A Survey on Honeypots Security

Amit Kumar*
Sonia Kumari**

Abstract

With the increasingly use of computer technology and the Internet, information security becomes more important. The tradition defense mechanism to detect the security risk has been unable to meet the requirement of the people. The honeynet technology as a protection technology to make up for the traditional system. This research paper describes a brief review on network security techniques, Honeynetand HoneypotTechnology. A Honeypot is a process of deception trap. It is structured to lure an attacker into intending compromise the information systems in an organization. But it is required a correct deployment, if it is deployed correctly, can serve as an early-warning system and advanced security surveillance tool. It minimize the risks from attack. It is also analyses the ways in which attacker try to compromise an information and networks system, providing valuable insight into potential system loopholes. This paper gives idea how honeypot technology can be used to detect, identify and gather information for a specific threat& how it can be deployed for the purpose to enhance the level of security in organization and enterprise.

Keywords: Honeynet, Honeypot, Honeywall, Intrusion Detection

Introduction

Basically, information security is the primarily defensive process. Administrator of the Network use a firewall, intrusion detection system (IDS) and number of information security method to protect their network from data breaches, intruders etc. The firewall control the inbound and outbound traffic according to the policies that has been configured as required for the particular system. The intrusion detection system (IDS) deployed between the local area network and the internet for detecting suspicious packets.

Every technology have some deficiencies of these systems. In case of firewall [1]:-

1. It cannot protect the system against an attacks that bypass it. For example, dial in or dial-out capability.
2. The firewall does not protect against internal threaton the network.
3. The firewall does not protect against the transfer of virus files and programs.

In case of Intrusion Detection Systems (IDS) [2]:-

1. High level of false positive and false negative alerts.
2. Must know signature detection patter [3].

The use of honeypots can overcome the deficiencies of intrusion detection system (IDS) and Firewall. The main advantage of honeypots is that they are designed for the interaction with attackers. This is the way honeypots collect smaller set of data with very high value. But there are also some deficiencies like others technologies. If we install honeypots behind the firewall and intrusion detection system (IDS), it can serve as part of defense in-depth system and can be used to detect attackers. It is called a honeynet.

Honeynet

The concept of the honeynet technology was started first in 1999 after the published of paper named "To Build a Honeypot" by Mr. lance Spitzer, founder of the Honeynet technology. In his paper, Mr. Spitzer says that instead of developing technology that emulated systems to be attacked, why we do not install system behind the firewall that waiting to be hacked.Honeynet are neither a product nor a software

Amit Kumar*
Scientific Assistant (Adhoc)
IGIPESS, B-Block, Vikaspuri, Delhi

Sonia Kumari**
Assistant Professor (Adhoc)
IGIPESS, B-Block, Vikaspuri, Delhi

solution that it install on the software. Basically honeynet is a architecture that create a highly controlled network in which all activity is controlled and captures in a proposed manner [4][5]. By doing together with firewall, intrusion detection system(IDS), and anti-worm software, honeypots form into a honeynet security defense system that ensure about the network security as shown in the figure 1.

Basic elements of Honeynet are:

