Network Security Enhancement through Honeypot based Systems

S Deepa Lakshmi [#1], G Arunkumar [*2,] V Madhu Viswanatham[$3]

[#] Student, School of Information Technology, VIT University Vellore, TamilNadu, India.
[*] Assistant Professor, School of Computer Science, VIT University Vellore, TamilNadu, India.
[$] Associate Professor, School of Computer Science, VIT University Vellore, TamilNadu, India.
[1] sdeepa.lakshmi2013@vit.ac.in
[2] arunkumar.g@vit.ac.in
[3] vmadhuviswanatham@vit.ac.in

Abstract—Computer Networks and Internet has become very famous nowadays since it satisfies people with varying needs by providing variety of appropriate services. Computer Networks have revolutionized our use of computers. Online bills, shopping, transactions and many other essential activities performed on the go by just a single click from our homes. Though it is a boon in this era, it also has its own risks and weaknesses too. Industries need to tussle to provide security to their networks and indeed not possible to offer a cent per cent security due to the intangible intelligence of hackers intruding into the network. This paper exploits the concept of honeypots for providing security to networks of industries which may not have custom intrusion detection systems or firewalls. The proposed model captures the various techniques used by hackers and creates a log of all hacker activities. Thus using this log, the production network system can be prevented from attackers.

Keywords- Honeypot, Honeynet, Network, Intrusion.

I. INTRODUCTION

The Internet is a network of networks. It is based on the concept of packet switching. Though the services offered by Internet are extensively used from a layman to multi-millionaire it also has its own defects. Many attacks on Internet are being identified and reported. Some of the common types of network attacks are eavesdropping, data modification, identity spoofing, password-based attacks and denial of service attacks. To overcome all these types of attacks an organisation usually installs an intrusion detection system to protect the confidential data exchanged over its network. The local network is then connected to the Internet thereby availing the employees to be online on the fly. Information security has three main objectives namely 1. Data confidentiality 2.Data integrity 3. Data availability. Data confidentiality ensures that the secure data can be accessed only by authorized persons. Data integrity allows secure modification of data. Data availability ensures that the data is available readily to authorized persons. Small scale industries often do not prefer on intrusion detection systems due to its installation and maintenance costs. Honeypots and Honeynets are an efficient alternative for such organizations. A Honeypot can literally be a computer which can act as a source for attacks. It attracts the hackers to try hacking it which in turn may log the techniques used by the attackers. This log is useful to prevent such attacks to the legitimate network. Honeypot computer usually do not have any important data or information to be secured. It only has fake services running on its ports to attract the attackers. There are many types of honeypots based on their deployment and design. Based on the deployment criteria honeypots may be classified into two types namely 1.Production honeypots 2.Research honeypots. Production honeypots are easily deployed in the live environment that may capture only some amount of information about the attacks. Research honeypot deployment is complicated and used mainly for research purposed by government organizations. On the basis of design, honeypots can be divided into 1.Pure honeypots, 2.High-interaction honeypots, and 3.Low-interaction honeypots. Pure honeypots are complete production systems. The honeypot computer is linked to the network and taps the attacks. Low-interaction honeypots allows restricted interaction with attackers and hence they are not infected by the attacks. High-interaction honeypots are vulnerable to attacks. No emulation takes place and hence more prone to get infected by attacks. Honeynet is a collection of honeypots installed to trap the attacker activities and log them.

