NETWORK SECURITY RESOURCE: HONEYPOT

Mriga Gupta*

Monika Sachdeva**

Krishan Kumar***

Abstract

In today's society people becomes more and more dependent on computer systems. The Internet shows an increasing trend regarding the usage of malicious activities such as intrusion attempts, denial-of-service attacks, phishing, spamming and worms which makes use of compromised web servers. To try to minimize this threat, it would be nice to have a security system which has the ability to detect new attacks and react on them. Use of honeypots provides effective solution to increase the security and reliability of the network. Honeypots, systems to lure and research attackers, are subject to intensive research for quite some time. They do not 'fix' anything. Instead, honeypots are a tool. How you use that tool is up to you and depends on what you are attempting to achieve. It is hoped that this paper helps in clear understanding of honeypots.

Key words – Honeypots, security, interaction

* M.Tech student, CSE Deptt., Shaheed Bhagat Singh College of Engg. & Tech., Ferozepur, Punjab, India.

** Assistant Professor, CSE Deptt., Shaheed Bhagat Singh College of Engg. & Tech,. Ferozepur, Punjab, India.

*** Associate Professor, CSE Deptt., Punjab Institute of Technology, Kapurthala, Punjab.

INTRODUCTION

There are mainly two reasons why information security continues to receive an increasing amount of attention. Firstly, new services providing critical services demand an increased level of security. Secondly, there is an ever growing increase in reported incidents and attempted attacks on computer systems [1]. As in the military, it is important to know, who your enemy is, what kind of strategy he uses, what tools he utilizes and what he is aiming for [2]. 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 [2]. A honeypot is a resource which pretends to be a real target. A honeypot is expected to be attacked or compromised. The main goals are the distraction of an attacker and the gain of information about an attacker, his methods and tools [3].

HONEYPOT

A honeypot is a trap for people who tamper with computers maliciously through the Internet, just as a pot of honey traps flies. Honeypots serve several purposes: to catch individual crackers, to determine whether they can get into a network, and to observe how they carry out their attacks.

A definition of a honeypot provided by Lance Spitzner, President of the Honeynet Project, is, “An information system resource whose value lies in unauthorized or illicit use of that resource” [4]. It is a resource that has no productive value. There is absolutely no reason for anyone to interact with a honeypot. Thus, any attempt to communicate with the system is most likely a probe, scan or attack. Conversely, if the honeypot initiates any outbound connections, the system has probably been compromised [5].

TYPES OF HONEYPOTS

Honeypots are categorized on the basis of their level of interaction and the way in which they are deployed. The level of interaction defines how much functionality or activity an attacker can have with a honeypot [6].

There are three types of honeypots: low-interaction honeypots, medium-interaction honeypots and high interaction honeypots.

a) Low-interaction Honeypots - These honeypots are typically the easiest honeypots to install, configure, deploy and maintain [7]. Since low interaction honeypots are simple, they have the lowest level of risk [8]. An obvious advantage of this type of honeypot is its lack of complexity and ease of deployment. An example of a low interaction honeypot is Honeyd.

b) Medium-interaction Honeypots - Medium-interaction honeypots offer attackers more ability to interact than do low-interaction honeypots but less functionality than high-interaction solutions. There are several problems with this approach. First, it is very complex; a great deal can go wrong or be misconfigured [7]. Second, it is very difficult to give the virtual environment the full functionality and interaction of a true operating system [4].

c) High-interaction Honeypots - These are the most elaborated Honeypots. In contrast, high interaction honeypots do not emulate services; instead they provide real applications for attackers to interact with. An example of a high interaction honeypot is Honeynets [6].

Honeypots are deployed primarily for either research or production purposes, as defined by Snort creator Martin Roesch.

a) Production Honeypots: In the production category, honeypots are applied to preventing attacks, detecting attacks, and responding to attacks. It determines how an attacker gained access to the network. The primary value of production honeypots is detection. For prevention purposes, production honeypots are of minimal value [9].

b) Research Honeypots: In the research mode, a honeypot collects information on new and emerging threats, attack trends, motivations, behavior, intentions, and identity of attackers which essentially, characterizes the attacker community. This information is then used to better understand and protect against these threats [9].

