International Journal of Information Security and Privacy
Volume 11 • Issue 3 • July-September 2017

Honeypot Baselining for Zero Day Attack Detection

Saurabh Chamotra, CDAC, Mohali, India
Rakesh Kumar Sehgal, CDAC, Mohali, India
Ram Swaroop Misra, CDAC, Mohali, India

ABSTRACT

Honeypots are the network sensors used for capturing the network attacks. As these sensors are solely deployed for the purpose of being attacked and compromised hence they have to be closely monitored and controlled. In the work presented in this paper the authors have addressed the problem of base-lining the high-interaction Honeypots by proposing a structured framework for base-lining any high interaction Honeypot. The Honeypot base-lining process involves identification and white-listing of all the legitimate system activities and the modeling of Honeypot attack surface. The outcome of the Honeypot base-lining process is an XML file which models the Honeypot attack surface. The authors claim that this Honeypot system modeling is useful at the time of attack data analysis, as it enables the mapping of captured attacks to the vulnerabilities exposed by the Honeypot. This attack to vulnerability mapping capability helps defenders to find out what attacks targets what vulnerabilities and could also leads to the detection of the zero day vulnerabilities exploit attempt.

KEYWORDS

Attack Surface, Honeypots, Security, Vulnerabilities, Zero Day Attacks

1. INTRODUCTION

Honeypots are information system resources which are deployed for being attacked and compromised. Honeypot captures information about attacks, motives of the attackers and technique used by the attackers (Sehgal et al., 2012; Vrable et al., 2005; Leita et al., 2008; Anagnostakis et al., 2005). This information is useful for the defenders in developing robust mechanisms for detection and mitigation of such internet attacks. This Attack information when collected on a large scale by strategically deploying the Honeypot sensors can be converted in to threat intelligence (IOCs-incident of compromises) which is required by LEA (Law enforcement agencies) for understanding the overall threat landscape and early warning of any major attack incident. Organizations such as CERTs, security companies and academic research labs regularly needs this threat intelligence as feed for incident response, research and development purposes. To cater the needs of these user communities organizations such as (Team-Cymru, n. d.; Shadowserver, n. d.; abuse-ch, n. d.; SpamHaus, n. d.; NorseIPVIiking, n. d.; ATLAS, n. d.) are actively engaged in the large scale collection and processing of the threat intelligence. These organizations offer threat feeds as a service to the multiple user agencies. Standards such as (MAEC, n. d.; STIX, n. d.; TAXII, n. d.; OpenIOC, n. d.; and CYBOX, n. d.) has emerged for effective sharing and efficient usage of threat intelligence feeds. The organizations involved in the business of offering threat feeds as a service uses Honeypots as prime tool for capturing and collection of the attack data. Worldwide many projects such as (hoeynet.org, n. d.; GenIII Honeynets, n. d.; Honeynet.org, n. d.;

DOI: 10.4018/IJISP.2017070106

UKHoneynet, n. d.; NOHA, n. d.; Vanderavero et al., 2004; honeytarg, n. d.) are actively engaged in the capturing and collection of attack data using Honeypots.

Honeypot attract attacker by exposing network service vulnerabilities. Attackers targeting the users connected with internet get attracted by these vulnerabilities and attack these Honeypots. At Honeypot all the communication with attacker along with the system level activities are being monitored, captured and logged. The exploitability of the Honeypot can be measured in terms of Honeypot attack surface. The notion of system attack surface was first introduced by Howard (Howard, 2003). He proposed a measurement method for measuring the windows operating system's attack surface. In case of Honeypots, Attack surface can be defined as the complete set of vulnerabilities exposed by the Honeypot. These vulnerabilities are present in the network services running on the Honeypot along with their dependencies which are indirectly accessible to the attackers. Honeypot attack surface is a key factor which affects both value and the volume of attack data captured by the Honeypots.

Till date there were no standards available for the quantification of Honeypot attack surface. In the work presented in this paper we have tried to quantify the Honeypot attack surface by modeling the Honeypot attack surface. We have proposed a framework for baselining any high interaction Honeypot. The Honeypot baselining framework enables users to 1) enumerate the Honeypot system software, 2) modeling attack surface and 3) identifying and whitelisting legitimate system activities. The outcome of the Honeypot baselining process is used as an input for attack to vulnerability mapping module. This module maps the successful attacks captured by the honeypots to the vulnerabilities exposed by the Honeypot. This attack to vulnerability mapping leads to the detection of the zero day vulnerability exploitation attempts. In the work presented in this paper we have explained various phases of Honeypot baselining process and demonstrated it with a sample case study for windows 8 operating system

2. LITERATURE SURVEY

Since the first Honeypot was introduced (Toll., 1990; Cheswick, 1992) capturing of attacks and gathering attacker's information has been the prime objectives of the Honeypot. Projects such as (Kumar et al., 2012; Vrable et al., 2005; Vanderavero et al., 2004; UKHoneynet, n. d.) had done large scale distributed deployments of Honeypot sensors for capturing and collection of attacks targeting user community from specific functional domain, IP subnet or geographical region. Honeypot sensors have also evolved to increase the scope of data capturing. Latest Honeypot classes are designed to capture new classes of internet attacks (i.e. drive by download, attack targeting webservers, attack targeting IoT, etc.) (Dtag, n. d.; Honeydrive n. d.). In this arm race between hackers and Honeypot developers the standardization of Honeypot technology has taken a back seat. The dynamism involved in the attack trends and techniques is one of the reasons behind the lack of standardization of Honeypot/Honeynet technologies. It was Honeynet.org (Gen II & Gen III Honeynet architecture, n. d.) who first standardized Honeynet technology by launching GEN-I, GEN-II and GEN-III Honeynet frameworks. These frameworks come with standards for three major aspect of Honeynets 1) Data capturing, 2) Data control and 3) Data collection.

Most of the work done in the area of Honeypots is focused on the capturing, analysis and maintenance aspects of Honeypots but not much attention has been paid towards baselining of the Honeypot environment. Baselining Honeypot refers to formally defining Honeypot capturing environment and its boundaries by modeling the Honeypot attack surface and whitelisting the legitimate activities.

This notion of attack surface was first informally introduced by Howard (Michael Howard, 2003). He used a weighted attack vector schema to measure the system attack surface. Mandhata et al. (Mandhata, 2004, 2005, 2006) in his work moved one step further and have formalized the notion of attack surface and introduced attack surface metrics for the measurement of attack surface in a systematic manner. A large value of the metrics devised by Mandhata et al. indicates that an attacker

Designing a Secure Cloud Architecture: The SeCA Model

Thijs Baars and Marco Spruit (2012). *International Journal of Information Security and Privacy (pp. 14-32).*

www.igi-global.com/article/designing-secure-cloud-architecture/64344?camid=4v1a

Without Permission: Privacy on the Line

Joanne H. Pratt and Sue Conger (2009). *International Journal of Information Security and Privacy (pp. 30-44).*

www.igi-global.com/article/without-permission-privacy-line/4000?camid=4v1a