International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 4 (May 2013), PP. 71-74

A Review on Honeypot as an Intrusion Detection System for Wireless Network

Pushpa Rani[1], Yashpal Singh[2], S Niranjan[3]
[1]M.Tech Student, Department of Computer Science & Engg. , PDM College of Engineering for Women.
[2]Assistant Professor, Department of Computer Science & Information Technology , PDM College of Technology & Management , Bahadurgarh Jhajjar Haryana.
[3]Professor, Department of Computer Science & Information Technology , PDM College of Technology & Management , Bahadurgarh Jhajjar Haryana.

Abstract:- Honeypots are decoy computer resources set up for the purpose of monitoring and logging the activities of entities that probe, attack or compromise them. Honeypot does work as an Intrusion Detection System which detect the attacker in a network. Activities on honeypots can be considered suspicious by definition, as there is no point for users to interact with these systems. In this paper, we proposed a honeypot system in the wireless network to attract the attackers. We have used different fake websites to do so. Honeypot helps in detecting intrusion attacking on the system. The information gathered by watching a honeypot being probed is invaluable. The honeypot act as a normal system in the network having fake detail or invaluable information. It gives information about attacks and attack patterns. The Honeypot will make the attacker to attack the particular sites and side by side monitor its illegal steps to confirm about its identity. This proposed work will make the IP address of attacker to be blocked for further access of any site in the network. The proposed model has more advantages that can response accurately and swiftly to unknown attacks and lifetime safer for the network security. In future the network can be preserved by getting the information regarding the attacker from the Honeypot system.

Keywords:- Honeypot, Network, Security, Wireless.

I. INTRODUCTION

Intrusion detection is the process of detecting attempts to gain unauthorized access to a network or to create network degradation. Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.[2]

Need intrusion detection:-

1. Information carried over networks are more valuable
2. The WWW has become a common delivery medium
3. Anonymous attackers

A honeypot is a system that is built and set up in order to be hacked. Honeypot can be used in a different scenario as intrusion detection facility (burglar alarm), defense or response mechanism. Moreover, Honeypot can be deployed in order to consume the resources of the attacker or distract him from the valuable targets and slow him down that wastes his time on the honeypot instead of attacking production systems[1]. The main functions of a honeypot are:

1. To divert the attention of the attacker from the real network, in a way that the main information resources are not compromised
2. To capture new viruses or worms for future study
3. To build attacker profiles in order to identify their preferred attack methods, similar to criminal profiles used by law enforcement agencies in order to identify a criminal's *modus operandi*
4. To identify new vulnerabilities and risks of various operating systems, environments and programs which are not thoroughly identified at the moment.[1]

A. Type of interaction level of honeypots

The level of interaction[2] of Honeypots defines the range of attacks possible through the Honeypot. [2]. On the basis of the possible range of attack the Honeypots are categorized into two:

Low interaction Honeypot
High interaction Honeypot

1) Low interaction Honeypots: In low interaction Honeypots there is no operating system that an attacker can operate on. Instead operating system emulators are installed which interacts with the attacker. It offers limited interaction level to the attackers. It will be used to scan the port and generates attack signatures.

2) *High interaction Honeypots:* High interaction Honeypots have actual operating system and has tools which motivates the attacker to attack so that their attack strategies can be recorded and later analysed. As high interaction Honeypot offers 24/7 internet connectivity, it attracts the attackers and to reduce the load of these high interaction Honeypots, only traffic filtered by low interaction. Honeypots is passed to them. So high interaction Honeypots basically process the packets sent only by malicious users.[2].

Currently there are a lot of Security techniques which includes firewalls and different IDS but due to limitations many unknown attacks could not be traced and the system get effected. Since the firewalls and IDSs are designed mostly for network level attacks, they are incapable of defending application level attacks.[7]. The proposed work is designed in such a manner that it works on the application level and captures the intruders directly effecting the database such as done through SQL injection attack.[8].

Features of Honeypot System:

The following features of the honeypot system makes it different from the others and complete our tour of construction.

1) It is based on real web application environments, constantly keeping surveillance on the data entry and taking instant reaction on detecting the intruder.
2) It can get complete attack sequence.
3) It captures the unknown attacks just by watching/monitoring the activities of the intruder.
4) It makes the network safer for the future.[7].

