IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Honeypot: A Trap for Attackers

Savita Paliwal

Dept. of Computer Science and Engineering, Walchand Institute of Technology, Solapur

Abstract: This paper introduces Honeypot, a new technology for Network Security. The paper deals with the basic aspects of Honeypots, their use in modern computer networks and their implementation in educational environments. It explains the different types i.e Production honeypot, Research honeypot, low level interaction honeypot, medium level interaction honeypot, high level interaction honeypot and functions of honeypots. The advantages & disadvantages related to honeypot are discussed further. Probable future work in the area of honeypot is discussed which includes enhancement in framework of honeypot.

Keywords: Honeypot, Honeynet, Honeyd, IDS (Intrusion detection system), Network security.

I. INTRODUCTION

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. For example: users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Some other methods for securing the network are: Cryptography, Encryption-Decryption, Bio-metrics, Firewalls, Intrusion Detection System(IDS), Honeypots.

Encryption: It is a process of translating a message, called the Plaintext, into an encoded message, called the Ciphertext.
Decryption: It is the process of extracting the original information from the encrypted data.
Cryptography: Prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense.
Intrusion Detection System (IDS): It inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
Firewall: It is a system which limits network access between two or more networks.
Biometrics: This technology measure a particular set of a person's vital statistics in order to determine identity.
HoneyPot: A honey pot is a computer security mechanism on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems.

II. RELATED WORK

Following are the tools used till now for detecting hackers [1]:

- In 1997, Fred Cohen's Deception Toolkit Version 0.1 was released, one of the first honeypot solution available to the security community.
- In 1999, Formation of the Honeynet Project and publication of the "Know Your Enemy" series of papers were published.
- In 2000/2001, use of honeypot to capture and study worm activity was developed. More organizations were adopting honeypot for both detecting attacks and for researching new threats.
- In 2002, A honeypot is used to detect and capture in the wild a new and unknown attack. Honeypot security system not only prevents the person illegally accessing accounts but detect him. It also shows the list of attacks and counts the no. of appearances [2].Some research states that it can be used in military field to detect unknown codes [3] .

III. WHAT IS HONEYPOT?

A Honey pot is a computer system that is expressly set up to attract and "trap" people who attempt to penetrate other computer systems (This includes the hacker, cracker).It contains some interesting data or sometimes it behaves like a real operating system to the attacker to be probed or attacked. It is used as decoy. The intruder is intended to detect the Honeypot and try to break into it. The purpose of a Honeypot is to detect and learn from attacks and use that information to improve security. A network

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

administrator obtains information about the current threats on his network. Honeypot can be used to examine vulnerabilities of the operating system or network. Moreover it can be used to observe activities of an individual which gained access to the Honeypot. Honeypots are a unique tool to learn about the tactics of hackers.

IV. TYPES OF HONEYPOT

Honeypots can be categorised [4][5][12]using two factors:

- The purpose of the honeypot and
- The level of interaction with attacker

Following table summarize the types of honeypot on the basis of these two categorization factors. On the basis of purpose of honeypots we can categorize honeypot into two categories– production honeypot and research honeypot. On the basis of level of interaction we can categorize honeypots into three categories– low level interaction honeypot, medium level interaction honeypot and high level interaction honeypot.

Categorization factor	Categories of Honeypot	Brief description
Purpose of Honeypot	**Production Honeypot**	A Production honeypot is one used within an organization and help to mitigate risk.
	Research Honeypot	A Research honeypot is used to gain the information about the hacker's or attacker's community and does not add any direct value to the organization.
Level of Interaction With Attacker	**Low- Interaction Honeypot**	The low-interaction honeypots are the easiest to implement. Basic services such as Telnet and FTP are emulated on low interaction honeypots.
	Medium- Interaction Honeypot	In terms of interaction, this is a little more advanced than low-interaction honeypots, but a little less advanced than high-interaction honeypots.
	High- Interaction Honeypot	High-Interaction honeypots are time-consuming to design, manage and maintain. These are generally used to gather the attacker's information for analysis. Information and evidence gathered for analysis are bountiful. The goal of a high interaction honeypot is to give the attacker access to a real operating system where nothing is emulated or restricted.

A. Classification According to Purpose

1. Production Honeypot

Production Honeypots[5] are primarily used for detection. Typically they work as extension to Intrusion Detection Systems performing an advanced detection function.

