BAB V

KESIMPULAN DAN SARAN

1. Kesimpulan

Setelah melakukan beberapa kali pengujian pada jaringan nirkabel yang menggunakan kemanan WEP, penulis berhasil membuktikan bahwa celah keamanan yang terdapat pada sistem keamanan WEP sudah tidak dapat ditoleransi lagi. Artinya sistem keamanan WEP tidak dapat diimplementasikan pada jaringan nirkabel yang benar-benar membutuhkan keamanan. Penulis telah berhasil membuktikan bahwa dengan menggunakan beberapa tool dan trik tertentu seorang *hacker* dapat dengan mudah masuk ke dalam jaringan WEP. Bahkan hanya dengan menggunakan beberapa tool sederhana dan gratis dalam hitungan menit.

Serangan-serangan pada kelemahan WEP antara lain :

1. Serangan terhadap kelemahan inisialisasi vektor (IV), sering disebut *FMS attack*. FMS singkatan dari nama ketiga penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyakbanyaknya. Semakin banyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan.
2. Mendapatkan IV yang unik melalui packet data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut *chopping attack*, pertama kali ditemukan oleh h1kari. Teknik ini

hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.

3. Kedua serangan diatas membutuhkan waktu dan packet yang cukup, untuk mempersingkat waktu, para hacker biasanya melakukan *traffic injection*. Traffic Injection yang sering dilakukan adalah dengan cara mengumpulkan packet ARP kemudian mengirimkan kembali ke access point. Hal ini mengakibatkan pengumpulan initial vektor lebih mudah dan cepat. Berbeda dengan serangan pertama dan kedua, untuk serangan traffic injection,diperlukan spesifikasi alat dan aplikasi tertentu yang jarang ditemui di toko-toko, mulai dari chipset, versi driver dll.

Selain sistem keamanan jaringan nirkabel dengan menggunakan WEP, terdapat sebuah alternatif lain yang relatif lebih aman apabila diimplementasikan dengan benar, sistem ini dikenal dengan WPA. Terdapat dua jenis keamanan WPA yaitu WPA-Radius dan WPA-PSK. Biasanya, untuk jaringan nirkabel rumahan dan kantor berskala kecil kemanan WPA-PSK banyak digunakan, selain mudah untuk diimplementasikan juga telah didukung banyak peralatan dan sistem operasi, sistem keamanan ini juga tidak membutuhkan server tambahan dengan konfigurasi yang cukup rumit seperti pada sistem keamanan WPA-RADIUS. Namun WPA-PSK tidak serta merta bebas dari masalah keamanan. Apabila tidak dikonfigurasi dengan benar sistem kemanan ini menjadi tidak berarti. Penulis telah melakukan pengujian untuk

membuktikan hal ini. Salah satu penyebab celah keamanan yang terdapat pada WPA-PSK yaitu passphrase yang lemah dan mudah ditebak. Dengan menggunakan tool tertentu dan juga didudukung dengan daftar kamus (dictionary) berukuran besar dan lengkap, bukan tidak mungkin passphrase yang lemah ini kemudian dapat dipecahkan. Serangan ini disebut dengan *brute-force attack*.

2. Saran

Dengan mengetahui kelemahan-kelemahan tersebut, diharapkan para administrator jaringan nirkabel mulai meninggalkan sistem kemanan WEP dan beralih minimal menggunakan sistem kemanan WPA-PSK dengan menggunakan passphrase yang kuat. Misalnya saja sebuah kalimat yang berupa gabungan dari huruf, angka, dan simbol. Sehingga mempersulit proses brute-force attack.

Sebelumnya penulis juga telah menuliskan langkah-langkah yang dapat dilakukan untuk mengurangi kegiatan hacking jaringan nirkabel, apabila langkah-langkah tersebut dijalankan dengan benar mudah-mudahan jaringan nirkabel anda akan lebih aman, minimal menghambat kerja hacker. Tapi yang perlu diingat adalah bahwa dunia kemanan jaringan merupakan wacana yang cukup menarik untuk diperbincangkan, bukan tidak mungkin sistem keamanan berlapis yang anda gunakan ditambah sistem kemanan baru yang telah diciptakan akan tetap bisa di tembus oleh para hacker. Untuk itu disarankan pula untuk tetap mengikuti perkembangan jaringan nirkabel dimasa datang.

Penelitian ini sebelumnya dapat berhasil dilakukan apabila pada jaringan nirkabel diterapkan DHCP untuk mengalokasikan IP address kepada client. Namun untuk jaringan nirkabel yang menggunakan IP statis, penulis belum melakukan penelitian lebih lanjut sehingga penulis belum menemukan cara untuk mengaudit atau melakukan kegiatan hacking pada jaringan tersebut. Diharapkan bagi peneliti yang ingin mengembangkan hasil penelitian ini, untuk dapat mengembangkan metode yang lebih baru sehingga dapat masuk pada jaringan nirkabel yang menggunakan IP statis. Disamping mencari dan menemukan celah kelemahan pada jaringan nirkabel, diharapkan juga pada penelitian berikutnya agar mampu menemukan bagaimana cara untuk menutupi kelemahan-kelemahan yang telah ditemukan pada penelitian ini sehingga hasil penelitian dapat lebih bermanfaat dalam dunia keamanan jaringan khususnya pada jaringan nirkabel.