Efficacy Measuring Framework for the Assessment of Dynamic Honeypot

Vaishali Shirsath
Research Scholar
Veermata Jijabai Technological Institute
Mumbai (India)
vpnile_p19@ce.vjti.ac.in

Madhav M Chandane
Associate Professor - CE & IT
Veermata Jijabai Technological Institute
Mumbai (India)
mmchandane@it.vjti.ac.in

2021 International Conference on Advances in Computing, Communication, and Control (ICAC3) | 978-1-6654-2634-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICAC353642.2021.9697296

Abstract **- Honeypots are the form of decoys deployed in the network to capture malicious and unauthorized activities, they are also used to observe adversary behavior, tools, and strategies in a variety of ways. However, the effectiveness of the honeypot is only determined when it is breached by the intruder. Unfortunately, implementing and maintaining honeypots is difficult and it is also hard to measure the efficacy that compounds the problems after implementation. There is a need for some processes to determine if honeypot is efficient while it is kept active round-the-clock. This is an active issue since an ineffective honeypot could result in poor efficiency, misrepresentation, or even premature detection by an attacker. As a result, a detailed and in-depth analysis framework for honeypot efficacy has been proposed in this paper, which has hitherto not appeared in much literature, and reveals several important limitations of active honeypot for the organization when it is not required. The objective is to determine the decision matrix to assess honeypot's ability to fingerprint, obtain valid adversary data, deceive intruders, and smartly monitor the network environment at an optimum cost.**

Keywords: Cyber Deception, Cyber Decoy, Honeypot, Efficacy Measuring Framework.

I. INTRODUCTION

It is unsurprising that with the number of computer services on a network increase in global cyberspace, the scale of attacks on cybersecurity and its frequency also grows. E.g., according to the Cisco annual report (2018-2023), the DDoS attacks are projected to double at the compound annual growth rate (CAGR) of 15.4 million by 2023 [1]. Figures of energy sectors are also alarming, for 12 months, 53% of industrial stakeholders reported cyber-attack, according to LNS Research [2] and 76% of energy managers have listed business disruption as their organization's most impactful cyber loss scenario [3]. These trends are probably persisting because researchers have a broad understanding of attack forms, but the necessity to defend against adverse behaviors within the optimum cost is either overlooked or given less importance.

To mitigate or prevent these attacks, and complement existing defense infrastructures, the use of honeypot has been extensively suggested. Honeypot has been promoted by many researchers to misdirect or confuse attackers from valuable resources [4], and to draw them into a system designed to collect their data or to detect their presence, while some devices also stored attacker credentials through the use of honeypot [5] [6]. Since honeypot itself is not a standalone security system and only complement the existing security system it is also necessary to assess the requirement of honeypot when not in use. Even though honeypots entice attackers by simulating known vulnerabilities in operating systems, unfortunately, applications and services are incredibly difficult to implement and manage. [7].

Traditional measurement techniques of honeypot efficacy and the selection of mitigation strategies using simple assumptions often do not support actual uses of honeypot activeness. In this paper, the example model has been proposed to optimize the choice of whether to keep the honeypot active or passive when not required. The best choice of activating honeypot is only beneficial when the aim is to avoid severe damage and the attack is triggered. This methodology can be further utilized to quantify cybersecurity costs and support decision-making for the selection of optimal defense strategies. There are numerous suggestions in the literature on how to implement or manage dynamic honeypots correctly [8]. However, quantitative validation of efficacy is limited, leaving researchers unable to distinguish between modalities of implementation or management.

II. RELATED WORK

The majority of honeypot decisions are currently made in qualitative terms, and it is considered that quantitative models are not inherently better than qualitative models [9] [10]. Though it is advised that relying solely on a mathematical model is not suited for administrative purposes. However, [11] [12] proposed that such mathematical models can be used as a framework for effective quantification to determine whether to keep honeypot active or passive. The advantage of a quantitative approach is to force threat transparency, increase efficiency, and costs of those defense resources. Of course, for cyber risk management, quantitative models have been developed where the calculation of the Annual Loss Expectations (ALE) is a fundamental approach [13] [14]. While ALE permits a reverse-end computation, it is inadequate in two key areas, first, it provides an estimated value, without any knowledge on the distribution. which can be helpful to calculate more information, like expected

978-1-6654-2634-3/21/$31.00 ©2021 IEEE