A Honeypot allows justifying the investment of a firewall. Without any evidence that there were attacks, someone from the management could assume that there are no attacks on the network. Therefore that person could suggest stopping investing in security as there are no threats. With a Honeypot there is recorded evidence of attacks. The system can provide information for statistics of monthly happened attacks. Attacks performed by employees are even more critical, typically an employee is assigned a network account with several user privileges. In many cases networks are closed to the outside but opened to the local network. Therefore a person with legal access to the internal network can pose an unidentifiable threat. Activities on honeypots can be used to prove if that person has malicious intentions. For instance a network folder with faked sensitive documents could be prepared. An employee with no bad intentions would not copy the files but in the case the files are retrieved this might reveal him as a hacker.

Another benefit and the most important one is, that a Honeypot detects attacks which are not caught by other security systems. An IDS needs a database with frequently updated signatures of known attacks. Example of production honeypot is Nepenthes"[3].Georg Wicherski originally wrote a tool called "mwcollect" while Paul Baecher and Markus Koetter were working on "Nepenthes". Mwcollect was merged into Nepenthes in February 2006. It is used to detect the attacks.

2. Research Honeypot

A research Honeypot [5] is used in a different scenario. A research Honeypot is used to learn about the tactics and techniques of attacker. It is used as a watch post to see how an attacker is working when compromising a system. In this case the intruder is allowed to stay and reveal his secrets. The Honeypot operator gains knowledge about hacking tools and tactics. When a system was compromised the administrators usually find the tools used by the attacker but there is no information about how they were used. A Honeypot gives a real-live insight on how the attack happened. Research honeypots are complex to both deploy and maintain but are used to capture extensive amounts of data. They can be very time

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

consuming. They are better to learn about the attackers but have very little contribution in the direct security of an organization. They are typically used by organizations such as universities, governments, the military or large corporations interested in learning more about threats research. Examples of such research honeypots are "Honeynets". Honeynet is nothing but a network having two or more Honeypots.

B. Classification According to Level of interaction

1) Low-interaction honeypots

Low-interaction honeypots [4][12]can be easily installed on the system and configured to any of the services such as TELNET, FTP, MESSAGING, etc. This low-interaction honeypot is both easy to deploy and maintain. But to prevent the system from being fully exploited by hackers, the administrator needs to ensure "patch management"[5]on the host system and to carefully monitor the alert mechanisms which alerts the administrator about the attack. Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Low-interaction honeypots have the lowest level of risk. The low-interaction honeypot is only good at capturing known attack patterns, but is worthless at interacting or discovering unknown attack signatures. The main objective of low-interaction honeypot is only to detect, such as unauthorized probes or login attempts. Examples of Low-interaction honeypot are "Honeyd".

Honeyd :

Honeyd [6][11] is an application which enables the setup of multiple virtual honeypots on a single machine, each with different characteristics and services.

Honeyd is a freely available framework for setting up virtual honeypots. With honeyd it is possible to setup honeypots with different personalities and services on one machine. Honeyd emulates the different operating system's IP stack and binds certain script to a desired port to emulate a specific service. Honeyd is able to fool network fingerprinting tools (which store the fingerprints of operating systems present in the network) to think they are dealing with a real operating system ranging from a Windows NT to an AIX box(Advanced Interactive eXecutive box) It is a proprietary operating system developed by IBM based on UNIX System V[6]. Even different router's IP stacks can be emulated. Honeyd relies on the Nmap fingerprinting file. When Nmap stores a fingerprint in memory, Nmap uses a tree of attributes and values in data structures that users need not even be aware of. But there is also a special ASCII-encoded version which Nmap can print for users when a machine is unidentified)[7] which is used to characterize different kind of operating systems and their IP stacks. Before honeyd is inserting a packet into the IP stream, the personality of the packet is adjusted according to the desired operating system and the corresponding TCP/IP flags. With honeyd it is even possible to emulate complex network architectures and their characteristics. Virtual routing topologies can be defined including different brands of routers, the latency of a network connection as well as the packet loss. When using tools to map the network (like trace route), the network traffic appears to follow the configured routers and network connections. The setup of virtual machines is very easy. A configuration file is used to tell honeyd what kind of operating system is desired, how it does respond to closed ports and what kind of service is listening on which port. Honeyd is capable of binding a script to a network port. The script can be a standard shell script which simulates a certain service. Most scripts are built as state machines where a command triggers a certain response or advances to a new state with new possibilities. Scripts for the most popular well known services like SMTP, HTTP and telnet are available at several locations on the Internet.

