Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 4; April-June, 2015 pp. 383-386

http://www.krishisanskriti.org/acsit.html

Active Defence System for Network Security – Honeypot

Sindhu S Pandya

Laxmi Institute of Commerce and Computer Application, Sarigam
E-mail: sindhubhilai@yahoo.com

Abstract—*Honeypot is an active defence system for network security that traps attacks, records intrusion information about tools and activities of the hacking process, and prevents attacks outbound the compromised system. Honeypots have a big advantage that they do not generate false alerts as each observed traffic is suspicious, because no productive components are running on the system. This paper will first introduce honeypots, its types and uses, features of honeypots and finally conclude by looking at the future of honeypots and honeynets.*

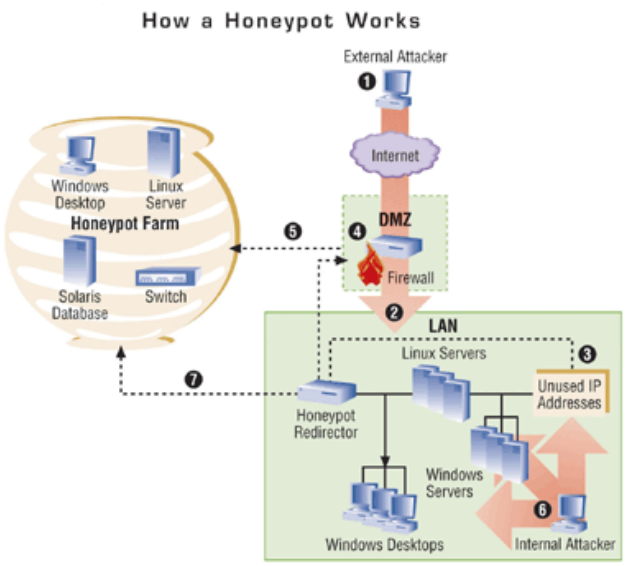
1. INTRODUCTION

Global communication is getting more important every day. At the same time, computer crimes are increasing. Computer security is among one of the main areas of information technology. An intruder can be defined as somebody attempting to break into an existing computer termed as a hacker or cracker. When combined with the increase in networking speed has made intrusion detection a challenging process. In this section we describe network intrusion detection systems, the traditional approach for network security. We then introduce and provide a brief history of honeypots. The section concludes with a discussion of the general advantages and disadvantages of honeypots.

1.1 Honeypots

The goal of an Intrusion Detection System (IDS) is to "identify, preferably in real time, unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators". Today's standard of security is using specifically configured firewall in combination with the Intrusion Detection System (IDS). But using only IDS is not sufficient. Attacker will attack in system, so that we can record all activities done by attacker that will help us to prevent actual data from these type of attackers, this technology is called as Honeypot. A honeypot is a deception trap, designed to entice an attacker into attempting to compromise the information systems in an organisation. If deployed correctly, a honeypot can serve as an early-warning and advanced security surveillance tool, minimising the risks from attacks on IT systems and networks.

A honeypot is primarily an instrument for information gathering and learning. A honeypot is an information system resource whose value lies in the unauthorized zed or illicit use of that resource.



The two main reasons why honeypots are deployed are:

1. To learn how intruders probe and attempt to gain access to your systems and gain insight into attack methodologies to better protect real production systems.
2. To gather forensic information required to aid in the apprehension or prosecution of intruders.

1.2 History of Honeypot

1990-1991: It is the first time that honeypot studies released by Clifford Stoll and Bill Cheswick.

1997: Deception Toolkit version 0.1 was introduced by Fred Cohen. After Clifford Stoll and Bill Cheswick.

1998: First commercial honeypot was released known as CyberCop Sting.

1998: BackOfficer Friendly honeypot was introduced which was free and easy to configure. It was working under Windows operating system.

1999: Honeynet project started at this year.

2000-2001: Honeypots started to be used for capturing malicious software from internet and being aware of new

threats. Companies began to use honeypots in their systems to improve security and see the malicious traffic.

2002: Honeypot concept became popular and honeypots improved their functionalities, so they became more useful and interesting for both researchers and companies.

1.3 Types of Honeypots

Based on the service level there are two broad categories of Honeypots, High-interaction and Low-interaction. **High-interaction Honeypots** lets the hacker to interact with the system with the goal of capturing the maximum amount of information on the attacker's techniques, whereas, **Low-interaction Honeypots** present the hacker emulated services with a limited subset of the functionality they would expect from a server, with the intent of detecting sources of unauthorized activity. Low-interaction honeypots that are often used for production purpose and high interaction honeypots that are used for research purpose.

