ABSTRAK

Internet merupakan media yang digunakan pengguna untuk mengakses layanan, misalnya layanan *web*. Pada suatu *web* memiliki *server* yang dikenal dengan istilah web *server* yang berfungsi untuk melayani permintaan dan menampung informasi penting pada *web*. Karena *web server* merupakan wadah dari informasi penting yang ada pada web, membuat *web server* menjadi pertimbangan utama untuk diamankan dari serangan yang dapat membahayakan sistem informasi. Karena hal tersebut, keamanan pada *web server* sangat dibutuhkan untuk mencegah penyerang melakukan serangan. *Port knocking* dan *honeypot* merupakan metode yang digunakan untuk mengamankan web *server* dari upaya penyerangan. *Port knocking* melakukan pencegahan dengan cara menutup *port logic* yang telah ditentukan. Akan tetapi, *port* tersebut tetap dapat diakses oleh *administrator* atau yang memiliki hak akses dengan cara mengetuk *port* sesuai dengan tahapan parameter yang sudah ditentukan. Kemudian, ketika penyerang mencoba masuk melalui *port logic* yang sudah dilakukan *port knocking* dan tidak mempunyai hak akses maka penyerang akan ditolak untuk masuk dan dialihkan ke *honeypot*. Pada metode *honeypot* digunakan sebagai *server* tiruan atau palsu dimana penyerang akan menyangka bahwa *server honeypot* adalah *server* yang asli. Selain menjadi *server* tiruan, *honeypot* juga dapat melihat aktivitas yang dilakukan penyerang saat berada di dalam *server honeypot*. Pengujian ini membutuhkan dua buah perangkat komputer, dimana satu sebagai komputer *client* yang digunakan untuk menyerang dan satu sebagai komputer *server*. Metode kombinasi *port knocking* dan *honeypot* akan diaktifkan pada komputer *server*. Parameter pengujian dilakukan dengan cara menggunakan serangan *port scaning* dan *brute force* untuk menguji keberhasilan kombinasi metode *port knocing* dan *honeypot.* Hasil pengujian dengan melakukan *review* literatur *port knocking* dan *honeypot* bekerja dengan baik. *Port knocking* dapat memberikan aturan *port*, sedangkan *honeypot* dapat membuat *server* bayangan dan dapat mencatat aktifitas penyerang.

Kata Kunci : *Brute force, Honeypot*, Keamanan jaringan, *Port Knocking, Port scanning*.