BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan apa yang telah didapat dari bab sebelumnya, maka pengujian keamanan *firewall* pada sistem X dan sistem Y Universitas Z dapat diambil beberapa kesimpulan, diantaranya:

1) Pengujian keamanan *firewall* dapat dilakukan dengan melakukan proses *penetration testing* yang melalui beberapa tahap mulai dari pencarian *IP address*, melakukan *traceroute*, mengirimkan *ping*, *fingerprint OS*, melakukan pemindaian *port*, melakukan pemindaian versi, melakukan pemindaian agresif, melakukan *scripting*, serta melakukan pemindaian kerentanan. Setelah melakukan pemindaian kerentanan, maka akan didapatkan hasil pemindaian kerentanan yang berisi dengan kerentanan-kerentanan dengan masing-masing tingkat kerentanannya, informasi-informasi yang perlu diperhatikan agar keamanan jaringan dapat semakin ditingkatkan beserta tawaran solusi yang dapat diterapkan.
2) Tingkat keamanan *firewall* yang dimiliki oleh sistem X dan Y pada Universitas Z memiliki hasil yang berbeda dimana:
   a) Sistem X memiliki tingkat keamanan yang cukup baik dikarenakan masih terdapat beberapa kerentanan tingkat tinggi, sedang, dan rendah yang masih perlu diperbaiki.
   b) Sistem Y memiliki tingkat keamanan yang baik dikarenakan masih memiliki beberapa kerentanan tingkat sedang dan rendah yang masih perlu diperbaiki.

   Dengan demikian dapat dikatakan bahwa sistem Y memiliki keamanan jaringan yang lebih baik dibandingkan dengan sistem X.

5.2. Saran

Saran yang dapat diberikan setelah melakukan pengujian ini adalah dengan menggunakan aplikasi pengujian kerentanan yang lain seperti OpenVAS, Cisco Auditing Tools (CAT), atau aplikasi lainnya untuk melakukan pengujian terhadap

firewall. Penggunaan aplikasi pengujian yang lain memungkinkan kita untuk melihat potensi-potensi kerentanan yang bisa saja terlewat atau tidak terdeteksi dengan menggunakan aplikasi yang digunakan pada penelitian ini. Selain itu, peneliti juga sangat menyarankan untuk menggunakan aplikasi *Nessus Profesional* dikarenakan aplikasi *Nessus Essentials* yang digunakan pada penelitian ini memiliki fungsi yang terbatas seperti hanya dapat melakukan pemindaian kepada 16 alamat IP saja serta tidak dapat melakukan audit kepatuhan, sedangkan pada *Nessus Profesional*, jumlah alamat IP yang dapat dipindai tidak terbatas, sedangkan audit kepatuhan dapat kita lakukan. Selain itu *Nessus Profesional* memperbolehkan kita untuk melakukan beberapa hal yang tidak dapat kita lakukan dengan menggunakan *Nessus Essentials*.