Low interaction honeypots is also known as GEN-I honeypot. This is a simple system which is very effective against automated attacks or beginner level attacks. They work by emulating certain services and operating systems and have limited interaction. The attacker's activities are limited to the level of emulation provided by the honeypot. For example, an emulated FTP service listening on a particular port may only emulate an FTP login.

The advantages of low-interaction honeypots are that they are simple and easy to deploy and maintain. However, with low-interaction honeypots, only limited information can be obtained, and it is possible that experienced attackers will easily recognise a honeypot when they come across one.

Example: Façades

A façade is a software emulation of a target service or application that provides a false image of a target host. When a façade is probed or attacked, it gathers information about the attacker. Some façades only provide partial application-level behaviour, while others will actually simulate the target service down to the network stack behaviour. The value of a façade is defined primarily by what systems and applications it can simulate, and how easy it is to deploy and administer.

High-interaction honeypots consists of the following elements: resource of interest, data control, data capture and external logs. They are also known as GEN-II honeypots and started development in 2002. They are more complex, as they involve real operating systems and applications. For example, a real FTP server will be built if the aim is to collect information about attacks on a particular FTP server or service.

Example: Spam Honeypots

Honeypot technology is also used for studying spam and email harvesting activities. Honeypots have been deployed to study how spammers detect open mail relays. Machines run as simulated mail servers, proxies and web servers. Spam email is received and analysed to ascertain the reasons why they were received. In addition, an email trap can be set up, using an email address dedicated to just receiving spam emails.

Based on the usage level there are two broad categories of Honeypots, Research Honeypots and Production Honeypots.

Research Honeypots are deployed and used by researchers or curious individuals. These are used to gain knowledge about the methods used by the black hat community. They help security researchers learn more about attack methods and help in designing better security tools. They can also help us detect new attack methods or bugs in existing protocols or software. They can also be used to strengthen or verify existing intrusion detection systems. They can provide valuable data which can be used to perform forensic or statistical analysis. Research honeypot is primarily for learning new attacking methods and tools.

Production Honeypots are deployed by organizations as a part of their security infrastructure. These add value to the security measures of an organization. These honeypots can be used to refine an organization's security policies and validate its intrusion detection systems. Production honeypots can provide warnings ahead of an actual attack. They protect the target system by deceiving and detecting attacks, giving alerts to administrator.

1.4 Examples of Honeypot Systems

1. **Honeywall CDROM8**: The Honeywall CDROM 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 can capture, control and analyse all inbound and outbound honeynet activity.
2. **Honeyd**: Created by Niels Provos, Honeyd is a powerful, low-interaction Open Source honeypot, and can be run on both UNIX-like and Windows platforms. It can monitor unused IPs, simulate operating systems at the TCP/IP stack level, simulate thousands of virtual hosts at the same time, and monitor all UDP and TCP based ports.
3. **Specter**: Specter is a commercial production honeypot whose value lies in detection. It's windows based software which offers 14 different network services and traps. Specter is a low interactive honeypot which fakes the reply of attacker's request. Attacker can't utilize the application to interact with the OS.
4. **Back Officer Friendly (BOF)**: BOF is designed to emulate a Back Officer server. BOF **is** developed by Marcus Ranum and crew at NFR. It is **a** lightweight honeypot and free to distribute. BOF represents an accurate distillation of the ideas and insights of honeypot. BOF emulates several common services such as http, ftp, telnet and mail. BOF user can have clear view of the attacking process.

5. **Honeytrap**: This is a low-interactive honeypot developed to observe attacks against network services. It helps administrators to collect information regarding known or unknown network-based attacks.
6. **HoneyMole**: This 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 analysis can be undertaken.

2. SECURITY ISSUES

Honeypots don't provide security for an organization but if implemented and used correctly they enhance existing security policies and techniques. There are two views of how honeypot systems should handle its security risks.

- **Honeypots that fake or simulate:** There are honeypot tools that simulate or fake services. They deceive an attacker to think they are accessing one particular system. A properly designed tool helps in gathering more information about a variety of servers and systems and can be used as alerting systems.
- **Honeypots that are real systems:** These honeypots don't fake or simulate anything and are implemented using actual systems and servers that are in use in the real world. These honeypots have a high risk factor and cannot be deployed everywhere. They need a controlled environment and administrative expertise.

2.1 Advantages of Honeypots

1. They collect small amounts of information that have great value. This captured information provides an in-depth look at attacks that very few other technologies offer.
2. Honeypots are designed to capture any activity and can work in encrypted networks.
3. They can lure the intruders very easily.
4. Honeypots are relatively simple to create and maintain.

2.2 Disadvantages of Honeypots

1. Honeypots add complexity to the network. Increased complexity may lead to increased exposure to exploitation.
2. There is also a level of risk to consider, since a honeypot may be comprised and used as a platform to attack another network. However this risk can be mitigated by controlling the level of interaction that attackers have with the honeypot.
3. It is an expensive resource for some corporations. Since building honeypots requires that you have at least a whole system dedicated to it and this may be expensive.

