

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Pada bab ini akan membahas kesimpulan apa saja yang diperoleh dalam pengerjaan Tugas Akhir ini. Berikut ini hasil kesimpulan pada *implementasi IDS Bro dan IP Tables*

1. Bro mampu mendeteksi serangan *port scanning, ssh bruteforce, syn flood* pada saat terjadinya serangan.
2. Bro mampu memberikan notice apabila terjadi serangan dengan pemberitahuan Email jika terjadi serangan.
3. Bro dapat mengirimkan pemberitahuan Email jika terjadi serangan. Postfix dapat terhubung pada Bro menggunakan bantuan SMTP Google.
4. Iptables mampu melakukan tindakan hanya melakukan tindakan pencegahan pada serangan *port scanning dan ssh bruteforce*, tetapi *ip tables* belum bisa mencegah apabila terjadi serangan *syn flood* pada server

5.2. Saran

Karena IDS Bro harus bekerja secara *real time* dan dalam waktu yang lama, maka dibutuhkan seorang administrator untuk mengawasi dan menjalankan IDS Bro.

Meskipun sudah diterapkan email sebagai pemberitahuan, hal tersebut masih kurang untuk mengawasi jaringan. Saran untuk penelitian kedepannya yaitu membuat IDS Bro. dapat digunakan untuk melakukan pengawasan dan pendeteksian secara maksimal meskipun administrator tidak berada ditempat. Cara untuk melakukan hal tersebut yaitu dengan cara Bro dapat diremote melalui jarak jauh dengan koneksi internet. Meskipun administrator tidak berada ditempat, tetapi administrator mampu mendeteksi serangan melalui remote jarak jauh.