ABSTRAK

Pada umumnya serangan terhadap suatu komputer dalam suatu jaringan ialah melalui aplikasi yang masuk pada port-port terbuka dalam server. Port-port yang terbuka ini rawan terhadap eksploitasi dari akses yang tidak diinginkan, untuk itu dibutuhkan suatu system yang dapat menangkal masalah tersebut.

Port Knocking adalah salah satu system keamanan yang dapat melakukan fungsi seperti yang digambarkan diatas yaitu mem-blok akses yang tidak diinginkan. Pada prinsipnya, *port knocking* menutup seluruh port yang ada di server. Bila user menginginkan akses ke server, user melakukan "ketukan" untuk menggunakan layanan, kemudian bila *user* telah selesai melakukan akses maka port ditutup kembali. Tujuan yang ingin didapat dari proyek akhir ini ialah server berhasil melindungi layanan yang ada (disini berupa file server) dengan mengintegrasikan aturan *firewall* yang ada dengan program port knocking yang digunakan, dan menunjukkan bahwa tanpa mengirimkan ketukan atau password yang tepat, user (client) tidak dapat menggunakan layanan pada server.

Dari hasil penelitian yang dilakukan didapat bahwa perbedaan yang didapat dari penggunaan kedua program ini ialah knockd tidak menggunakan enkripsi dalam mekanisme pengiriman ketukannya, sedangkan fwknop menggunakan enkripsi. Untuk penggunaan fwknop, ketukan yang dikirimkan menuju server sebagai kunci autentikasi ialah sebesar 206 bytes (ketukan yang dikirim hanya menuju sebuah port 62201 (UDP)), kemudian jika client keluar dari layanan file server setelah batas 30 detik yang ditentukan konfigurasi program, maka client diharuskan melakukan proses autentikasi kembali seperti sebelumnya. Berbeda dengan program Knockd yang menggunakan mekanisme pengiriman ketukan menuju beberapa port pada server, baik untuk buka ataupun tutup koneksi tanpa menggunakan batas waktu untuk autentikasinya.

Kata kunci : ***autentikasi, eksploitasi, enkripsi, firewall, port knocking***