IMPLEMENTASI SURICATA SEBAGAI IDS DAN ELASTIC STACK SEBAGAI SIEM PADA LAB DEVELOPMENT BPPT

NURUL HANIFAH PRATIWI

Sekolah Vokasi
College of Vocational Studies

PROGRAM STUDI TEKNIK KOMPUTER
SEKOLAH VOKASI
INSTITUT PERTANIAN BOGOR
BOGOR
2020

PERNYATAAN MENGENAI LAPORAN AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan laporan akhir berjudul "Implementasi Suricata sebagai IDS dan Elastic Stack sebagai SIEM pada Lab Development BPPT" adalah karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir laporan akhir.

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Institut Pertanian Bogor.

Bogor, Juni 2020

Nurul Hanifah Pratiwi
J3D117100

Sekolah Vokasi
College of Vocational Studies

RINGKASAN

NURUL HANIFAH PRATIWI. Implementasi Suricata Sebagai IDS dan Elastic Stack Sebagai SIEM pada Lab Development BPPT. *Implementation of Suricata as IDS and Elastic Stack as SIEM at BPPT Development Lab*. Dibimbing oleh RINGGA GILANG BASKORO.

Sebuah keamanan jaringan merupakan suatu aspek penting dalam membangun sebuah jaringan. Aliran data pada jaringan memiliki kerentanan terhadap berbagai paket data yang keluar maupun yang masuk pada lalu lintas jaringan. Kerentanan pada aliran data tersebut menjadi celah bagi seorang *hacker* untuk melakukan kejahatan terhadap lalu lintas jaringan. Kejahatan tersebut dapat berupa penyalahgunaan hak akses, maupun kegiatan ilegal lainnya.

Pembuatan implementasi Suricata sebagai IDS dan Elastic Stack sebagai SIEM merupakan salah satu solusi untuk mengamankan dan mengelola *log* pada sebuah jaringan. IDS (*Intrusion Detection System*) merupakan sebuah teknologi yang dapat mendeteksi serangan-serangan pada aliran data sebuah jaringan dengan memberikan *alert* dan informasi kepada administrator, salah satu perangkat lunak untuk membangun IDS yaitu Suricata. *Log* pada IDS akan dikelola oleh Elastic Stack yaitu perangkat lunak untuk membangun SIEM. SIEM (*Security Information and Event Management*) adalah teknologi yang digunakan untuk mengelola *log* dan *monitoring* lalu lintas jaringan. Pada implementasi ini SIEM digunakan untuk mengelola *log* data dari IDS.

Kata Kunci: *Intrusion Detection System, Suricata, Security Information and Event Management, Elastic Stack*

Sekolah Vokasi
College of Vocational Studies

IMPLEMENTASI *SURICATA* SEBAGAI IDS DAN ELASTIC STACK SEBAGAI SIEM PADA LAB DEVELOPMENT BPPT

NURUL HANIFAH PRATIWI

Sekolah Vokasi
College of Vocational Studies

Laporan Akhir
sebagai salah satu syarat untuk memperoleh gelar
Ahli Madya pada
Program Studi Teknik Komputer

PROGRAM STUDI TEKNIK KOMPUTER
SEKOLAH VOKASI
INSTITUT PERTANIAN BOGOR
BOGOR
2020

Penguji pada ujian laporan akhir : Anggi Mardiyono S.Kom., M.Kom

Judul Laporan Akhir	:	Implementasi Suricata sebagai IDS dan Elastic Stack sebagai SIEM pada Lab Development BPPT
Nama	:	Nurul Hanifah Pratiwi
NIM	:	J3D117100

Disetujui oleh

Pembimbing

Pembimbing 1 : Ringga Gilang Baskoro, S.Kom, M.Kom

Sekolah Vokasi
College of Vocational Studies

Diketahui oleh

Ketua Program Studi : Dr. Shelvie Nidya Neyman, S.Kom., M.Si
NIP. 19770206 200501 2 002

Dekan : Dr. Ir. Arief Darjanto, Dip.Ag.Ec., M.Ec.
NIP. 196106181986091001

Tanggal Ujian: 8 Juli 2020

Tanggal Lulus: 11 September 2020