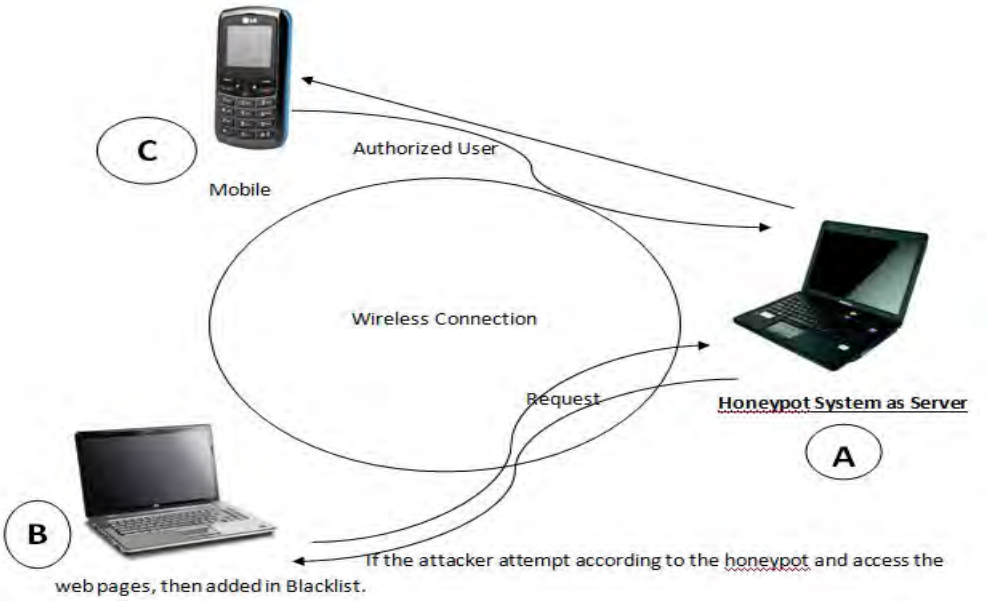

Fig 1: Network with Honeypot

II . RELATED WORK

The study about Honeypots has been over a decade and it is one among the fields which have high scope for research. Most important research papers on honeypots are being discussed in this section.

A. Research applied in LAN security

This paper proposes how honeypots can be applied in the LAN system incorporating physical and virtual honeypots. It focuses on variety of technologies like IDS, honeypot technology and firewall.

B. Honeypots to capture Network attack traffic

This paper proposed a system to solve the issues faced by honeyd which is an open source honeypot for UNIX. It focuses in solving the log size problem by designing two modules namely logging and log analysing modules.

C. Dynamic honeypot for Intrusion Detection

This paper proposed a dynamic honeypot design for dynamic networks. This model associates active and passive probing and virtual honeypots.

D. Securing WMN using hybrid honeypot system

This paper proposed an attack detection model for wireless mesh network using honeypot technique. A Honeynet is modelled to trap the attackers.

E. Banking security using honeypots

This paper proposed a secure system for banking applications using honeypot technology.

F. Visual analytic approach for SSH honeypots

This paper proposed an analytic model that can be used by experts to visualize SSH honeypot data. Experts can be able to quickly identify the sessions to trap the attackers.

G. Honeypots in network security

This paper proposed a security model for small scale industries which uses a hybrid structure composed of snort, Nmap and Xprobe.

III . PROPOSED WORK

In this paper, we have used the concept of honeypots for providing security against attackers. A honeypot computer is set up to act as an easily attacked prey than true or genuine systems. There are two goals for setting up a honeypot.

1. From the logged information learn how the attackers probe into the network.

2. Collect appropriate evidences for intrusions of the attackers to submit to law enforcement officers for legal action.

To achieve these goals, the honeypot systems should satisfy certain conditions.

1. The honeypot computer should be similar to other production systems.

2. Usage of interesting information in honeypots to attract hackers.

3. Restrict the traffic sent out to the Internet by an intruder.

A. Levels of Tracking

Hackers' information retrieved depends on the level of tracking set during setup. It may include firewall logs, system logs and sniffer tools.

a. Firewall logs

Setting up a firewall into a network is always very useful in addition to honeypot system. It helps in identifying the methods used by an intruder to penetrate into a honeypot computer. Firewalls have different notification capabilities like sms, pager etc.

b. System Logs

Windows and UNIX are majority operating systems used in Internet and supports logging feature. In Windows, Event Viewer is a tool which provides security by logging the events details. The User Manager provides user management and services run are captured using netsvc.exe. In UNIX, utmp, wtmp, btmp, lastlog are the user activity logs and Syslogd is an log to a remote server.

c. Sniffer Tools

These tools capture the packets that are flown between honeypot computer and the firewall. Sniffer tools collect more detailed information about intruders when compared to the system and firewall logs. They also offer storage of logs.

B. Building a Honeypot

a. Depending on the operating system the tools to be used for building a honeypot varies.

b. Major Pre-requisites

1. Computer or Workstation

2. Operating system (either Microsoft NT or RedHat)

There are many money-making honeypots readily available in the market namely Tripwire, Cybercop sting etc. These can be purchased from the market and installed into the local network.

