# ABSTRAK

## ANALISIS DAN MANAJEMEN *LOG HONEYPOT* PADA *INFRASTRUCTURE AS A SERVICE (IAAS)* MENGGUNAKAN *ELASTIC STACK*

*Honeypot* merupakan salah satu sistem keamanan yang kerap diterapkan pada sebuah jaringan komputer dan digunakan untuk mengetahui perilaku serta jenis serangan pada suatu sistem atau infrastruktur jaringan. Data serangan dari *honeypot* biasanya disimpan dalam bentuk *log* pada *server* dimana *honeypot* tersebut dipasang. Seiring semakin banyaknya serangan yang memasuki *honeypot* tentu *log* tersebut akan memenuhi penyimpanan pada perangkat dan menyebabkan penuhnya ruang penyimpanan (*overload capacity)*. Pada penelitian ini akan dibuat sebuah mekanisme pemindahan data *log honeypot* dari sebuah *Virtual Private Server (VPS)* ke sebuah *server* pengumpul pada *Infrastructure as a Service (IaaS)* yang berada di jaringan internal UGM. *Log* yang berada pada *server* pengumpul selanjutnya disimpan ke dalam Elasticsearch dan MongoDB untuk dianalis serta ditampilkan menggunakan *platform* Elastic Stack.Protokol SMB menjadi protokol yang paling banyak diserang dengan jumlah 437.436 serangan. Selanjutnya, alamat IP 218.92.1.154 terdeteksi melakukan serangan *brute force* terbanyak dengan jumlah percobaan *login* gagal sebanyak 80.822 kali. Selain itu, *ransomware* WannaCry menjadi *malware* yang paling banyak tertangkap oleh sensor *honeypot*.

Kata Kunci : *log, honeypot, VPS, IaaS, MongoDB, Elastic Stack.*

# *ABSTRACT*

## *ANALYSIS AND MANAGEMENT OF HONEYPOT LOG ON AN INFRASTRUCTURE AS A SERVICE (IAAS) USING ELASTIC STACK*

*Honeypot is a security system that is often applied on a computer network and is used to determine the attackers behaviors and type of attacks on a network system or infrastructure. Attack data from honeypot is usually stored as logs on the server where the honeypot is implemented. As the number of attacks that enter the honeypot increase, of course the log will fill the storage on the server and cause overload (overload capacity). In this study will be created a mechanism for transferring honeypot log data from a Virtual Private Server (VPS) to a collector server in the Infrastructure as a Service (IaaS) is located on the UGM internal network. Logs that are on the collector server then will be stored into Elasticsearch and MongoDB to be analyzed and displayed using the Elastic Stack platform. SMB protocol is the most attacked protocol with 437,436 attacks. Furthermore, the IP address 218.92.1.154 was detected to carry out the most brute force attack with the total of failed login attempts 80,822 times. In addition, the WannaCry ransomware is the most caught malware by honeypot sensor.*

***Keywords****: log, honeypot, VPS, IaaS, MongoDB, Elastic Stack.*