EXAMPLES OF HONEYPOT SYSTEMS

Examples of freeware honeypots include:

a) Deception Toolkit [10]: 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.

b) LaBrea [11]: 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.

c) Honeywall CDROM [12]: 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 analyze all inbound and outbound honeynet activity.

d) Honeyd [13]: 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.

e) Honeytrap [14]: 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.

f) HoneyC [15]: This is an example of a client honeypot that initiates connections to a server, aiming to find malicious servers on a network. It aims to identify malicious web servers by using emulated clients that are able to solicit the type of response from a server that is necessary for analysis of malicious content.

g) HoneyMole [16]: 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.

In the corporate environment, the following commercial products are available:

a) Symantec Decoy Server [17]: This is a "honeypot" intrusion detection system (IDS) that detects, contains and monitors unauthorized access and system misuse in real time.

b) Specter [18]: This is a smart honeypot-based intrusion detection system. It can emulate 14 different operating systems, monitor up to 14 different network services and traps, and has a variety of configuration and notification features.

CONCLUSION

Honeypots are positioned to become a key tool to defend the corporate enterprise from hacker attacks it's a way to spy on your enemy; it might even be a form of camouflage. Hackers could be fooled into thinking they've accessed a corporate network, when actually they're just banging around in a honeypot -- while the real network remains safe and sound.

Honeypots have gained a significant place in the overall intrusion protection strategy of the enterprise. Security experts do not recommend that these systems replace existing intrusion detection security technologies; they see honeypots as complementary technology to network- and host-based intrusion protection.

The advantages that honeypots bring to intrusion protection strategies are hard to ignore. In time, as security managers understand the benefits, honeypots will become an essential ingredient in an enterprise-level security operation.

We do believe that although honeypots have legal issues now, they do provide beneficial information regarding the security of a network .It is important that new legal policies be formulated to foster and support research in this area. This will help to solve the current challenges and make it possible to use honeypots for the benefit of the broader internet community.

References

[1] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2004). The ninth annual CSI/FBI computer crime and security survey. Computer Security Institute (CSI) / Federal Bureau of Investigation (FBI). Available from http://www.csi.org.

[2] The Honeynet Project. Problems and challenges of honeypotshttp://www.honeynet .org/papers/honeynet/.

[3] John P. John, Fang Yu, Yinglian Xie, Arvind Krishnamurthy, Martin Abadi, (2011). "Heat–seeking Honeypots: Design and Experience", WWW 2011 – Session: Web Security.

[4] E. Cole, R. Krutz, James W. Conley. (2005) Network Security Bible. Wiley Publishing.

[5] Spitzner, L (2002). "Honeypots: Definitions and value of honeypots," http://www.enteract.com/~lspitz.

[6] Singh, R. K, Ramanuajm, T; (2009) "Intrusion Detection System using Advanced Honeypots", International Journal of Computer Science and Information Security, Vol 2, No 1.

[7] Spitzner, L. (2002). Honeypots: Tracking Hackers. Addison-Wesley, Boston.

[8] Stoll, C. (1988) "Stalking the Wily Hacker," Communications of the ACM. pp 484- 497.

[9] Know Your Enemy: Honeynets (2005) http://www.honeynet.org/papers/honeynet/.

[10] http://www.all.net/dtk/index.html

[11] http://labrea.sourceforge.net/labrea-info.html

[12] http://www.honeynet.org/tools/cdrom/

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

[14] http://honeytrap.mwcollect.org/

[15] https://www.client-honeynet.org/honeyc.html

[16] http://www.honeynet.org.pt/index.php/HoneyMole

[17] http://www.symantec.com/business/support/documentation.jsp?language=english&view= ma nuals&pid=51899

[18] http://www.specter.com/default50.htm