INTISARI

IMPLEMENTASI *ANSIBLE* PADA OTOMASI *HONEYPOT DEPLOYMENT* BERBASIS WEB

Dalam era digital yang semakin kompleks ini, keamanan sistem informasi menjadi masalah penting bagi organisasi di berbagai industri. Peningkatan serangan siber serta polanya yang semakin bervariatif bisa menimbulkan ancaman bagi kerahasiaan data atau integritas dari suatu organisasi. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) mencatat bahwa hingga sepanjang bulan April 2022, serangan siber di Indonesia telah mencapai angka 100 juta kasus dengan jenis serangan yang didominasi oleh serangan *ransomware* dan *malware*. Salah satu solusi untuk mengatasi permasalahan ini adalah dengan mengimplementasikan sistem *honeypot*. *Honeypot* telah berkembang menjadi salah satu alat yang berguna untuk mengidentifikasi serangan dan mempelajari strategi penyerang, yang memungkinkan organisasi untuk memperkuat pertahanan mereka. Namun, penerapan dan pengelolaan *honeypot* secara manual dapat memakan banyak waktu dan sumber daya. Oleh karena itu, penelitian ini bertujuan untuk melakukan otomasi proses *honeypot deployment* dengan menggunakan alat manajemen konfigurasi yang populer yang dikenal sebagai *Ansible*. Selain itu, untuk mempermudah pengoperasian *Ansible* dalam melakukan *honeypot deployment*, maka dibuat sebuah aplikasi *user friendly* berbasis web. Aplikasi tidak hanya sekedar melakukan *honeypot deployment*, namun juga memantau prosesnya. Berdasarkan hasil pengujian, aplikasi berhasil melakukan *honeypot deployment* ke semua sensor yang berjalan di *Google Cloud Platform* dengan tiga *region* berbeda.

Kata kunci: Otomasi, *Ansible*, Aplikasi Web, *Honeypot*, *Flask*, *Ansible AWX, Google Cloud Platform*

ABSTRACT

ANSIBLE IMPLEMENTATION FOR WEB-BASED HONEYPOT DEPLOYMENT AUTOMATION

In this increasingly complex digital era, information system security has become a crucial issue for organizations across various industries. The rising number of cyberattacks and their evolving patterns pose threats to the confidentiality and integrity of an organization's data. In Indonesia, the National Cyber and Crypto Agency (BSSN) reported that as of April 2022, cyberattacks in Indonesia had reached 100 million cases, dominated by ransomware and malware attacks. One solution to address this problem is the implementation of a honeypot system. Honeypots have evolved into a valuable tool for identifying attacks and studying attacker strategies, enabling organizations to strengthen their defenses. However, manually implementing and managing honeypots can be time-consuming and resource-intensive. Therefore, this research aims to automate the honeypot deployment process using a popular configuration management tool known as Ansible. Additionally, to streamline Ansible's operation in honeypot deployment, a user-friendly web-based application has been created. This application not only deploys honeypots but also monitors the process. Based on the test results, the application successfully deployed honeypots to all sensors running on Google Cloud Platform across three different regions.

Keywords: Automation, Ansible, Web Application, Honeypot, Flask, Ansible AWX, Google Cloud Platform.