The DecoyPort: Redirecting Hackers to Honeypots

Iksu Kim and Myungho Kim

School of Computing, Soongsil University,
1-1 Sangdo-dong, Dongjak-gu, Seoul 156-743, South Korea
skycolor@ss.ssu.ac.kr, kmh@ssu.ac.kr

Abstract. Most of computer security systems use the signatures of well-known attacks to detect hackers' attacks. For these systems, it is very important to get the accurate signatures of new attacks as soon as possible. For this reason, there have been several researches on honeypots. However, honeypots can not collect information about hackers attacking active computers except themselves. In this paper, we propose the DecoyPort system to redirect hackers toward honeypots. The DecoyPort system creates the DecoyPorts on active computers. All interactions with the DecoyPorts are considered as suspect because the ports are not those for real services. Accordingly, every request sent to the DecoyPorts is redirected to honeypots by the DecoyPort system. Consequently, our system enables honeypots to collect information about hackers attacking active computers except themselves.

1 Introduction

As the need for computer security increases, so does the need for computer security systems to be developed to provide adequate protection to all users. These may include Intrusion Detection Systems(IDS)[1,2], Intrusion Protection Systems(IPS), and others. Most IDS and IPS use the signatures of well-known attacks to detect hackers' attacks. Accordingly, it is important and necessary to collect data regarding the attack strategies and tools of hackers. For this reason, there have been several researches on honeypots[3,4,5,6].

Honeypots are security resources which are intended to get compromised. They aim at collecting data regarding the attack strategies and tools of hackers. The data can be analyzed with analysis tools so that security systems can be updated to respond to new types of attacks. The more honeypots deloyed, the greater the chance of tracking hackers activities. Unfortunately, the more honeypots are deployed, the more IP addresses and computer hardware are required.

In this paper, we propose the DecoyPort system to redirect hackers toward honeypots. The DecoyPort is a port which is not used for a service but is used to lure hackers. The DecoyPort system creates the DecoyPorts on active computers. All interactions with the DecoyPorts are considered as suspect because the ports are not those for real services. Accordingly, every request sent to the DecoyPorts is redirected to honeypots by the DecoyPort system. Consequently,

T. Enokido, L. Barolli, and M. Takizawa (Eds.): NBiS 2007, LNCS 4658, pp. 59–68, 2007.

our system can complement the problem that honeypots can not collect information about hackers attacking active computers except themselves. First of all, the DecoyPort system can increase the chance of capturing and tracking hackers activities without wasting additional IP addresses and computer hardware. Unlike existing port-forwarders, the DecoyPort system can control the network traffic load caused by hackers, and prevent them from recognizing existence of a honeypot.

The rest of this paper is structured as follows. Section 2 gives an overview of the honeypot and honeytrap for collecting data regarding the attack strategies and tools of hackers. Section 3 and 4 describe the design and implementation of the DecoyPort system respectively. The DecoyPort system is evaluated in Section 5. Lastly, we conclude this paper in Section 6.

2 Background

2.1 Hacker and Internet Worm

When a hacker attacks a server, he generally start with OS fingerprinting and port scanning to identify the type of OS and the set of services in it. After that, he exploits vulnerabilities in a service daemon to run a root shell. He also install a keystroke logger on the server to gain more users IDs and passwords.

Internet worms are designed to exploit vulnerabilities found on many computers. They can find vulnerable computers by sending some packets. For example, Linux Slapper worm uses an OpenSSL buffer overflow exploit to run a shell on a remote computer. When the Linux Slapper worm finds vulnerable servers, it attempts to connect on port 80. It also sends an invalid GET request to the server to identify the Apache system. After the worm finds an Apache system, it tries to connect on port 443 to send the exploit code to the SSL service that is listening on the remote computer. Internet worms harm the computers and consume the bandwidth of networks.

2.2 Honeypot

The time delay involved in resolving new types of attacks makes it important and necessary to collect and analyze data regarding the attack strategies and tools in the most efficient and effective manner possible.

A honeypot is a security resource whose value lies in being proved, attacked, or compromised[7]. It aims to collect information regarding the attack strategies and tools of hackers. All activities within a honeypot are suspicious because it is not a production system. The information collected by honeypots are highly valuable and provide white hats a much fuller understanding of the intent, knowledge level, and modes of operation of hackers. Moreover, honeypots do not produce vast amounts of logs. On the other hand, traditional security systems, including firewalls, IDSs and others, collect vast amounts of data every day. These data make it difficult to find out new types of attacks. A honeypot is normally located at a single point and the probability can be quite small that attackers will