BAB V

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Dengan adanya penyelesaian dalam pelaksanaan skripsi dan observasi pada CV. Cyber Makassar ini dapat disimpulkan antara lain :

1. Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada di dalam rule IDS atau tidak. Oleh karena itu, rule IDS harus secara rutin diupdate.
2. Secara garis besar, Peletakkan sistem Snort-IDS pada suatu topologi jaringan bisa dimana saja, asalkan memasukkan IP gateway jaringan di file konfigurasi Snort, maka sistem akan mendeteksi dan memantau *traffic* di seluruh host yang ada pada jaringan gateway yang sama.
3. Untuk mempermudah analisa terhadap catatan-catatan IDS (sequrity event) perlu ditambahkan modul tambahan seperti ACID (Analysis Console for Intrusion Databases).

5.2 SARAN

Adapun saran mengenai penyelesaian dalam pelaksanaan kerja praktek antara lain :

1. Update rule pada firewall seharusnya dalam bentuk daemon proses sehingga proses bekerja secara realtime, yang kami bangun masih dalam bentuk script yang dieksekusi secara periodik (1 menit sekali)
2. Manajemen rule sebaiknya dibuat tersendiri, dapat dilakukan dengan pemrograman aplikasi berbasis web bukan menggunakan applikasi Webmin, dikarenakan Webmin merupakan administrasi secara keseluruhan system Linux dan hanya dilindungi dengan form autentification sehingga jika suatu saat Webmin dapat dikuasai, maka keseluruhan sistem akan dikuasasi juga.
3. Perlu diuji pada jaringan dengan *traffic* yang sangat tinggi sehingga kinerja IDS dapat terukur-tidak hanya fungsionalitasnya saja yang mampu mendeteksi penyusupan .
4. Perlu dikembangkan sesuai kebutuhan organisasi dan perkembangan teknologi.