciences colleges, 20(4), 282-293.