Definition of Attack in Context of High Level Interaction Honeypots

Pavol Sokol[1], Matej Zuzčák[2], and Tomáš Sochor[2]

[1] Institute of Computer Science, Faculty of Science
Pavol Jozef Šafárik University in Košice, Jesenná 5, 040 01 Kosice, Slovakia
pavol.sokol@upjs.sk
[2] Department of Informatics and Computers, Faculty of Science,
University of Ostrava, 30. dubna 22, 701 03 Ostrava, Czech Republic
{matej.zuzcak,tomas.sochor}@osu.cz

Abstract. The concept of attack in the context of honeypots plays an important role. Based on the definition of the attack, honeypots obtain information about attackers, their targets, methods, and tools. This paper focuses on the definition of attack in context of high-interaction server honeypots. Paper proposes the definition of attack from the perspective of information security and network forensics analysis.

Keywords: honeypot, computer attack, high-interaction honeypot, network security, server honeypot.

1 Introduction

Network security is an important part of security policies in each organization. Traditional tools (e.g. iptables, snort, surricata) and approaches applied in protection are currently becoming increasingly ineffective. It is due to the fact that the "bad" community (e.g. hackers) is always several steps ahead of defensive mechanisms (firewalls, IDS, IPS etc.). Therefore it is necessary to learn as much information as possible about the attackers. The specialized environment, in which vulnerabilities have been deliberately introduced in order to observe attacks and intrusions, has been introduced 20 years ago and it is called a **honeypot.** It can be defined as "a computing resource, whose value is in being attacked". The honeypot computer system is "a system that has been deployed on a network for the purpose of logging and studying attacks on the honeypot." [1].

Honeypots can be classified into several types. Two classifications are used in this paper. The former classification is **based on the level of interaction**. From this point of view, it is distinguished between low-interaction and high-interaction honeypots. The difference between these types lies in an extent, to which the attacker is allowed to interact with the system. **Low-interaction honeypots** implement targets to attract or detect attackers using software to emulate the characteristics of a

R. Silhavy et al. (eds.), *Software Engineering in Intelligent Systems*,
Advances in Intelligent Systems and Computing 349, DOI: 10.1007/978-3-319-18473-9_16

particular operating system and its network services on a host operating system. Examples of this type of honeypot are Dionaea [2] and HoneyD [3].

In order to get more accurate information about attackers, their methods and attacks, a complete operating system with all services must be used. This type of honeypot is called **high-interaction honeypot.** The goal of this type of honeypot is to provide an attacker access to the complete operating system, where nothing is emulated, nor restricted [1].

Another classification of honeypots is based on the **role** of honeypot**.** According to this classification, honeypots are divided in server-side honeypots and client-side honeypots. **Server side honeypots** are useful in detecting new exploits, collecting malware, and enriching research of the threat analysis. On the other hand, **client-side honeypots** collect information about client side attacks. They detect attacks directed against vulnerable client applications, when a client interacts with malicious servers. The aim of these honeypots is to search and detect these malicious servers. This paper focuses on server-side high-interaction honeypots.

2 Motivation

The primary motivation for elaborating this paper fact that the definition of an attack against high-interaction honeypots remained unchanged since 2004 [4]-[6]. Honeynet's community [1] considered each connection to be an attack against the honeypot. Such definition is based on the fact that legitimate connections should not be normally directed at honeypots since it does not provide any productive value or service. Therefore any traffic going to the sensor is considered as an attack.

According to the previous paper, where attacks against low-interaction honeypots were defined [7], the above-mentioned approach is inconsistent with techniques used by administrators of sensors to increase the attractiveness of honeypots for research purposes. In order to make a sensor sufficiently sensitive to attacks, it is necessary to raise the awareness of honeypots or pretend already mentioned productive value.

2.1 Presented Contributions

There are two **main contributions** of this paper. The first one is the analysis of the notion of the attack against high-interaction server honeypots from several perspectives in details. This analysis is based on the results of works [8] and [9]. The second contribution represents a comparison of definition of attack against low-interaction honeypots and high-interaction honeypots. The comparison is based on the authors' paper [7]. The paper focuses on the definition of attack against low-interaction server honeypots for two cases, namely emulation of Windows services and emulation of linux SSH services.