

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 dimiliki.

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

Penyerangan ini dilakukan dengan lima cara yaitu menggunakan *directiory buster brute force*, RFI, SQL Inject, *strest test* dan DoS. *Honeypot* dapat menyimulasikan serangan tersebut dengan sangat baik, namun tidak dengan serangan DoS. Sehingga *honeypot* ini mampu untuk menipu peretas karena mampu memberikan respon yang baik dari penyerangan tersebut.

Kata kunci: *honeypot*, *high interaction*, *web server*, keamanan