Dynamic honeypot deployment in the cloud

Ivan Beres

Technical Report

RHUL–ISG–2022–2

11 April 2022

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

Honeypots are security defence tools, fake hosts designed to lure attackers away from real systems and capture malware threat analytics and attacker behaviour data for later analysis. This project sets out to research honeypots, their efficacy and the state of the art of honeypot development. Based on the research, a novel honeypot deployment concept is designed, implemented, tested and analysed leveraging cloud technologies.

Introduction

Honeypots are security defence tools. They are fake hosts designed to lure attackers away from real systems and capture malware threat analytics and attacker behaviour data for later analysis. The efficacy of a honeypot in attack mitigation and collecting attack behaviour analysis lies in its ability to obfuscate itself as a real system. Attackers are often successful in identifying honeypots because of the limitations inherent to fake systems. Honeypots are a vital part of the defence against attacks on computer networks. Their ability to lure attackers away from real targets makes them a crucial security tool. However, attackers are coming up with new ways of identifying and taking over honeypots. In the never-ending race against novel attacks, honeypots and how we use them must also be further developed.

This project solves some of the inherent limitations of honeypots by designing, building and evaluating a novel honeypot deployment concept leveraging cloud technologies. This new concept, a small, substantial contribution in the field, shifts the approach of deploying honeypots into the cloud. It is a new development in how honeypots are used and deployed in the cloud reducing the maintenance costs of honeypots in mitigating attacks by relying on resources that do not exist when the attack is started.

In section one of the project, the efficacy of common honeypots is researched, and gaps are identified in the literature to explore the state of the art of honeypot development and to pinpoint the issues with common honeypots, how attackers can identify them and the lack of research in leveraging the possibilities of the cloud in honeypot deployment. Section two breaks down the issues identified to honeypot believability, security, availability, automation and resource usage, setting the objectives to deploy honeypots in a resource-aware, timely and stealthy manner to resist identification by attackers by making honeypots indistinguishable from legitimate hosts. A novel, dynamic honeypot deployment concept is designed and implemented on a cloud platform in section three. Tests are set up, executed, and test results are captured in section four to prove the feasibility of the novel honeypot deployment design. Section five contains the analysis of the test results, and section 6 concludes the project. In section seven, further research opportunities of interest are discussed.