Honey Pots: A Defence System for Security of Network

Anjali
Assistant Professor, Computer Science & Engineering, BFCET, Bathinda, Punjab,India
anjali.2317@gmail.com

Abstract
In the days there are large number of systems to provide security to the network but still the network is not secure because of various security threats that is worms, virus and crackers that harms the network. There are various security mechanisms i.e. Intrusion Detection System, Firewalls etc to secure the network. With the increasing use of internet securing a network is a very challenging process. As compare to other mechanisms Honey pot is one of the security systems to record all the activities of attackers.Honey pots are computers which masquerade as unprotected. In these programs, services and operating system is provided so that attacker can interact with it. Honey pot is a cost effective solution to increase the security of network.In this paper the concept of honey pot is discussed along with its history, working, typesand advantages to further analyze the honey pots and its taxonomy.
Keywords: Security of Network, Honey pot.

1. Introduction

1.1 Honey Pots:

Ahoney pot is an “an information system resource whose value lies in unauthorized or illicit use of resources” [11]. It is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. It consists of a computer, data or a network site that appears to be a part of a network, but is actually isolated and monitored and which seems to contain information or a resource of value to attackers. Most honey pots are installed with firewalls. Honey pots and firewalls work in reverse direction to each other as the honey pots allow all traffic to come in but blocks all outgoing traffic. Most honey pots are installed inside network firewalls and is a means for monitoring and tracking hackers. Honey pots are a unique tool to learn about the tactics of hackers [11].

In the below figure 1the Honey pot coloured orange is shown. In any other production systems or in naming servers the honey pot is not registered. This is necessary because within a configured network only it can be assumed that every packet that is forwarded to the Honey pot, is susceptible for attack. If packets that are not properly configuredarrive, the amount of false alerts will increase and the value of the Honey pot decreases.

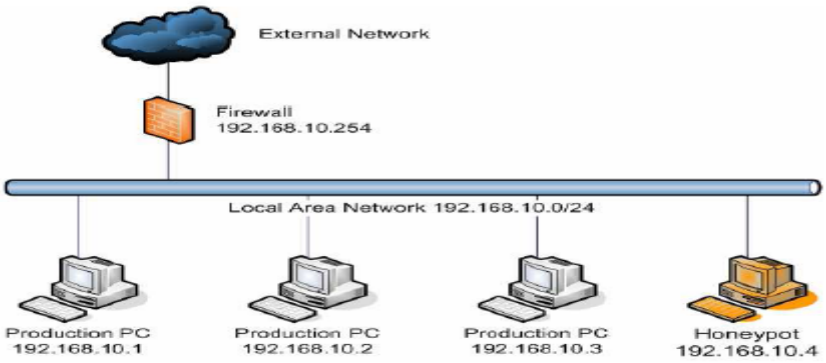

Figure1: Deployment scenario of a single Honey pot

1.2 History of Honey Pots:

In 1991 the idea of honeypots began with two publications, “The CuckoosEgg” by Clifford Stoll and “An Evening with Breford” by Bill Chewick.“The Cuckoos Egg”.Was about the experience of author to find acomputer hacker that was in hiscorporation finding the secrets and “An Evening with Berferd” was about acomputer hacker’s who moves through traps that he and his colleagues used to catch him. These both publications were the beginnings of what became honeypots. The first type of honey pot called the Deceptive Toolkit came in 1997. The point of this kit was to use deception to attack back. In 1998 the second type of honey pot called “Cybercop Sting” came out. This was the first commercial honey pot. In 2002 the honey pot could be shared and used all over the world. After that the honey pot technology has improved a lot. In the year, 2005, The Philippine Honey pot Project was started to promote computer safety over in the Philippines [11].

2. Categories of Honey Pots:

There are two categories of honeypots:

- High-interaction Honey Pots
- Low-interaction Honey Pots

- **High Interaction Honey Pots**

High-interaction honeypotshave the actual operating system and tools which attract the attacker to interact with it so as to monitor the actions of attacker. The aim of this honey pot is to capture the maximum amount of information on the attacker’s strategies. To decrease the load of high interaction honey pot only traffic that is filtered by low interaction honey pots is passed to them so these honey pots only process the packets that are sent by attackers[12].

