Honeypot

Narinder Kaur
AP CSE, IET Bhaddal
er.narinder@gmail.com

Abstract
Honeypot is a supplemented active defense system for network security. It traps attacks, records intrusion information about tools and activities of the hacking process, and prevents attacks outbound the compromised system. Integrated with other security solutions, honey pot can solve many traditional dilemmas. Located either in or outside the firewall, the honeypot is used to learn about an intruder's technique as well as determine vulnerabilities in the real system ". A honey pot is used in the area of computer and Internet security. It is a resource which is intended to be attacked and compromised to gain more information about the attacker and the used tools. It can also be deployed to attract and divert an attacker from their real targets. One goal of this paper is to show the possibilities of honeypots and their use in a research as well as productive environment. Compared to an intrusion detection system, honey-pots have the 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 fact enables the system to log every byte that flows through the network to and from the honeypot, and to correlate this data with other sources to draw a picture of an attack and the attacker.

Keywords: Honeypot, IDS, Internet Security, shadow honeypots, traffic management.

1. Introduction

Global communication is getting more important every day. At the same time, computer crimes are increasing. Countermeasures are developed to detect or prevent at-tacks - most of these measures are based on known facts, known attack patterns. By knowing attack strategies, countermeasures can be improved and vulnerabilities can be fixed. To gather as much information as possible is one main goal of a honeypot. Generally, such information gathering should be done silently, without alarming an attacker. All the gathered information leads to an advantage on the defending side and can therefore be used on productive systems to pre-vent attacks. A honeypot is primarily an instrument for information gathering and learning. Its primary purpose is not to be an ambush for the blackhat community to catch them in action and to press charges against them. The focus lies on a silent collection of as much information as possible about their attack patterns, used programs, purpose of attack and the blackhat community itself. In practice, honeypots are computers which masquerade as unprotected. The honeypot records all actions and interactions with users. Since honeypots don't provide any legitimate services, all activity is unauthorized (and possibly malicious).

2. Honey pots

2.1 Honey pot Basics

It is a security resource used to detect, deflect or counter attacks attempts at unauthorized use of information system. It consist of a computer ,data or a network site that seems to be a part of network but actually it is not .It is an isolated ,protected and monitored terminal which seems to have valuable information for the attackers. Honeypots can be defined in three layered networks:

- Prevention: Honeypots can be used to slow down or stop automated attacks
- Detection: It is used to detect unauthorized activity and capture unknown attacks. Generate very few alerts, but when they do you can almost be sure that something malicious has happened.
- Response: Production honeypots can be used to respond to an attack. Information gathered from the attacked system can be used to respond to the break-in.
- A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. (This includes the hacker, cracker, and To set up a honey pot, it is recommended that you:
- Install the operating system without patches installed and using typical defaults and options.
- Make sure that there is no data on the system that cannot safely be destroyed
- Add the application that is designed to record the activities of the invader

Maintaining a honey pot is said to require a considerable amount of attention and may offer as its highest value nothing more than a learning experience (that is, you may not catch any hackers).

A honeypot is a resource which is intended to get com-promised. Every traffic from and to a honeypot is suspicious because no productive systems are located on this resource. In general, every traffic from and to a honeypot is unauthorized activity. All data collected by a honeypot is therefore interesting data. A honeypot will in general not produce an awful lot of logs because no productive systems are running on that machine which makes analyzing this data much easier. Data collected by a honeypot is of high value and can lead to a bet-ter understanding and knowledge which in turn can help to increase overall network security. One can also argue that a honeypot can be used for prevention because it can deter attackers from attacking other systems by occupy-ing them long enough and bind their resources. Against most attacks nowadays (which are based on automated scripts) a honeypot does not help deceiving individuals as there are no persons to deceive.

If a honeypot does not get attacked, it is worthless. Honeypots are normally located at a single point and the probability can be quite small that an attacker will find the honeypot. A honeypot does also introduce a certain risk - blackhats could get attracted to the whole network or a honeypot may get silently compromised.