1. A firewall computer
2. Intrusion Detection System (IDS)
3. Log server
4. Honeypots

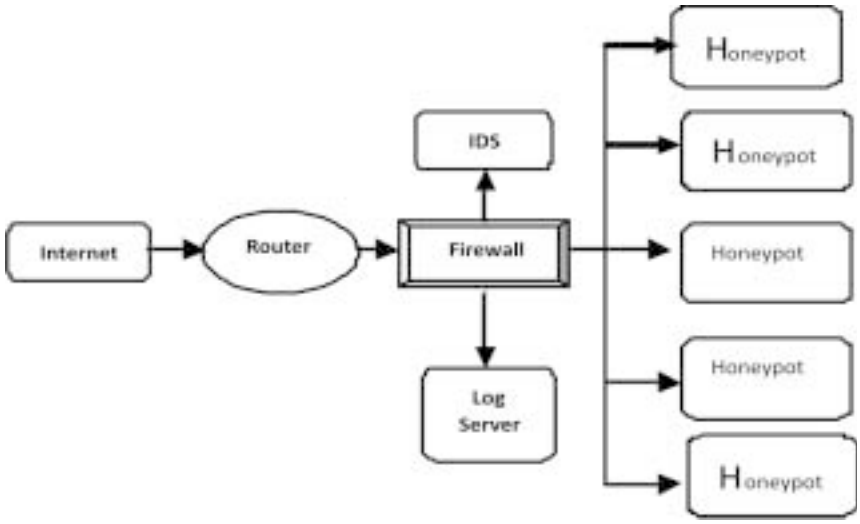

Figure 1: Network Security

Honeywall [6] is a key to design of honey net, all the data that access to the honey net must go through the honey wall and it separate the honey network and external network which is control the entire honey net network hub as shown in figure 2. It has three network interfaces.

1. External Network interface that connected with service host.
2. Internal Network interface that connected with the honeynet.
3. Network Interface connection logging server that connected with internal network interface.

Honeywall facilitate the remote management and intrusion prevention system detection rules and policies for timely updates.

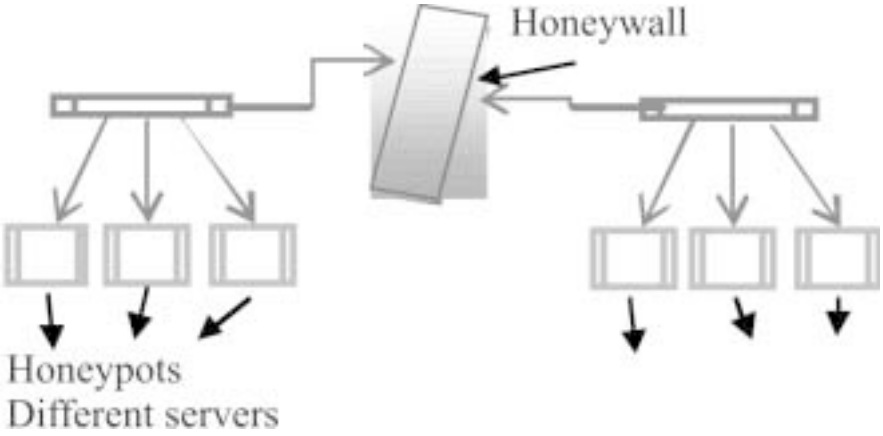

Figure 2: Honeywall Network Hub

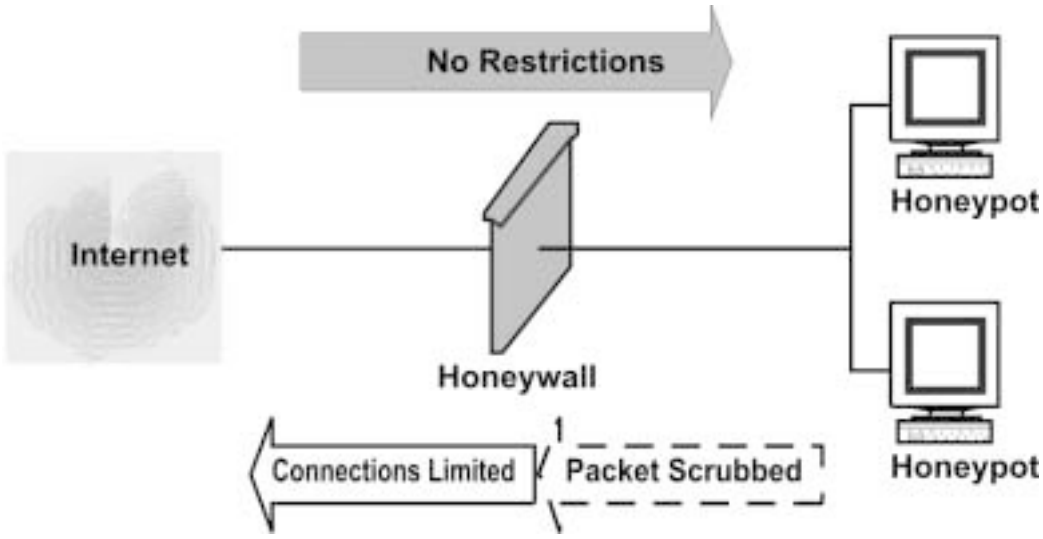

Figure 3: Honeyball

Basic Requirement for the implementation of honeynet:-

1. **Data Control** is the containment of activity that mitigates the risk. We always try to ensure that once an attacker is found within our honeynetaccidentally or purposefully harm the other honeynet. This is more challenging scenario as shown in figure 3.
2. **Data Capture** is the process of monitoring and logging of all of the threat's activities within the honeynet or system. The challenge is to capture the data without the threat.
3. **Data Analysis** is another detection of worthless if do not have an ability to convert the data. We must have some ability to analyze the data.
4. **Data Collection** applies to those organizations that have multiple honeynets in distributed environments.

