ABSTRAK

Internet adalah suatu hubungan antara berbagai jenis komputer dan juga dengan jaringan di dunia yang punya sistem operasi dan juga aplikasi yang berbeda-beda. Berdasarkan hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia mencapai 215,63 juta orang pada periode 2022-2023. Semakin bertambahnya pengguna internet, semakin tinggi serangan siber yang mengancam komputer. Penelitian ini membahas tentang serangan pada *server* tiruan dan memperkuat *server* asli. *Server* tiruan tersebut dibuat menggunakan *honeypot* supaya sistem mampu merekam dan memonitoring aktivitas yang dilakukan oleh penyerang sehingga dapat memberi informasi ke pada seorang administrator. Pada penelitian ini akan menggunakan dua jenis *honeypot* yaitu Kippo dan Dionaea untuk mengamankan *server*, kedua *honeypot* ini memiliki kemampuan berbeda-beda. Dimana pada proses pengujian *honeypot* kippo digunakan untuk memonitoring serangan *Brute Force* sedangkan Dionaea digunakan untuk memonitoring serangan DoS dan Sql. Pengujian dilakukan dalam dua skenario, skenario pertama menyerang *server* tiruan dan skenario kedua menyerang *server* asli yang sudah diperkuat dengan melihat hasil pada skenario pertama. Hasil penelitian pada skenario pertama menunjukkan bahwa sistem *honeypot* yang di implementasikan pada penelitian berhasil merekam setiap kegiatan yang dilakukan oleh *attacker* dimana informasi tersebut terekam secara *real time* dan disimpan dalam bentuk *log file*, kemudian pada skenario kedua penyerang tidak dapat masuk ke *server* asli dikarenakan penulis sudah memblokir ip penyerang dan menutup semua *port* yang memungkinkan dimasuk oleh si penyerang.

Kata Kunci: *Brute Force, Daniel of Server, Honeypot, Honeypot Kippo Graph, Honeypot Dionaea, Medusa, SQL.*