- **Low Interaction Honey Pots:**

In low-interaction honeypots there is no operating system but os emulators were installed to which attacker can interact with.In this there is a limited subset of the functionality they would expect from a server, with the intent of detecting sources of unauthorized activity. It will beused to scan the port and generates attack signatures [12].

2.1 Working of Honey Pots:

Honey pots are generally based on a real operating system, real server and withdata that appears to be real. Honey pots work by monitoring and/orcontrolling the attacker during their use of the honey pot. Data capture, the ability to log, alert is the most critical elements of Honey Pot. Various honeypot solutions, such as Honeyd or Specter, have theirown logging and alerting capabilities. It is

recommend deploying Snort when honey pot is deployed. Snort is an Open Source intrusion detection system that in addition to alert and detect attacks against honey pot also captures the packets and packet payloads involved in the attack. This information can prove critical in monitoring the attacker'sactivities [11].

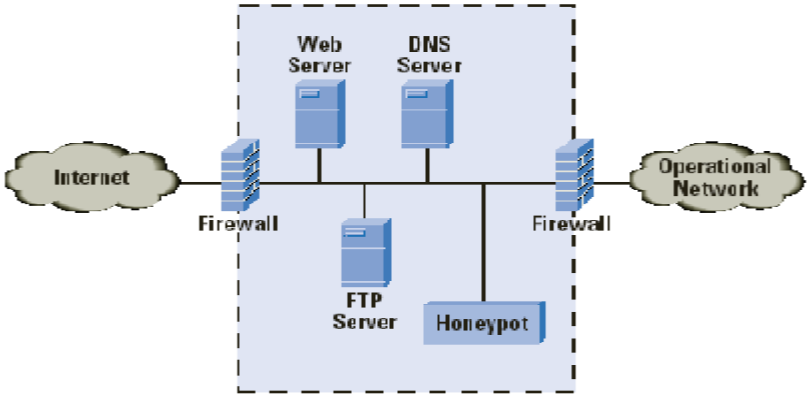

Figure 2: Working of a Honey pot

2.2 Advantages of Honey Pots:

There are various advantages of Honey Pots over other security mechanisms, including network intrusion detection systems:

2.2.1 Fewer false positives since no legitimate traffic uses honey pot
2.2.2 Collect smaller, higher-value, datasets since they only log illegitimate activity
2.2.3 Work in encrypted environments
2.2.4 Do not require known attack signatures, unlike IDS
2.2.5 Honey pots collect very little data, and it is of high value. This cuts the noise level down which make it much easier to collect and archive data.
2.2.6 Honey Pot is simple to design, use and implement. Due to this honey pot is a desirable method to increase security conditions in any organization.

3. How does Honey pot Gather Information?

Honey pot capture data in an area that is not accessible to an attacker. Datacapture happens on a number of levels [11]:

3.1 Firewall Logs:Simple, yet effective

3.2 A Packet Sniffer (or similar IDS sensor):The IDS should be configured to passively monitor network traffic (for an added levelof invisibility, one might set the system up to have no IP address or, in some instances, the sniffer could be configured to completely lack an IP stack). This willcapture all clear text communication, and can read keystrokes.

3.3 Local and Remote Logs:These should be set up just as you would on any other system, and will possibly be disabled, deleted, or modified by an experienced hacker, but plenty of useful information will still be available from all the previouscapture methods.Remotely Forwarded Logs: will capture dataon a remote log and then instantly forward the data to a system even further out of the range of the attacker.

4. SECURITY CATEGORIES:

Security is break into three categories:

4.1Prevention:A honey pot cannot prevent an unpredictable attack but can detect it. One case where they prevent the attacker is when he directly attacks the server. It will prevent attack on a production system by making the hacker waste his time on a non sufficient target.

4.2Detection: Detecting intrusions in networks is similar to the function of an alarm system for protecting facilities when an unauthorized activity appears. A system might alert on suspicious or malicious activity, even if the data is valid. Due to the high network traffic on most networks, the chances of false alarms and non-detected attacks are more leaving it unscanned and benefiting the attacker.

