ABSTRAK

Perkembangan teknologi jaringan komputer semakin meningkat. Kemajuan teknologi ini menambah perkembangan teknologi sebagai *trend* baru untuk mengekspresikan kreativitas. Namun terdapat dampak yang tidak bisa dihindari. Salah satunya serangan ke *server* yang terjadi belakangan ini yang mulai banyak terjadi. Seperti penyerangan terhadap SSH (*Secure Shell*) untuk melakukan *remote server*. Sehingga diperlukan pengamanan terhadap SSH, salah satunya dengan menggunakan *Fail2ban*. *Fail2ban* digunakan untuk menangani serangan *brute force* dan *dictionary attack* pada *linux* dengan cara membaca *log file* dari SSH, *apache* dan lainnya, kemudian secara otomatis menerapkannya pada *IPtables* untuk memblok serangan. Pada *Fail2ban* ini terdapat konfigurasi untuk mengatur waktu blok akses, dan jumlah maksimum berapa kali *user* dapat mencoba *login*. Tidak hanya keamanan, diperlukan juga *monitoring* pada SSH *server* agar *admin* tidak perlu berada 24 jam di depan *server* untuk mengawasi *port* SSH. Pada *monitoring* ini terdapat notifikasi ketika *user login* ke *server* yang akan dikirim ke *Telegram Messenger*. Notifikasi yang dikirim berupa tanggal, jam masuk, alamat IP *Host*, IP pengguna, serta informasi ISP, kota, dan Negara pengguna. Hasil pengujian menunjukan bahwa *Fail2ban* dapat mencegah serangan dari aplikasi *Hydra* dan *Metasploit*.

Kata Kunci: *Fail2ban*, SSH, *Telegram Messenger*