IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Secure Network System using Honeypot

Ms. Khairkar Ashwini[1], Gollar Pratiksha[2], Kulakarni Anuja[3], Suryawanshi Varsharani[4], Swami Gayatri[5]

Department of Information Technology, Faculty of Engineering, Savitribai Phule Pune University,

Bharati Vidyapeeth's College of Engineering for Women, Pune, India[1,2,3,4,5]

Abstract: Honeypot is new concept used in the network security. Honeypot can detect the attack as well as the attacker's information. Honeypot block out the access to the real system. Honeypot is physical system which acts as original server in the network to make client fool. Honeypot can used with IDS system to make network more secure. This paper consist the honeypot architecture which contains honey net. It also contains how honeypot works in the network for security purpose? Advantages, disadvantages of honeypot. This paper also consist all information about Honeypot and types of honeypot on level of interaction in the network.

Keywords: Honey pot, IDS, SQL injection attack, XSS attack, data leakage attack.

I. INTRODUCTION

As we know that, the use of internet is increases continuously. There is tremendous growth in the networking and connection people together using internet. As well , the attack on the network is also increases.so that security issue comes forward. Honeypot is new strategy used in the network security. There are existing system which is already used for this purpose.
Honeypot is slightly different strategy. Honeypot pretend like original server, which makes client fool. Honeypot allows client to attack on system and while client attaching, honeypot observing the clients behaviour. On that basis. Honeypot detect the attack and attackers information. As per level of security and interaction we can use different honeypot.

There are three level of interaction
1. Low level Interaction.
2. Middle Level Interaction
3. High Level Interaction

Honeypot has two types
1. Research Honeypot.
2. Production Honeypot.

Different types of attack can be detected using honeypot. Honeypot is simple and easy strategy, as there is no need of any separate algorithm for working. In this paper we are using production honeypot. We uses it with IDS (Intrusion Detection System) to provide more security to network.

II. LITERATURE SURVEY

Firewall

Firewall software is installed on computers to monitor incoming and outgoing packet requests. A firewall contains hardware and software that divisions an organizations internal network from other networks, allows some packets from networks, allow some packets to pass and block others. It functions to avoid illegal sessions established to the devices in the network areas it protects. Firewalls are configured to protect against unauthenticated logins from the outside world. Firewall works in two ways : first it block unauthorized packets and second is admin has to set up some rules for firewall [1].

Advantages

1. Firewalls prevent the traffic which unauthenticated.

2. Firewalls filter those protocols and services that can be easily committed.

3. A firewall helps protect the internal network by hiding name of internal systems from the outside host.

Disadvantages

1. Firewall use set of rules that can manually configured to differentiate authorized traffic from unauthorized traffic.

2. Most firewalls don't analyse the contents of the data packets that makes up network traffic.

3. Firewall can't prevent attacks coming from Intranet/local network.

4. Filtering rules of the firewall can't prevent attack coming from application layer.

Intrusion Detection System (IDS)

Intrusion Detection System (IDS) help information systems to deal with attack. This is accomplish by collecting information from a variety of systems and network source. The information collected is analyzed and process for possible security problems. An IDS gather and analyzes information from various sources within a network to identify possible security attacks. The intrusions may include attacks both from outside the organization as well as within the organization[1].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Advantages

1. IDS are easy to deploy as it does not affect existing system or infrastructure.
2. Network based IDS sensors detect many attacks by checking the packet any malicious attack like TCP SYN attack, fragmented packet attack etc.
3. Network based IDS detect malicious activity as normal activity.
4. IDS sensor deployed outside the firewall can detect attack on resources the Firewall.

Proxy Server

Proxy server plays an intermediate/ bridge between the client computer and server computer. The client usually takes the help of proxy server for requesting any files, any web pages or any other resource. The proxy server acts as an identification /detection shield between the server and the client machine. The main feature of a proxy server is , it act as a security protector device between the client computer and the server computer.

Advantages

1. Proxy server help the client to protect their important detail information from getting hacked by hacker.
2. Load Balancing
3. The proxy server is also used to enhance privacy level of the clients device while doing surfing using different proxies.

Disadvantages

1. It happens many time, although using the encrypted connections or network, Our data or information can be leak using the technique of SSL encrypted connection.

2. With the help of proxy server any blocked websites can be accessed. So it is found many time that any blocked and offensive websites.

Double honeypot System

The inbound honeypot is not authorized to establish the outbound connection. But when an attack comes to the inbound honeypot, it tries to establish the outbound connection because worms are having the self-replication property. As soon as the inbound honeypot tries to establish the outbound connection the malicious traffic is forwarded to the inbound honeypot, so that it can gather the malicious traffic. In this architecture the inbound honeypot can establishes the connections to the machines requested from outside (non-local to LAN). Hence it is implemented as high–interaction honeypot[2].