4.3Response: Honey pots provide exact evidence of malicious activities and give the information of the attack to prevent any such in the future and to start the countermeasures.

5. Various Popular Honey Pots:

The popular honey pots are:

5.1 Back Officer Friendly (BOF):

- It is a Low Involved Honey pot
- It Emulates Services like FTP, Telnet, HTTP.
- Records scans, probes etc.
- It also works on Windows platform
- With BOF, this low-interaction honeypot is both easy to deploy and maintain

5.2 Specter:

- Is also an example of Low Involved Honey pot.
- It is Similar to BOF it also Emulates Services like FTP, Telnet, HTTP etc.
- It works on different Operating Systems as well.

5.3 Honeyd:

- It is a Low Involved Honeypot.
- It emulates Services like FTP, Telnet and HTTP etc.
- It emulates different Operating Systems as well.

5.4 Mantrap:

- It is Highly Involved Honeypot
- It emulates Services like FTP, Telnet and HTTP etc.
- It emulates different Operating Systems as well.
- It gives more in-depth knowledge on malicious attackers.

6. Examples of Honey Pot Systems:

6.1Deception Toolkit6:DTK was the first Open Source honeypot released in 1997. It is a collection of Perl scripts and C source code that emulates a variety of listening services. Its primary purpose is to deceive human attackers[12].

6.2LaBrea7: This is designed to slow down or stop attacks by acting as a sticky honeypot to detect and trap worms and other malicious codes. It can run on Windows or Unix.

6.3Honeywall 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 ofdeploying a honeynet gateway known as a Honeywall. It can capture, control and analyse all inbound and outbound honeynet activity.

6.4 Honeyd9: This 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.

7. Conclusion:

In this work, the concept of honeypots in is explored depth and its usefulness in the field ofnetwork security. Honey pot is agood tool supplements other security technologies toform an alternative active defence system for networksecurity. It is proved to be a useful tool for interaction with luring and trapping attackers, capturing information and generating alerts. The attacking techniques and methods can be analysed from the information provided by the activities of the attackers. No extra burden to existing network bandwidth is added as honeypots only capture and archive data and requests coming in to them. New way to attacks prevention, detection andreaction are provided by Honey pot.The commontechnologies of data control and data capture are shared by different kinds of honey pot.Most importantly, they serve as a learning tool forsystem administrators and also involved studying issues concerning intrusion detection systems the challengesthat these systems faced.The scope for development of honey pot tools increases asawareness and interest in honeypots increases, which facilitate the different aspects of honeypots like logging, tracing back to the source etc.

8. References:

[1] CERT Coordination Center, ‘‘Results of the distributed systems intruder tools workshop,” Nov. 1999

[2] FengZhang, Shijie Zhou. Zhiguang Qin and JindeLiu,"Honeypot: a Supplemented Active Defense System for Network Security",IEEE,ISBN 0-7803-7840-7,Aug. 2003

[3] LjiljanaTrajovic. Distributed Denial of Service Attacks,IEEE International Conference on Systems, Man and Cybernetics, pp. 2275-2280,Oct. 2000.

[4]PUSHPA, S. YASHPAL and S. NIRANJAN, "IMPLEMENTATION OF HONEYPOT AS AN INTRUSION DETECTION SYSTEM FOR WIRELESS NETWORK", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR),Vol. 3, Issue 3, pp. 57-64,Aug. 2013

[5] Yogendra Kumar Jain," Honeypot based Secure Network System", International Journal on Computer Science and Engineering (IJCSE),ISSN No. 0975-3397 Vol. 3, No. 2 , pp. 612-620,Feb 2011

[6] http://www.cert.org/reports/dsit-workshop.pdf.

[7] http://www.honeynet.org

[8] www.topsite.com/best/honeypot

[9] www.en.wikipedia.org/Honeypot

[10] www.trackinghackers.com/honeypots

[11] www.123seminarsonly.com/.../66498955-abstract-on-honey-pots.pdf

[12] www.infosec.gov.hk/english/technical/files/honeypots.pdf