BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan dan pengujian yang telah dilakukan dalam penerapan Snort IDS sebagai pendeteksi serangan DDoS pada server Kali Linux dapat disimpulkan bahwa :

1. Serangan DDoS dapat terjadi pada jaringan dan dapat bertujuan membuat server tidak bisa diakses oleh klien yang mengakibatkan downtime pada server Kali Linux. Hal tersebut bisa terjadi karena adanya traffic flooding yang mana teknik ini penyerang berusaha membanjiri lalu lintas jaringan server dengan data paket sebanyak mungkin yang mengakibatkan server mengalami downtime yang tidak bisa diakses oleh klien.
2. Dengan sistem Snort IDS yang telah diterapkan untuk memonitoring jaringan pada serangan DDoS dan Port Scanning telah berhasil dibangun dan dikembangkan dengan baik. Sistem Snort IDS ini berfungsi sebagai firewall pendeteksi instrusi keseluruhan sistem Snort IDS dapat bekerja dengan efektif sebagai sistem keamanan jaringan komputer dalam mendeteksi sebuah intruder atau penyusup pada server Kali Linux. Untuk mengamankannya Snort akan langsung mengatasi serangan tersebut, dengan cara langsung melalui sistem server memberikan notifikasi alert log serangan DDoS dan Port Scanning melalui websnort jika terjadi serangan terhadap server 106 maka akan mengirimkan alert log yang akan dikelola oleh websnort interface.
3. Dengan menerapkan Snort sebagai sistem pendeteksi instrusi pada server Kali Linux dapat membuktikan bahwa Snort mampu berpotensi melakukan pendeteksian dalam memantau dan menganalisis aktifitas dengan mengirimkan peringatan berupa alert yang telah terjadi penyerangan terhadap server Kali Linux. Maka dari itu untuk menganalisis yang berpotensi melakukan serangan tersebut adalah PC Attacker yang dimana PC Attacker tersebut melakukan penyerangan terhadap PC Server, hal tersebut akan dideteksi oleh Snort pada sistem server.

5.2 Saran

Saran-saran yang diberikan pada penelitian ini yang telah dilakukan adalah sebagai berikut :

1. Dalam segi pendeteksian dapat dilakukan dengan baik karena dapat melihat lalulintas jaringan yang sedang terjadi. Akan tetapi dari sisi pencegahan masih harus dikembangkan lagi dalam melindungi aset yang terdapat pada server yang menjadi tujuan dari penyerangan.
2. IDS hanya bisa melakukan monitoring pada jaringan, akan lebih baiknya IDS diterapkan dapat melakukan pencegahan dari serangan yang terjadi secara otomatis.
3. Penambahan pelaporan rekapan data Instrusi pada administrator server bukan hanya dari notifikasi websnort dan bot telegram, tetapi juga 107 dalam bentuk dokumen seperti .pdf, .xls, dsb untuk lebih detail lagi dalam pendeteksian.