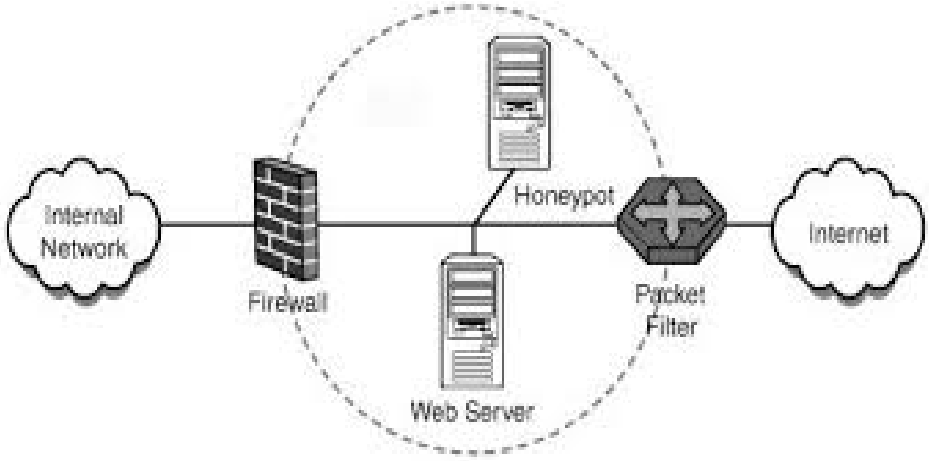

Fig 2: Honeypot Architecture

In this paper, we have implemented the honeypot for capturing hacker information like social security number and ip address. In a honeypot computer, a fake banking website is made available. A login page is displayed which requires the login id as the social security number and a password to enter into the bank network. Suppose a hacker tries to intrude into the bank network by providing wrong information or use sql injection techniques a log is captured for the provided details. The honeypot allows the hackers to enter into the login page as if his login details were validated and displays the page for doing fund transfer which is ultimately a fake page and thereby no harm can be done to the bank. By this way, a honeypot can be used to capture hacker information intruding into a local network used by small scale industries.

IV. CONCLUSION

The proposed design can block particular IP addresses of hackers and also provide evidences like SSN to the legal authorities for taking legal action. As a future enhancement more interesting facts can be added to attract the hackers. Due to the rapid development in honeypot usage, hackers started to focus on the methods to bypass the honeypots and intrude into the network. Network administrator should restrict these issues by using strong gateways. Log size is also a major constraint to be looked after. Growing logs are always a performance bottleneck and suitable steps should be taken for purging them in regular intervals.

V. REFERENCES

[1] Li Li et al, "The Design and Research of Honeypot System Applied in the Security of LAN", IEEE-2011
[2] R.C.Joshi et al, "A Honeypot System for Efficient Capture and Analysis of Network Traffic", IEEE-2008
[3] Iyad Kuwatly et al, "A Dynamic Honeypot Design for Intrusion Detection", IEEE- 2010
[4] Paramjeet Rawat, Sakshi Goel, Megha Agarwal and Ruby Singh, "SECURING WMN USING HYBRID HONEYPOT SYSTEM ",International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2011
[5] Pushpa Rani, Yashpal Singh, S Niranjan," A Review in Honeypot as IDS for Wireless Network", IJERD 2012
[6] Sandeep Chaware, "Banking Security using Honeypot ", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011
[7] Jop van der Lelie, Rory Breuk, "A visual analytic approach for analysing SSH Honeypots", IEEE2012
[8] Abhishek Sharma, "HONEYPOTS IN NETWORK SECURITY", International Journal of Technical Research and Applications 2013.
[9] Collin Mulliner et al, "Poster: HoneyDroid - Creating a Smartphone Honeypot", IEEE2013
[10] Radhika Goel, Anjali Sardana, and R. C. Joshi, "Wireless Honeypot: Framework, Architectures and Tools" International Journal of Network Security 2013
[11] Matthias Wählisch, Sebastian Trapp, Christian Keil†, Jochen Schönfelder, "First Insights from a Mobile Honeypot", ACM 978-1-4503-1419-0/12/08.