ABSTRAK

Teknologi internet saat ini tidak lepas dari banyak masalah ataupun celah keamanan. Banyaknya celah keamanan ini dimanfaatkan oleh orang yang tidak berhak untuk mencuri data-data penting. Kasus serangan terjadi karena pihak yang diserang juga tidak menyadari pentingnya keamanan jaringan untuk diterapkan pada sistem yang dimilki.

Honeypot adalah suatu sistem yang didesain menyerupai *production system* asli dan dibuat dengan tujuan untuk diserang / disusupi. *Honeypot* diimplementasikan menggunakan *honeypot* jenis *low interaction* yaitu Glastopf serta menggunakan *software* pendukung lainnya. Uji coba ketahanan dilakukan dengan cara penyerangan langsung untuk mengetahui keamanan dari sistem.

Hasil dari penelitian ini adalah *low interaction honeypot* pada *embedded system* berupa Cubieboard yang dapat mengemulasikan celah keamanan *directory buster brute force*, *LFI*, *RFI*, namun masih belum dapat mengemulasikan celah *SQL Injection*. Salah satu hasil *stress test* dengan 773 sampel, didapatkan waktu *average* 5275 ms, deviasi 2067 ms, throughput 367,012 sampel per menit, dan dengan median 5831 ms yang dilakukan dengan 50 *threads* dan 10 *ramp-up* per detik.

Kata kunci: *honeypot*, Cubieboard, *low interaction*, *web server,* keamanan