BAB IV

KESIMPULAN DAN SARAN

1.1 Kesimpulan

Dengan adanya penyelesaian dalam pelaksanaan kerja praktek 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. Untuk mempermudah analisa terhadap catatan-catatan IDS (*sequrity event*) perlu ditambahkan modul tambahan seperti ACID (*Analysis Console for Intrusion Databases*).

1.2 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 .