ABSTRAK

Kemunculan ilmu dan teknologi memunculkan lebih banyak kerugian dalam bidang teknologi itu sendiri. Sama hal nya seperti jaringan, semakin kompleks jaringan tersebut dirancang, semakin kompleks pula masalah yang akan timbul dari sebuah serangan yang tidak bertanggung jawab. Serangan yang tidak dapat di prediksi kapan terjadi, terkadang membuat pemilik *server* lengah akan serangan yang terjadi saat jaringan tidak selama nya ia pantau.

Berdasarkan permasalahan yang terjadi, penulis membuat sebuah sistem monitoring aktifitas serangan yang dilakukan oleh pihak yang tidak bertanggung jawab dengan menerapkan jebakan untuk mengelabui pihak tersebut. Implementasi ini diterapkan pada sebuah Raspberry Pi dengan mengimplementasikan Honeypot didalamnya. Segala aktifitas penyerang yang terjadi akan tercatat oleh Cowrie dan menyimpannya dalam sebuah *database*. Informasi yang telah didapat lalu divisualisasukan pada Grafana dan dinotifikasikan secara otomatis kepada pemilik *server*.

Hasil dari pengimplementasian ini, dapat menangkap seluruh aktifitas penyerang tanpa ada kesalahan yang berarti pada trafik jaringan saat pemilik *server* menggunakan *server*nya secara bersamaan. Serangan yang dapat dicatat diantaranya *bruteforce* dan *port scanning* serta aktifitas masuk biasa pada *server*. Catatan serangan dikategorikan menjadi dua kondisi, jika serangan *success* dalam menginputkan kombinasi username dan *password* akan bersimbol angka 1 dan sebaliknya jika *failed* akan bersimbol 0, yang nantinya membantu dalam memvisualisasikan aktifitas yang terjadi.

Kata Kunci: Cowrie, *Server*, Grafana, Raspberry Pi, Telegram