2.2 Types of Honeypots

Honeypots come in many shapes and sizes, making them difficult to get a grasp of. To help us better understand honeypots and all the different types, we break them down into two general categories, low-interaction and high-interaction honeypots. Interaction defines the level of activity a honeypot allows an attacker.

- Low-interaction honeypots have limited interaction; they normally work by emulating services and operating systems. Attacker activity is limited to the level of emulation by the honey pot.
- High-interaction honeypots are different, they are usually complex solutions as they involve real operating systems and applications. By giving attackers real systems to interact with, you can learn the full extent of their behavior, everything from new root kits to international IRC sessions. The second advantage is high-interaction honeypots make no assumptions on how an attacker will behave.

2.2.1 Honeynet: High-interaction honeypot

Honeynets are a prime example of a high - interaction honeypot. Honeynets are not a product, they are not a software solution that you install on a computer. Instead, Honeyents are an architecture, an entire network of computers designed to attack. The idea is to have an architecture that creates a highly controlled network, one where all activity is controlled and captured. Within this network we place our intended victims, real computers running real applications. The bad guys find, attack, and break into these systems on their own initiative. When they do, they do not realize they are within a Honeynet. All of their activity, from encrypted SSH sessions to emails and files uploads, are captured without them knowing it. This is done by inserting kernel modules on the victim systems that capture all of the attacker's actions. At the same time, the Honeynet controls the attacker's activity. Honeynets do this using a Honeywall gateway. This gateway allows inbound traffic to the victim systems, but controls the outbound traffic using intrusion prevention technologies. This gives the attacker the flexibility to interact with the victim systems, but prevents the attacker from harming other non-Honeynet computers. An example of such a deployment can be seen in Figure 1

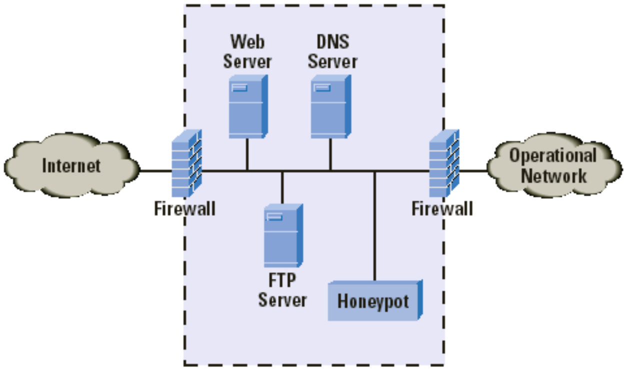


Figure 1

2.2.2 Honeyd: Low Interaction Honeypot

Honeyd is a low-interaction honeypot. Developed by Niels Provos, Honeyd is OpenSource and designed to run primarily on Unix systems (though it has been ported to Windows). Honeyd works on the concept of monitoring unused IP space. Anytime it sees a connection attempt to an unused IP, it intercepts the connection and then interacts with the attacker, pretending to be the victim. By default, Honeyd detects and logs any connection to any UDP or TCP port. In addition, you can configure emulated services to monitor specific ports, such as an emulated FTP server monitoring TCP port 21. When an attacker connects to the emulated service, not only does the honeypot detect and log the activity, but it captures all of the attacker's interaction with the emulated service. In the case of the emulated FTP server, we can potentially capture the attacker's login and password, the commands they issue, and perhaps even learn what they are looking for or their identity.

