BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan dengan hasil analisa dan pengujian yang telah dilakukan, dapat diketahui bahwa perkembangan *website* yang semakin cepat dengan berbagai fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan *webserver*. Terutama dengan semakin terbukanya pengetahuan *hacking* dan *cracking*, didukung dengan banyaknya *tools* yang tersedia dengan mudah dan *tools* tersebut dapat diperoleh gratis (*free*), sehingga semakin mempermudah para *intruder* dan *attacker* untuk melakukan aksi penyusupan ataupun serangan.

Dengan adanya pengujian serangan *Denial of Service* (*DoS*) terhadap *webserver*, dapat diketahui bahwa serangan *DoS* dapat mengakibatkan *webserver* menjadi lambat. Hal ini terbukti ketika terjadi peningkatan nilai *CPU history* dari keadaan normal 7,1% menjadi 62,4% setelah serangan, begitu pula dengan nilai traffic pada memory, received, dan sending data. *Webserver* juga mengalami kegagalan dalam melayani permintaan halaman *web* dari *client* karena tidak dapat menangani beban *request* yang banyak dalam waktu yang singkat dan berakhir dengan menghentikan aktivitas atau berhenti dengan sendirinya karena tidak mampu melayani *request*. Hal ini terbukti pada saat pengujian serangan *DoSHTTP*, *webserver* menerima 179709 request dan kemudian merespon sebanyak 175820. Dengan demikian, keamanan suatu jaringan *webserver* sebelum

diterapkan *firewall* dapat dikatakan tidak aman dimana terdapat celah-celah yang dapat meretas ke jaringan *webserver.*

Keamanan webserver berhasil ditingkatkan ketika diterapkan *Iptables*, *Iptables* dapat melakukan *filtering* ketika terjadinya serangan *DoS* saat dilakukan simulasi dengan komputer penyerang. Hal ini terbukti pada saat simulasi serangan *DoS*, *webserver* mengalami perubahan dari sebelum diterapkan *Iptables*, *webserver* merespon sebanyak 175820 dari total 179709 *request* (97,8%) menjadi 19 *request* dari total 23520 *request* yang dihasilkan, sehingga *webserver* tidak mengalami kewalahan melayani *request* yang terkirim sebanyak itu. Oleh karena itu, dengan menerapkan *Iptables* sebagai *firewall* dalam keamanan jaringan *webserver* dapat memblokir adanya serangan *DoS* atau penyusupan serta dapat diantisipasi dengan cepat.

5.2 Saran

Hasil penelitian ini diharapkan dapat bermanfaat bagi pihak-pihak terkait dan dapat mendorong dan memicu dilakukan penelitian-penelitian berikutnya. Pada perkembangan selanjutnya, disarankan agar dapat menerapkan sistem keamanan jaringan berlapis, yaitu dengan menerapkan *Iptables* sebagai *firewall* dan *Instrusion Detection System* (*IDS*) sebagai pendeteksi. Dengan adanya *Iptables* yang berfungsi melakukan *filtering* terhadap (*traffic*) lalu lintas data dan membatasi atau mengontrol akses terhadap pengguna yang tidak berhak seperti *hacker* dan *intruder*. Kemudian, *instrusion detection system* sebagai pendeteksi aktivitas yang mencurigakan seperti serangan atau penyusupan dalam sebuah

sistem atau jaringan, dan memberikan peringatan (*alert*) kepada sistem atau administrator jaringan sehingga para administrator dapat langsung melakukan aksi pemblokiran seorang user atau alamat IP yang dianggap tidak normal.

Sedangkan, bagi perusahaan disarankan agar selalu memperbaharui sistem keamanan jaringan yang telah ada sesuai dengan perkembangan kemajuan teknologi keamanan jaringan komputer, karena perkembangan yang terjadi sangatlah cepat.