2) Medium-Interaction Honeypots

In terms of interaction, this is a little more advanced than low level interaction honeypots, but a little less advanced than high level interaction honeypots. Medium level Interaction honeypots still do not have a real operating system, but the bogus services provided are more sophisticated technically. Similar to low level interaction Honeypots, medium level interaction Honeypots are installed as an application on the host operating system and only the emulated services are presented to the public. But the emulated services on medium level interaction Honeypots are more powerful, thus the chance of failure is higher which makes the use of medium level interaction Honeypots more risky.

Example of Medium interaction honeypot is "Nepenthes" [7][8].

Nepenthes:

Nepenthes is medium level interaction Honeypot, which emulates known vulnerabilities and captures worms as they attempt to infect it.

Nepenthes not only detect the attacker, but also give the information about new techniques used by attacker. It provides bogus services to the attacker which is more sophisticated technically. As compare to low level honeypot it is more risky.

3) **High- Interaction honeypots**

These kinds of honeypots are time-consuming to design, manage and maintain. The goal of a high level interaction honeypot is to give the attacker access to a real operating system where nothing is emulated or restricted. As they offer a full operating system the risk involved is very high. An intruder could easily use the compromised platform to attack other devices in the network or cause bandwidth losses by creating enormous traffic. An example of High-interaction honeypot is "Honeynets".

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Honeynet:
Two or more honeypots on a network form a honeynet [10]. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion detection systems. The concept of the honeynet first began in 1999 when Lance Spitzner, founder of the Honeynet Project, published the paper "To Build a Honeypot. A Honeynet is a high-interaction honeypot, meaning it provides real operating systems for attackers to interact with. This high interaction can teach us a great deal about intruders, everything from how they break into systems to how they communicate and why they attack systems. Honeynets accomplish this by building a network of systems. This network is highly contained, where all inbound and outbound traffic is both controlled and captured. Each system within the network is really a honeypot, a system designed to be attacked. However, these honeypots are fully functional systems, the same found in most organizations today. When these systems are attacked, Honeynets capture all of the attacker's activity. This information then teaches a great deal about the threats we face today.

V. ADVANTAGES OF HONEYPOT

Honeypots have several distinct advantages [9][12]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 orlow 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.

VI. DISADVANTAGES OF HONEYPOT

Honeypots have several risks and disadvantages. Although few in number, it is these disadvantages [9][12] that prevent honeypots from completely replacing your current security mechanisms.

• Limited Vision – The only activity tracked and captured by a honeypot is when the attacker directly interacts with them. Attacks against other parts of the system will not be captured unless the honeypot is threatened also.
• Discovery and Fingerprinting – Fingerprinting is when an attacker can identify the true identity of a honeypot because it has certain expected characteristics or behaviours. A simple mistake such as a misspelled word in service emulation can act as a signature for a honeypot.
• High level of Risk- In case of High level interaction honeypots there is huge risk as it provides real operating system to be probed or attacked.

VII. FUTURE WORK

In this paper I have provided a brief overview of what honeypots are, and what they are used for. I have discussed the different types of honeypots such as production honeypots, research honeypots, low level interaction honeypot, medium level interaction honeypot, high level interaction honeypot. For example, the level of interaction of your honeypot depends on what you want to use it for. 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, I believe they can prove a useful tool in digital forensics investigations. Honeypot frameworks available till now are not up-to-date and have not been developed completely. So the framework can be developed up to the middle level interaction honeypot.

VIII. CONCLUSION

The paper provides a brief overview of honeypot and their usage. Different types of honeypot such as production honeypot, research honeypot, low level Interaction honeypot, medium level Interaction honeypot and high level Interaction honeypots are discussed with examples.
The honeypots is relatively a new technology and has good scope for future work. Honeypot can be used with other well established security tools such as IDS or Firewalls to make them more effective.

REFERENCES

[1] . Lanz Spitzner, “Know Your Enemy: Honeywall CDROMRoo 3rd Generation Technology”, 2005.
[2]. Christian Doring, “Improving network security with honeypot.”
[3]. The Government of the Hong Kong Special Administrative Region, “Honeypot security” February 2008.
[4]. Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses
[5]. http://project.honeynet.org/papers/individual/Doering.pdf
[6]. http://security.rbaumann.net/download/honeyd.pdf
[7]. Setting Up And Running A Honeypot – Nepenthes,Brian Allen (ballen at wustl.edu) Network Security Analyst ,Washington University in St. Louis
[8]. http://www.pixel-house.net/midinthp.pdf
[9]. http://www.honeypots.net/.
[10]. http://www.honeynet.org/papers/kye.html.
[11]. http://www.honeyd.org/background.php.
[12]. http://cs.millersville.edu/~csweb/lib/userfiles/honeypot.pdf