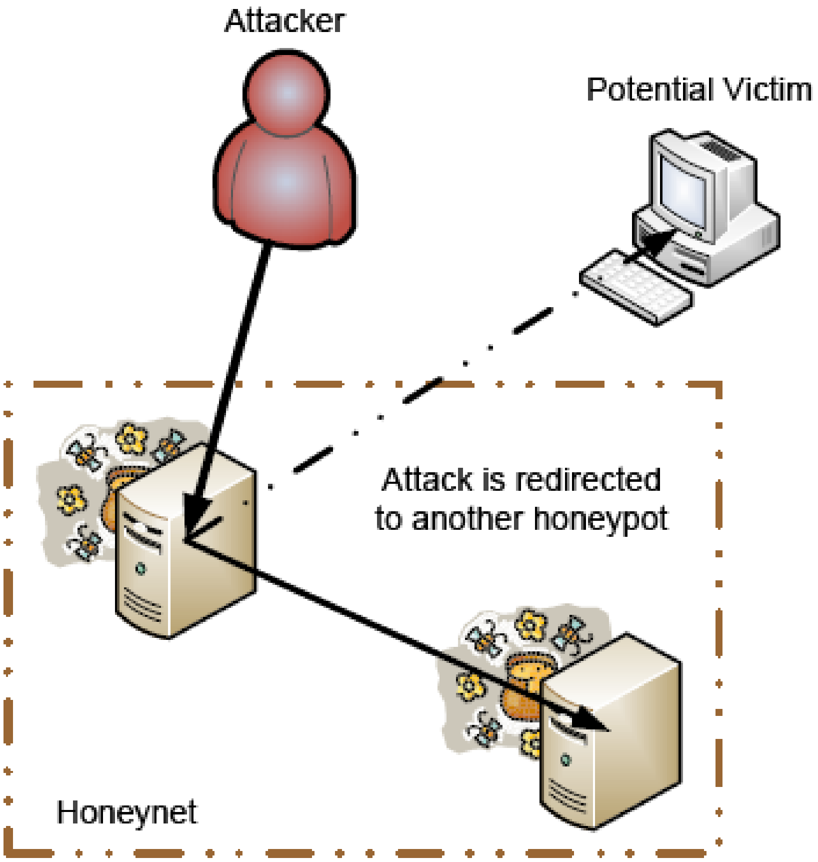
3. Recent Trends and Advances

In this section, we discuss the trend towards grouping honeypots into honeynets or honey farms. Shadow Honeypots and distributed honeypots, both cutting edge technologies, are then introduced.

3.1 Honeynets and Honey Farms

Honeynets and honey farms are the names given to groups of honeypots. Honeyfarms tend to be more centralized. Grouping honeypots provide many synergies that help to mitigate many of the deficiencies of traditional honeypots. For instance, honeypots often restrict outbound traffic in order to avoid attacking non-honeypot nodes. However, this restriction allows honeypots to be identified by an attacker. These redirection nodes also behave like real victims. Figure 2 shows the redirection of outbound traffic from a honeypot to another node in the honey farm.

Figure 2. 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. Shadow honeypots first segment anomalous traffic from regular traffic. The anomalous traffic is sent to a shadow honeypot which is an instance of a legitimate service as shown in Figure 3. 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. While shadow honeypots require more overhead, they are advantageous in that they can detect attacks contingent upon the state of the service.

