Chapter 29
Honeypots and Honeynets: Analysis and Case Study

José Manuel Fernández Marín
University of Almería, Spain

Juan Álvaro Muñoz Naranjo
University of Almería, Spain

Leocadio González Casado
University of Almería, Spain

ABSTRACT

This chapter presents a review and a case of study of honeypots and honeynets. First, some of the most important and widely used honeypots in the current market are selected for comparative analysis, evaluating their interaction capacity with an attacker. Second, a self-contained honeynet architecture is implemented with virtual machines. An intrusion test is performed against the honeynet to observe the quality and quantity of the information collected during the attack. The final goal of this analysis is to assess the capacity of monitoring and threat detection of the honeynets and honeypots.

INTRODUCTION

Honeypots are network resources, machines or servers that offer easily exploitable services in order to attract possible attackers (Spitzner, 2002; Mokube & Adams, 2007; Mairh, Barik, Verma & Jena, 2011). A honeynet is a network architecture composed of honeypots network, network devices and security tools. The use of honeypots and honeynets allows network and system managers to improve their technological infrastructure security thanks to information collection (The Honeynet Project [THP], 2002; Sadasivam, Samudrala & Yang, 2005). Furthermore, these systems are essential in research environments oriented to network security since they give the chance to capture, analyze and learn about new threats (Jones & Rommney, 2004; Mairh et al., 2011).

The first section of this chapter classifies honeypots according to their characteristics and interaction levels (Spitzner, 2002). Different locations where a honeypot can be placed within the network infrastructure of an organization will be analyzed, as well as the advantages and drawbacks of using honeypots when they are compared with other current technologies such as IDS, NIDS (Tiware & Jain, 2012), sandboxes and darknets (Mairh et al., 2011; ENISA, 2012). Some of the

DOI: 10.4018/978-1-4666-6324-4.ch029

most important and widely used honeypots in the current market will be selected for comparative analysis (Song et al., 2011). The analysis will be based on the interaction capacity, the realism of the emulated services, and the configuration and administration flexibility of each honeypot (ENISA, 2012).

In the second section, existing classifications and requirements of honeynets will be described (Spitzner, 2002; THP, 2002). Distributed honeynets, widely used in research work, will be introduced in addition to deployed architectures in local environments (Sadasivam et al., 2005; Tiware & Jain, 2012).

Next, a case study which implements a virtual honeynet using virtual machines is proposed (Asrigo, Litty & Lie, 2006). The scheme of this honeynet is based on The Honeynet Project and the Linux Honeywall Roo distribution (THP, 2002; Curran et al., 2005). An intrusion test, simulating a computer attack, will be carried out. Using available tools (THP, 2002), an analysis of the information will be performed before, during and after the attack. The intention of this analysis is to assess the capacity of monitoring and threats detection of the honeynets.

Finally, we will provide the main conclusions of the chapter, discussing the actual value of honeypots and honeynets within an organization (Levine, 2003; Song et al., 2011; ENISA, 2012; Tiware & Jain, 2012).

CYBERCRIME

Cybercrime has become a primary concern for users, governments and companies due due to the scarcity of security professionals in organizations, poor management practices of private and confidential information by employees and misinformation of society. The scope of professional cybercrime is broadening and keeps covering new fields and technologies to commit crimes. The first cybercriminals acting alone or in small groups, but today have evolved to a modular organizational model comprising a large number of skilled people that communicate over the network.

Today, there exist different roles within fraudulent organizations like victim recruiters (through phishing or other social engineering techniques), malware coders, money launders (through mules and movements between bank accounts), and more. With this infrastructure, profits increase and the chances of identification and arrest of the organizational components decrease.

Honeypots allow to detect new malware infection vectors, zero-day attacks, intrusion detections, etc. The honeypots are resources used in the detection of those activities related to cybercrime, increasing responsiveness to a malignant activity. They are also widely used for the study of new attack vectors conducted by criminal organizations in the network. The most famous case of the role of honeypots in crime prosecution to the date is known as *United States vs. Ivanov* (United States vs. Ivanov, 2005).

HONEYPOTS

A honeypot is an intentionally exposed computational resource with the aim of being tested, attacked, compromised, used or accessed in anyway unauthorized. The resource can be a system service, an application user or server, a complete system or just a piece of information as records in a database or office documents (ENISA, 2012).

In a production environment, any attempt to access or interact with the honeypot is a suspicious activity. All activities between a supposed attacker and the honeypot are monitored and analyzed in order to detect and confirm an unauthorized use. In this way, it is possible to take prevention measures or contingency.

There is a large variety of honeypots. Some general purpose honeypots are Honeyd, Specter or Dionaea, capable of simulating several services, even the type of operating system.