Honeypot

Lance Spitzner, founder of the Honeynet Project said that a honeypot is a system structured to learn how "black-hats" enquiring for and utilize weaknesses in an IT System [7]. It can also be defined as "an

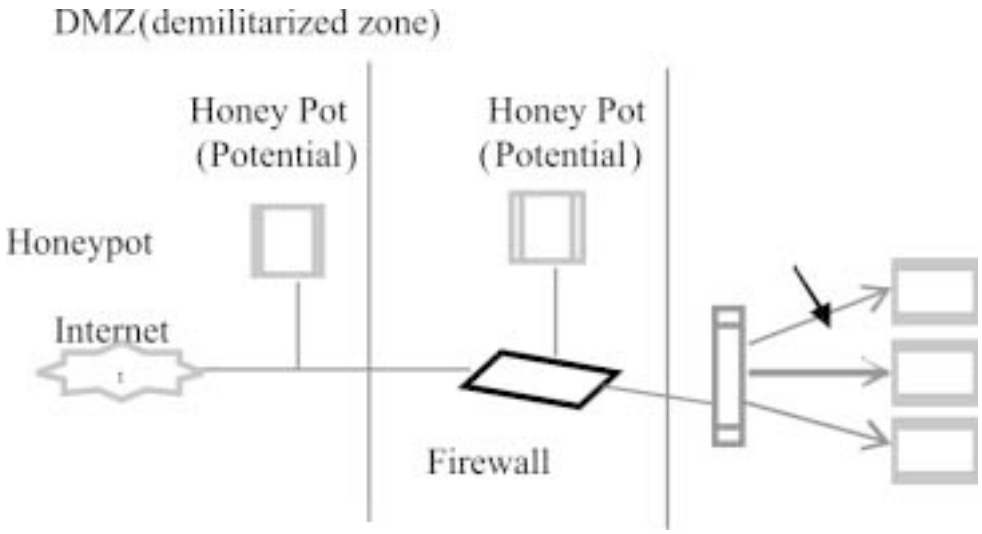

Figure 4: Honeypot

information system resource whose value lies in unauthorized or illicit use of that resource" [8]. In other words, it is a lure, put out on a network as bait to attract the attackers. Honeypots are a virtually machines that has been designed to imitate real machines.

A Honeypot works by making fool the attackers into believing that it is legitimate system, as they attack the system without knowing that they are being observed covertly. When an intruder try to attempts to compromise a honeypot, attack-related information, like IP address of the intruder, will be captured.

It can be used for the purpose of production or research. A production honeypot is used for risk mitigation.

Research Honeypots are the example of real operating systems and services that intruders can interact with the system. That's why it involves higher risk. They collect huge information regarding the situation of the types of attacks being execute. It provides the more improved attack prevention and attack detection information captured during the process.

Classification of Honeypots

Honeypots are classified into two categories. These are the following.

1. Low-interaction honeypots: It is used for production purposes.
2. High-interaction Honeypots: It is used for research purposes.

Low-Interaction Honeypots

It is work by imitating the certain services and operating systems and have a limited interaction.

Advantages

The advantages of low-interaction honeypots are that they are simple and easy to deploy and maintain. In addition, the limited emulation available or allowed on low-interaction honeypots reduces the potential risks brought about using them in the field. However, with low-interaction honeypots, only limited information can be obtained, and it is possible that experienced attackers will easily recognize a honeypot when they come across one.

Example:

Facades:

It is a kind of software emulation of a selected services or application that provides a wrong perception of a selected host. When a façade is attacked, it collects the data about the intruder. Some facades provide partial application-level behavior and some others simulate the target service.