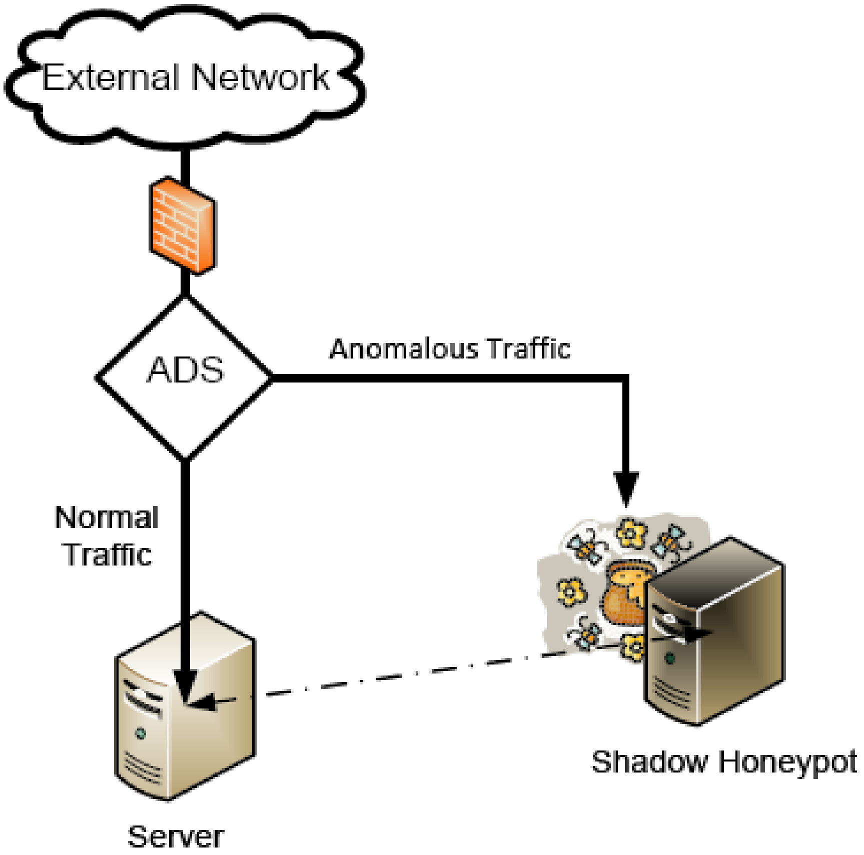


Figure 3. Segmenting traffic in a shadow honeypot system

3.3 Distributed Honeypots

One disadvantage of honeypots is that must take up a large portion of the address space in order to be efficient and useful (since attackers and malware must target the honeypots). It provide a distributed framework for grid computing in which legitimate hosts redirect suspicious users to a single honeypot. An alternative is used by Honey@home in which each client is responsible for a single unused IP address. The client traffic is redirected anonymously through the Tor network to a collection of central honeypots. Honeyfarms, honeynets, and distributed honeypots all address the need to monitor a large set of network addresses in order for a honeypot to be effective. As discussed in Section 2.1, grouping honeypots can also add functionality to honeypots by allowing for operations such as simulated outbound traffic. Honeynets, shadow honeypots, and distributed honeynets are just a few of the advances occurring in the field of honeypots. We encourage you to explore journals and online to read about the latest advances.

Advantages

Honeypots have several distinct advantages when compared to the current most commonly used security mechanisms:

- Small Data Sets - Honeypots only pay attention to the traffic that comes to them. They are not concerned with an overload of network traffic or determining whether packets are legitimate or not. Therefore they only collect small amounts of information – there are no huge data logs or thousands of alerts a day. The data set may be small, but the information is of high value.
- Minimal Resources – Since they only capture bad activity, they require minimal resources. A retired or low end system may be used as a honeypot.
- Simplicity – They are very simple and flexible. There are no complicated algorithms to develop, state tables or signatures to update and maintain..
- Discovery of new tools and tactics – Honeypots capture anything that is thrown at them, which can include tools and tactics not used previously.
- Reviewing these advantages show how honeypots add value and can enhance the overall security of your organization.

Conclusions

In this paper we have provided a brief overview of what honeypots are, and what they are useful for. We have discussed the different types of honeypots such as production honeypots, research honeypots, and honey tokens. We also looked at factors that should be considered when implementing a honeypot. For example, the level of interaction of your honeypot depends on what you want to use it for. The legal issues surrounding honeypots and their implementation were examined, and throughout we mentioned the advantages of honeypots. An important point to remember is that experts advise using honeypots together with some other form of security such as IDS. Honeypots are a relatively new technology that is becoming increasingly popular, and will become even more so as commercial solutions become available that are easy to use and administer. Because they can be used to collect information on attackers and other threats, we believe they can prove a useful tool in digital forensics investigations.

References

1. www.projecthoneypot.org
2. honepet Project.
3. http://www.honeynet.orgrgimisc/project.htm
4. Reto Baumann, Christian Plattner. White Paper:
5. Honeypots. Feh, 2002.
6. http://security.rbaumann.net/download/whitepaper.pdf
7. Lance Spitzner. Honeypot: Definitions and Values.
8. May, 2002. http://www.spitzner.net
9. Honeynet Project. Know Your Enemy: Honeynets.
10. http://www.honeynet.org/papers/honeynets
11. Honeynet Project. Know Your Enemy: http://www.honeynet.org/papers/forensics/
12. Honepet. Tools for Honeynets.
13. http://w.honeynet.org/papers/honeynet/