Chapter 68
Assessment of Honeypots: Issues, Challenges and Future Directions

B. B. Gupta
National Institute of Technology Kurukshtra, India

Alisha Gupta
National Institute of Technology Kurukshtra, India

ABSTRACT

Honeypots act as an easy target for attackers but it is actually a "decoy" in which attacker is trapped. It is a defensive technique which lures the attacker into performing some illicit operations on it and subsequently using it to trace the activities of attacker, generating signatures and protecting the real system. In this article, a recent survey on Honeypots is presented, its deployment in smartphone scenarios, its usage to curb Distributed Denial of Service attacks in variegated frameworks including Cloud environments, copious datasets and open source. Also described are the types Honeypots available, their various security problems, and existing solutions. Furthermore, there is light shed on disparate issues and the challenges in the existing solutions and scope of further research.

1. INTRODUCTION

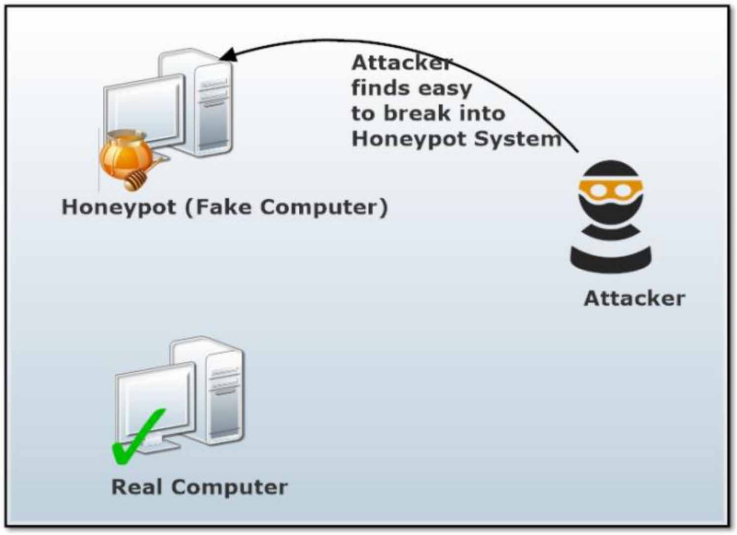
As with upswing in a number of cyber-attacks, it has become evident to detect attacks. Advanced techniques and mechanisms are used to identify new trends and patterns in the adversaries. According to the study of an Assocham-Mahindra SSG, in 2015 cyber lawlessness number in India may twofold to 3 lakhs (Assocham, 2015). With such a large increase in cyber-crimes, relying upon the traditional lines of defense intrusion detection system and firewall alone, would not be able to provide the comprehensive solution for the attacks (Gupta et al., 2016; Zhang & Gupta, 2016; Jouini & Rabai, 2016). Hence, honeypots are a novel approach to network security. We can define honeypot as: "Honeypot can be outlined as a data system resource with its uncertified or unlawful use of that resource that is its value".

DOI: 10.4018/978-1-7998-2466-4.ch068

It can be compared with the pots of honey used to trap unsuspecting wasps. The same concept is applied to the system also, honeypots put on a network to lure attackers. It is information learning and gathering instrument. Honeypots create a fake network by emulating the different services of a real computer with open ports and thus attacker finds easily to attack in this system as shown in Figure 1.

Honeypots are used in the cyber physical system that emulates the components of different physical system. It is created like a complex infrastructure so that intruder believes that it is a real network infrastructure. Use of honeypots in Industrial Control System (ICS) can be used to protect the infrastructure of such systems. One such example is Conpot (n.d.). It is a low interaction honeypot emulating the different services of ICS. HoneyPhy is one such honeypot for cyber physical system that is made for complex infrastructure (Litchfield et al., 2016). Usage of honeypots in these domains can protect the country from any type of terrorist attacks. It can be used as a bait to lure the intruders of country and then the information collected can be used to trace back the intruders. Thus, information collected can be used for mitigation purpose.

Figure 1. Concept of Honeypot



A large amount of work is progressing on honeypots by the means of projects that are running to curb the different attacks. One such project is Project Honey Pot (n.d.), distributed project started in 2004 to tackle spammers and spambots that lacerate address from different websites. It has collected a huge amount of data as different traps and IP are monitored. Security about the top countries that have to overlook some invasion is discussed. Figure 2 and Figure 3 illustrates the number of disparate plodder, robots, and spider till September 2016.

Figure 4 shows the top 6 comment spammer countries. Figure 5 embellish top six spam server countries in which China is pigeonholed as first and India is at fifth. India is top dictionary attacker countries followed by Brazil, Russia, and China as shown in Figure 6.

As per the statistics figured from this project has shown usage of a honeypot is eminent and can be used as an additional layer of internet security.