Facades provide easy installation as it requires minimal installation effort and devices. It can emulate a large variety of systems. We know that, it is not a real systems, it does not have any other real vulnerabilities themselves. It is used by small to medium sized organization or by big organization in coordination with other types of security technology because it provides only basic information about a potential threat.

High-Interaction Honeypots

High-Interaction honeypots are complex as compared with the low-interaction honeypots because it uses a real operating systems, services and applications. For example, a SSH server will be built if the objective is to collect the information about attacks on a particular SSH server or services.

It is a kind of system policies that provides the real system for direct interaction to the attackers. There are not any kind of restriction are imposed on attack behavior. This model allows administrator to gather extensive information about the attacker's method. Enough protection measures need to be implemented as required in the system.

Example:

1. Sacrificial Lambs

It is a system intentionally left vulnerable to attack. The administrator will examine the honeypot to determine if it has been compromised and if so what was done to it.

2. Instrumented Systems

It is an off-the-shelf system with an installed operating system and kernel level modification to provide information, containment, or control. The OS and kernel have been modified by engineers of security. After the modification in operating system and kernel,

the running system will leave the in the network as a real target. This model combines the strengths of both sacrificial lambs and facades.

3. Spam Honeypots

Honeypot technology is used for identifying spam and email harvesting activities. Honeypots have been installed to study how spammers detect open mail relay system. Machine run as simulated mail server proxy server and web server. Spam email is received and analyzed [9].

Strategies of honeypot deployment

For minimize the risk and maximize the soundness of the honeypots, it is required the installation should be carefully planned.

1. Honeypots install with the production server. The honeypot need to mirror the original information and services from the production server in order to lure the intruders. In that model, honeynet security loosened slightly that increase the probability of being compromised. The honeynet capture attack related data. When a successful attack takes place on the honeypot within the network, that compromised honeypot machine may be used to scan for other threat target in the network. The main drawback of implementing honeynet within the production system.
2. Paired the servers with a honeypot. It routed the suspicious traffic destined for the server to the honeypot. For example, traffic on port number 80 on TCP can be directed to a web server IP address as normal and other traffic to the web server will be routed towards the honeypot.
3. Build a Honeynet: It is a collection of honeypots that imitate and mirror an original network. This will show to intruders as if different types of application are available on several platforms. A honey net provides an early warning system against the attacks and offers a good way to analyses the intruder's intention. The Honeynet Project [10] is an excellent example of a research honeynet.

Building the Network of Honeypot

Building a honeypot network is not difficult. I build it at my college computer lab and it has been successfully intruded number of times.

I used window 8 system with a DVD-ROM drive. It was the best as compared others that is available as it is more secured.

I install a program called Snort. This program is an open source network intrusion prevention and detection system that is utilizing a rule-drive language. It is combines the benefits of signature, protocol and anomaly based inspection methods. Snort is the most popular and widely deployed intrusion detection and prevention technology. In fact, it has the standard for the industry. Snort is a free program that is extremely powerful. This is part of an intrusion detection system.

I also found Windows based Honeypot that is HoneyBot. It works by opening on 1000 UDP and TCP listening sockets on computer and these sockets are designed to mimic vulnerable Services. When an attacker connects to these services they are fooled into thinking they are attacking a real server. The honeypot safely captures all communications with the attacker and logs these results for future analysis.

Examples of Honeypot

1. Deception Toolkit [11]: DTK was the first open source honeypot. It is a collection of Perl scripts and c code that emulates a variety of services.
2. LaBrea [12]: It is structures to slow down or stop attacks. It can run on Windows or UNIX.
3. Honeywall CDROM [13]: It is a bootable CD with a collection of open source software. It makes honeynet deployments simple and effective by automating the process of deploying a honeynet gateway known as a honeywall. It is used to capture, control and analyses all inbound and outbound honeynet activities.
4. Honeyd [14]: This very powerful, low-interaction honeypot. It is run on both UNIX and windows platforms. It can monitor the IPs that is unused, simulate thousands of virtual hosts at the same time and monitor all UDP and TCP based ports.
5. Honeytrap [15]: It is a low-interaction honeypot technology that is designed to observe attacks against network services. It helps administrators to collect information regarding known or unknown network-based attacks.