The Paper is organized as follows: Section II presents the related work on honeypot which has been already done and performed. Section III shows a brief idea about the proposed work.

Resources Required:

Tools/Platform used are:

- FRAMEWORK:- ASP.NET version 2 .0 with C#
- DATABASE:- SQL Server
- PLATFORM USED:- Windows XP

S/w Requirement specification:

- .NET framework 2.0
- Visual Studio.NET 2005
- ASP.NET
- ADO.NET
- SQLServer 2005
- Visual C#.NET
- HTML
- Internet Information Services (IIS) v 5.1

H/w Requirement specification:

- Pentium 3, 1.5 GHz and above
- 256 MB DDRAM or more
- 20 GB HDD
- Pen Drive 2Gb

Network Required:

WIRELESS NETWORK.

II. RELATED WORK

A) Already existing Honeypot products are:-

1) Honeyd : Honeyd is a honeypot for linux/unix developed by security researcher Niels Provos. Honeyd was ground-breaking in that it could create multiple virtual hosts on the network (as opposed to just using a single physical host). The honeypot can emulate various operating systems and services.

2) HoneyBOT : HoneyBOT is a Windows medium-interaction honeypot by Atomic Software Solutions. It originally began as an attempt to detect by the Code Red and Nimda worms in 2001 and has been released for free public use since 2005[4]. HoneyBOT allows attackers to upload files to a quarantined area in order to detect trojans and rootkits.

3) Specter : Specter's authors describes Specter as a "honeypot-based intrusion detection system"[5]. The product is primarily a honeypot designed to lure attackers away from production systems. Specter has a few interesting features :

- Specter makes decoy data available for attackers to access and download.
- Specter can emulate machines in different states: a badly configured system, a secured system, a failing system (with hardware or software failures), or an unpredictable system.
- Specter actively attempts to collect information about each attacker.

B) Related Work/Papers are summarized below:-

1) **"Design Considerations for a Honeypot for SQL Injection Attacks", Thomas M.Chen and John Buford, 5th Worshop on Security in Communications Networks, October 2009**. (In this Paper the Honeypot was created to emulate the appearance of common defence against SQL injection and they described considerations to implement an experimental honeypot with honeyd).

2) **"High Interaction Honeypot System For SQL Injection Analysis", Wei Huang, Jiao Ma and Kun Chai, 2011 International Conference of Information Technology.** (In this Paper they proposed a high-interaction web honeypot system for SQL injection analysis. By (i)modifying PHP extension for MySQL to intercept data-base requests and (ii)adopting exception based and signature based detection techniques).

3) **"Securing WMN using Hybrid Honeypot System", Paramjeet Rawat, Sakshi Goel, Megha Agarwal and Ruby Singh, International Journal of Distributed and Parallel Systems (IJDPS), May 2012**. (In this Paper, a Honeynet is proposed that is able to trap the attackers by analyzing their attack techniques and thereby sending the logs to a centralized repository to analyze those logs so as to better understand the technique used for attacking).

4) **"Hybrid Honeypot System for Network Security", Kyi Lin Lin Kyaw, Department of Engineering Physics, Mandalay**. (In this Paper, they described the usefulness of low-interaction honeypot and high-interaction honeypot and comparison between them. And then they proposed hybrid honeypot architecture that combines low and high interaction honeypot to mitigate the drawback).

III. PROPOSED WORK

This paper describes the important features of honeypot by attracting the attackers and saving the network in future. The System work as HoneyPot or the server which consist of fake websites and applications that attract the attacker/hacker. The websites have no connection with the real world, they were only meant for the attackers. If the user act according to the Honeypot then the particular user will be blacklisted. The system belongs to research honeypots and is deployed on real windows platform. It emulates vulnerable websites, tempting intruders to attack by providing large amount of attractive information and exposing vulnerabilities. Proposed work helps to detect the unknown attacks and secure the network in future.

