Chapter 5
The Role of Deception in Securing Our Cyberspace:
Honeypots Are a Viable Option

Banyatsang Mphago
https://orcid.org/0000-0002-9451-3119
Botswana International University of Science and Technology, Botswana

Dimane Mpoeleng
Botswana International University of Science and Technology, Botswana

Shedden Masupe
Botswana Institute for Technology Research and Innovation, Botswana

ABSTRACT

The use of deception systems is a viable option in reducing the never-ending tussle between the attackers and the defenders. The deception systems give the defenders an edge over their counterparts since they provide the platform to learn the methods and techniques the attackers use. However, the effectiveness of the deception system is highly dependent on how they truly hide their identity. A deceptive honeypot has the capacity to persuade and change the cognitive behavior of an attacker. An attacker whose cognitive behavior has been altered by the deception capabilities of a honeypot is more likely to reveal his attack methods; hence, the defenders are able to learn how to defend against those future attacks.

DOI: 10.4018/978-1-7998-9430-8.ch005

INTRODUCTION

Computer security has been a concern ever since the inception of computers, hence the never-ending struggle in the status quo requires a shift in mindset. Traditional approaches are firmly based on the premise that the network perimeter is an effective means to protect the information assets within the organization and that employees within the organization can be trusted. In the face of this challenges, some leading enterprises have changed the tactics and employed a ‘need-to-know’ approach as an effective way to secure their assets. The emergence of deception systems is becoming more and more a viable option to protecting computer assets. The use of honeypots in protecting computer and information assets comes from the notion that ‘you cannot protect what you don’t know’. Therefore, honeypots came as a viable option to understand attackers and their attack methods. Once deployed, a successful honeypot must be able to deceive, lure, and record all the attackers’ activities.

BACKGROUND

Honeypot Definitions

Honeypots are special systems designed to track and trap attackers and learn their attack methods. They are special in the sense that they are not a solution but rather a general technology that do not solve a specific security problem which is continuously changing, and can be involved in many facets of security such as information gathering, detection, and prevention (Verizon, 2019). Security researchers and administrators often use honeypots to unobtrusively track and monitor what *malicious* attackers are doing in order to compromise computer resources. A honeypot is a tool designed to learn the attack methods the adversaries use to query and exploit vulnerabilities in a system. So, a honeypot is a security resource whose value lies in being probed, attacked, or compromised (WhiteHatSecurity, 2016).

Several definitions for the term `honeypot’ have been proposed, and below we present some of those definitions:

- **Definition 1**: “a honeypot is a security resource whose value lies in being probed, attacked and compromised” (Spitzner, 2002).
- **Definition 2:** “a honeypot is a computer which has been configured to some extent to seem normal to an attacker, but actually logs and observes what the attacker does” (Gibbens, 1999).