6. HoneyC [16]: It is a client honeypot that initiates connections to aserver. The main objective of that technology to find malicious servers on a network.
7. HoneyMole [17]: It is a tool for the deployment of honeypot farms, or distributed honeypots, and transport network traffic to a central honeypot point where data collection and analyses can be undertaken.
8. Symantec Decoy Server [18]: This a type of honeypot intrusion detection system that detects and monitors unauthorized access and system misuse in real time.
9. Specter [19]: It is a smart honeypot-based intrusion detection system. It can emulate 14 different operating system and have acceptability to monitor 14 different network services and trap.

Result

The result was too good. It was surprising to see how fast the computer was attacked. I let it run for eight hours and found port 162 got quite a bit of scanning while port 67 and 68 were occasionally hit as well. Port 162 is commonly known as SNMP (simple network management protocol) trap. It looks every 3 to 5 seconds, ports were being scanned to see if they were open or closed. This was my first experience using a honeypot on system.

Conclusion

As the growing IT field, there is a requirement to strengthen its security. Preventive and Detective method measures used to improve IT Security. To improve our Security, we must having a knowledge of intruders, attackers, hackers, etc. Hackers can hack our computer. Attackers are constantly scanning our network looking for vulnerable loopholes and open ports. But without the knowledge of the enemy, we cannot defend our network or system. We have to think like a hacker in order to stop a hacker. Honeypots can be used simply to confuse and deflect attacks or to collect evidence. There are many free Windows based and Linux based honeypot programs available to individuals and companies.

Honeypots is a technology. Every technology have their advantages and disadvantages as this is possible in honeypots like other technologies. It is a useful tool for deception and apprehend the intruders that ensnare the information and create alerts when someone is trying to interact with them. This takes of intruders provides the valuable information for analyzing their attacking mode of techniques and methods. Because honeypot capture and collect data.

There are some disadvantage of that technology. It only track and capture activity that directly interacts with them. It cannot detect that attacks against other systems in the network. This is possible be the most controversial drawback of honeypots.

References

1. Holostov, V., Neystadt, John, *"Automated identification of firewall malware scanner deficiencies*, in United State Patent Application Publication, Published date Sep., 18, 2008.
2. http://cryptome.org/sp800-31.htm accesed on January 8, 2015 in the Internet
3. Renuka Prasad B et al., "Hybrid Framework for Behavioral prediction of Network Attack using Honeypot and Dynamic Rule Creation with Different context for Dynamic Blacklisting", RV college of Engineering, Banglore, Karnataka, IEEE, I.S.B.N : 987-14244-5726-7, pp-471-476.
4. Ryan Talabis, "Honeynets: A Honeynet Definition:, A Student IT Security Awareness Initiative by the Philippine Honeynet Project.
5. "Know Your Enemey : Honeynets.", Honeynet Project.
6. Peng Hong et al. "Intrusion Prevention system in the Network of Digital Mine" Chine University of Mineing Mechanical and Electrical Ebngineering Beijing, Chine IEEE,2010,Vol. 6, pp:296-299.
7. http://rootprompt.org/article.php3?article=210 accessed on jan 25, 2015 on the Internet.

8. http://www.spitzner.net/honeypots.html accesses on the Internet.
9. http://www.honeyd.org/spam.php accessed on jan 25,2015 on the Internet.
10. http://www.honeynet.org accessed on Jan 26, 2015 on the Internet.
11. http://www.all.net/dtk/index.html accessed on Jan 26, 2015, on the Internet.
12. http://labrea.sourceforge.net/labrea-info.html accessed on Jan 26, 2015 on the Internet.
13. http://www.honeynet.org/tools/cdrom/ accessed on Jan 27, 2015 on the Internet.
14. http://www.honeyd.org accessed on Jan 27, 2015 on the Internet.
15. http://honeytrap.mwcollect.org accessed on Jan 27, 2015 on the Internet.
16. http://www.client-honeynet.org/honeyc.html accessed on Jan 28, 2015 on the Internet.
17. http://www.honeynet.org.pt/index.php accessed on Jan 28, 2015 on the Interenet
18. http://www.symantec.com/business/support/documentation. jsp?language=english&view=manuals&pid=51899 accessed on Feb 1, 2015 on the Internet
19. http://www.specter.com/default50.htm.