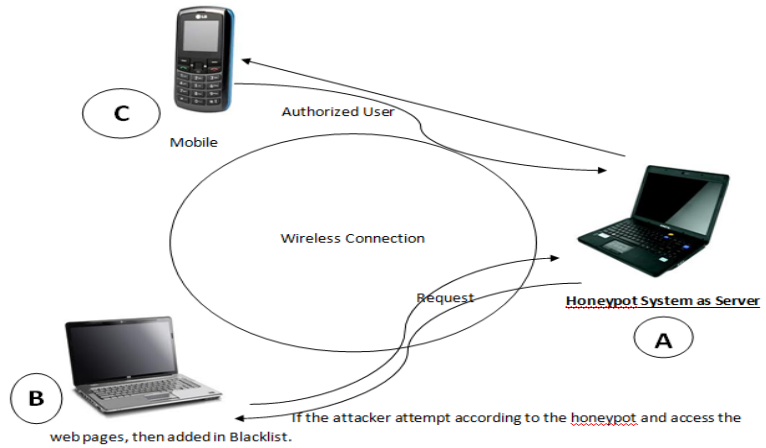

Fig. 1: Network between the systems and their working

From the above the figure this can be seen that a wireless network has been created and in that network we are having a System as our Honeypot System or Server that will attract the attacker by providing him fake and vulnerable web sites. The sites will provide fake and more and more disinformation to the attacker. If a normal user doesn't find any benefit in that sites then he will himself close that and does not continue, so the particular user will be placed in the whitelist while if the user/attacker found that if they hack or disturb the database in those particular sites and continue in that, will be blacklisted.

It consists of log having two list of database-

First(Blacklist)-It contains the list of IP blocks from the database and generate the output scheme.

Second(Whitelist)-It consist of IP addresses which should never be added(either you own them or because they belong to somebody whom you trust a lot).

The proposed work carried out with the help of different Case Studies through different vulnerable websites designed specially for attackers. Different Case Studies are:

Case Study : 1 Providing Greed to Attacker.

In this a normal Goggle Page has been created with an attached message that if anybody want to know the password of others then click on the button. And after that some information is gathered from the attacker to show him that he was using a genuine site. In this way if the attacker comes in trap will be blacklisted.

Case Study : 2 Capturing the intruder if he uses SQL Injection on the Login Page.

A simple Login Page has been created and a database too. If any attacker uses the SQL injection or the special characters to go into the database then that particular user will be blacklisted.

Case Study : 3 Fake Bank website attracting the attackers.

A bank login page will be shown to the attacker, he uses hit and trail method and guesses ID and password. The Honeypot will provide fake detail about some user to show him that his trail or the guess was correct and now he can do the changes or transfer money from that account. Side by side the Honeypot was monitoring its activities and blacklist the user.

IV. CONCLUSION

The proposed Honeypot system can make up for the shortcomings of firewalls and other IDSs. The Honeypot will make the attacker to attack the particular sites and side by side monitor its illegal steps to confirm about its identity. This proposed work will make the IP address of attacker to be blocked for further access of any site in the network. It obtains complete attack vectors and grasping the intention of the intruders. Moreover, it can clearly found the attack by saving the time of security researchers on reading log files and tracking intruders. Such Honeypot could be valuable tool for securing web applications when web applications are certain to continue to be attractive targets.

REFERENCES

[1]. Kyi Lin Lin Kyaw, Department of Engineering Physics, Mandalay Technological University, Pathein Gyi, Mandalay., "Hybrid Honeypot system for network Security," World Academy of Science, Engineering and Technology 48 2008.

[2]. "Securing WMN using Hybrid Honeypot System", Paramjeet Rawat, Sakshi Goel, Megha Agarwal and Ruy Singh, International Journal of Distributed and Parallel Systems (IJDPS), May 2012.

[3]. Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study," The 11th National Computer Security Conference, October, 1988.

[4]. Thomas M. Chen and John Buford, "Design Considerations for a honeypot for SQL Injection Attacks", LCN Workshop on Security in communications Networks, Switzerland; 20-23 October 2009.

[5]. Wei Huang and Jiao Ma, "High-Interaction Honeypot System For SQL Injection Analysis", International Conference of Information Technology, 2011.

[6]. "Honeypots, Honeynets", Honeypot & Honeynet Articles, Honeypot Links, Honeypot Whitepapers (Honeypots, Intrusion Detection Incident Response), Web, 27 july 2011,<http://WWW.honeypots.net>

[7]. From Wikipedia en.wikie,"en.wikipedia.org/wiki/wireless_network".