Literature Review: A Particular Perspective Of The “Red Hat”

Introduction

With the advent of the internet, computer networks are becoming increasingly vulnerable to variety of attacks. This in part is because information is a protected asset, to safeguard confidentiality, integrity, and availability. Honeypot has been a subject of academic and popular literature that has been largely viewed from a particular perspective- the “REDHAT”. Based on the literature review described in this article, it is thought that the term honeypot is used broadly as the solution to all cyberattacks. This is believed to be subjective and uninformative. For Somwanshi, Joshi (Somwanshi A, 2016) Honeypot is an avenue through which online attacks can be traced.

This topic can be treated under two headings.

1. Literature review and current research
2. Solution and Implementation

Literature review and current research

Research in this area has resulted in several papers discussing the specific topics concerning honeypot creation and deployment. Although there are legal challenges amongst other issues, a large and growing body of literature has investigated honeypot detection. According to Tsikerdis (Tsikerdekis, 2018) malware detection evasion technique is said to be limited, whereas he is optimistic about machine learning as a way out. Baykara (Baykara M, 2018) in A novel honeypot-based security approach suggested a combination of Intrusion Detection System (IDS) with honeypot to achieve a high performance.

In an interesting analysis of honeypot by Naik et al (Naik N, 2018) in A Fuzzy Approach for Detecting and Defending Against Spoofing Attacks on Low Interaction Honeypot argued that High Interaction Honeypots (HIHs) should be used for backends of investigation. Pitman, Hoffpauir et al (Pittman J M, 2020)in A Taxonomy for Dynamic Honeypot Measures of Effectiveness, suggested a dynamic honeypot as the most effective. This view is supported by Naik et al (Naik N, 2018). The study would have been more interesting if they had included implementation. The study is therefore overambitious.

Moreover, Uitto, Rautti (Uitto J, 2017) in a survey on anti-honeypot and introspection method differ from Pitman, Hoffpauir (Pittman J M, 2020), in a number of ways that the honeypot is self-aware and can adapt to different environment at the same time, it can tell when it is discovered by honeypot ‘hunter’. This account must be approached with some caution because it argued about the ability of the honeypot to look real, which is feasible but impracticable.

Solution and Implementation

The most obvious finding to emerge from this study is that dynamic honeypot would be the most effective method for preventing honeypot detection. However, an ineffective implementation may lead to poor performance. This study was limited by the absence of qualitative validation of its effectiveness. In this regard, it leaves professionals, researchers, and educators without the means to differentiate the implementation from the theoretical modalities. A natural progression of this work, therefore, is to use python programming to visualise and analyse comparative data. The future area of study is preventing honeypot detection: An Analysis.

1. Baykara M, D. R., 2018. A novel honeypot based security approach for real time intrustion detection and prevention systems. ScienceDirect, Volume 41, pp. 103-116.
2. Naik N, J. P., 2018. A fuzzy approach for detecting and defending against spoofing attacks on low interaction honeypots. Cambridge, IEEE.
3. Pittman J M, H. K. e. a., 2020. A Taxonomy for Dynamic Honeypot Measures of Effectiveness. arXiv, Issue 2005, p. 10.
4. Somwanshi A, J., 2016. Implementation of honeypot for server security. IRJET, 03(03).
5. Tsikerdekis, M. Z. e. a., 2018. Approaches for preventing honeypot detection and compromise. Thessaloniki, IEEE.
6. Uitto J, R. S. e. a., 2017. a survey on anti-honeypot and introspection method. s.l., Springer Link.