Advantages of Honeypot

1. Honeypot prevent attack coming from Internet.
2. Human interaction not needed.
3. Information save in log.
4. To provide security to multiple server

III. PROPOSED METHODOLOGY

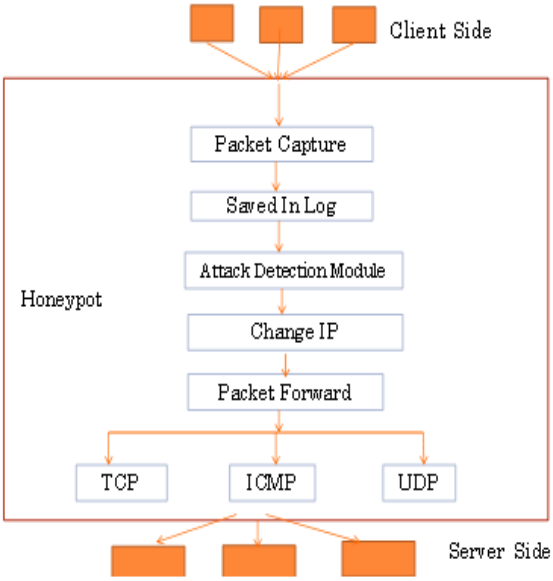


Fig. 1.Architecture of Honeypot

In these paper, three main parties are available which are client side, honeypot and server side. Following components are as follows:

1. Client side - The clients can be of two types: Genuine Client and Fake Client.

2. Honeypot - It is in the middle of client and server which accepts requests from Clients by giving fake IP address to them and gives responses to the Clients. Honeypot works to secure the Servers and makes fool to theClients. Honeypot contains the log file and config file.

Log File: It saves the visitor's information like port no, IP address and MAC address. Config File: It saves all the Client's information which are present in the network.

3. Server side - In these paper, the two main servers are using for giving responses to honeypot: Apache Tomcat and Glassfish.

WORKING

The Clients can communicate to the servers through the honeypot only. The clients has the fake IP address of the honeypot and not the server's. If the client is a genuine client then its request goes to honeypot. Honeypot changes its IP address and forwards the request to the original server. After that server gives response to honeypot.

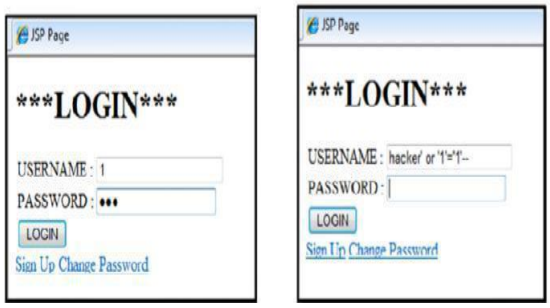
Again honeypot changes its IP address and sends response to client. If the client is fake client, then attacker will be tracked , located, identified and saves information about attackers at the honeypot. Though it is an attacker it gives response to make them fool. In all these scenario, security is maintained.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

IV. ATTACKS

SQL Injection Attack

SQL injection attack mostly applied on the websites. In SQL injection attack the attackers are used different queries to make the successful attack, Where malicious users caninjectSQLcommandsintoSQLstatement via web page input[2]. The SQLinjection attacks are successful when user input is[2] weak typed and unexpectedly executed. SQL injection mostly known as an attack scalar for websites but can be used to attack any type of SQL database [4].



Normal User Attacker

Fig. 2. SQL Injection Attack

Cross-site Scripting Attack

Cross-site scripting attack occur when an attacker uses a web application/websites to send malicious code, generally in the form of a browser side script, to a different end user. XSS refer to client sides code injection attack where in an attacker execute malicious script into a legal website. XSS is the most uncontrolled of web application vulnerabilities and occur when web application makes use of invalid or not encode user input within the output generates[3].

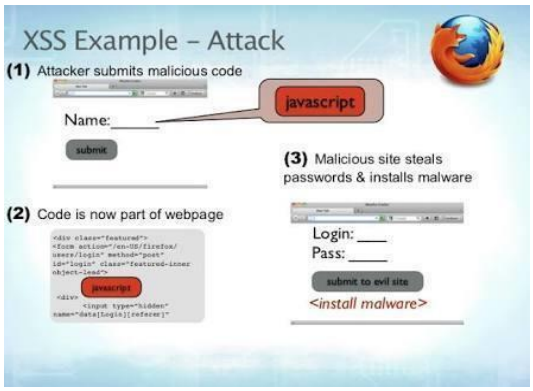


Fig. 3. XSS Attack

Data Leakage Attack

A data leakage is a security interruption in which sensitive, protected, viewed by an individual unofficial to user. Data leakage may involve financial information such as credit card or bank details, personal health information. The most data leakage involve over unprotected and vulnerable non-structured data files, documents, and important information.

V. CONCLUSION

We can conclude that, In the literature survey, there are some drawbacks which overcome in our honeypot concept. We explained honeypot system in detail and implemented middle interaction production honeypot. Our main goal is to secure the server side using honeypot from the attackers. The honeypot is relatively a new technology and having good scope for future work. Honeypot can be used with other well established security tools such as IDS or firewall to make them more secure and effective.

REFERENCES

[1] T.Kaur and V. Malhotra, "Comparison of network security tools-Firewall Intrusion Detection System and Honeypot", International Journal of Enhance Research in Science Technology & Engineering, ISSN:2319-7463 ,pp(200-204),Feb-2014.
[2] H.N. Pratihari, ”Etended Honeypot Framework to Detect Old/New Cyber
[3] Attacks”IJEST,ISSN:0975-5462,March 2011.
[4] P.Thopate, “Cross Site Scripting Attack Detection & Prevention System”, IJARCE T,ISSN:2278-1323,Nov 2014.
[5] Yogendra Kumar Jain, "Honeypot based Secure network System", International Journal on Computer Science and Engineering,ISSN:0975-3397,Feb-2011.
[6] Srivathsa S Rao, "Web based honeypots network", International Journal of Scientific and Research Publication,ISSN:2250-3153,August-2013.