3. ADVANCEMENTS

3.1 Honeynets and Honeyfarms

Grouping honeypots form honeynets and honeyfarms. Honeyfarms tend to be more centralized. Grouping honeypots help to mitigate the deficiencies of traditional honeypots. For example, honeypots often restrict outbound traffic in order to avoid attacking non-honeypot nodes which allows honeypots to be identified by an attacker. Use honeyfarms as redirection points for outbound traffic from each individual honeypot. These redirection nodes also behave like real victims. Figure 1 shows the redirection of outbound traffic from a honeypot to another node in the honeyfarm. Honeynets are mainly used for research work. Honeynet is more interactive than honeypot and strongly resemble an actual net.

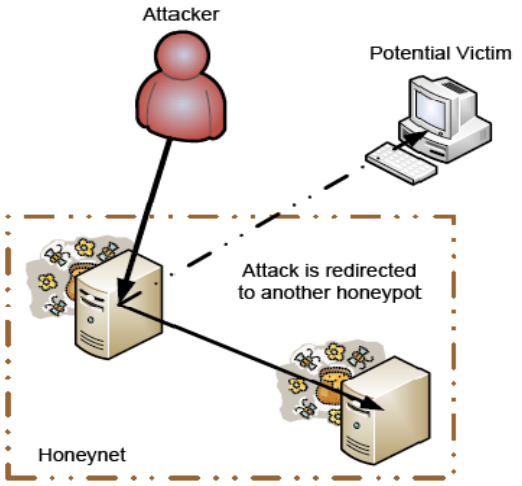


Fig. 1: Redirecting an outbound attack in a honeynet

3.2 Shadow Honeypots

Shadow honeypots are combination of honeypots and anomaly detection systems (ADS), which are another alternative to rule-based intrusion detection systems. Shadow honeypots first segment anomalous traffic from regular traffic. The anomalous traffic is sent to a shadow honeypot. If an attack is detected by the shadow honeypot, any changes in state in the honeypot are discarded. If not, the transaction and changes are correctly handled.

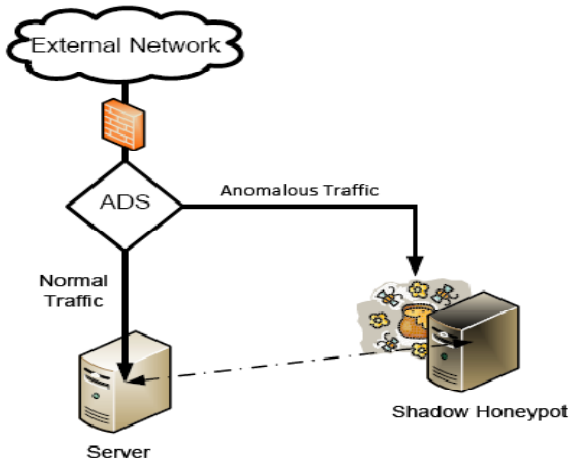


Fig. 2: Segmenting traffic in a shadow honeypot system

4. CONCLUSION

Honeypots becoming highly-flexible solution, Not only their deployment and management become more cost-effective , but also provide a much better integration into the system, thereby minimizing the risk of human error during manual configuration. Honeypots have their advantages and disadvantages. They are clearly a useful tool for luring and trapping attackers, capturing information and generating alerts when someone is interacting with them. The activities of attackers provide valuable information for analysing their attacking techniques and methods. Because honeypots only capture and archive data and requests coming in to them, they do not add extra burden to existing network bandwidth.

However, honeypots do have their drawbacks. Because they only track and capture activity that directly interacts with them, they cannot detect attacks against other systems in the network. Furthermore, deploying honeypots without enough planning and consideration may introduce more risks to an existing network, because honeypots are designed to be exploited, and there is always a risk of them being taken over by attackers, using them as a stepping-stone to gain entry to other systems within the network. This is perhaps the most controversial drawback of honeypots.

REFERENCES

[1] http://www.macom.com/

[2] http://www.honeyathome.org/

[3] http://www.symantec.com/connect/articles/open-source-honeypots-part-two-deploying honeyd-wild

[4] http://www.honeyd.org/

[5] http://www.honeynet.org/papers/

[6] Jian Bao and Chang-peng Ji, and Mo Gao, “Research on network security of defense based on Honeypot”, IEEE International

[7] Conference on Computer Application and System Modeling (ICCASM), vol. 10, pp. V10-299 - V10-302, 2010.

[8] 12lhonepet Project.

[9] www.honeynet.orgrgimisc/project.html

[10] Talabis,R.,2005.Honeypots 101: Risks and Disadvantages.