BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dalam penelitian ini penulis telah berhasil membuktikan celah keamanan pada jaringan nirkabel yang menerapkan WEP. Beberapa celah keamanan WEP yang penulis manfaatkan yaitu:

Pertama, *keystream reuse*, berasal dari kesalahan managemen IV. Karena *secret key*, *k*, sangat jarang berubah, menyebabkan IV sering digunakan berulang kali dan berpengaruh juga pada *keystream*. Karena IV di publik, duplikasi IV sangat mudah di deteksi oleh *hacker*. Penggunaan IV yang berulang kali ini disebut dengan *collisions*. Dengan demikian, hacker hanya perlu mengumpulkan sejumlah IV untuk mendapatkan *secret key* WEP.

Kedua, keterbatasan numerical 24-bit pada IV, yang menghasilkan nilai 16.777.216, dimana untuk mengumpulkan jumlah ini diperlukan waktu sekitar 5 jam. Namun dalam prakteknya menulis bisa mengumpulkan dalam waktu 30 menit, dengan cara mempercepat proses *sniffing* menggunakan metode *packet injection*.

Ketiga, terdapat kelemahan pada protokol WEP yaitu tidak dapat memfilter replay paket yang dikirimkan. Sehingga dapat dimungkinkan pesan di replay atau mengirimkan kembali pesan tersebut walaupun tidak dimodifikasi. Kelemahan inilah yang menyebabkan terjadinya metode *packet injection*, karena dengan memanfaatkan fungsi protokol ARP, *hacker* dapat dengan mudah melakukan pengiriman paket ke AP. Kemudian AP akan mereplay paket tersebut.

Selain itu penulis juga menyimpulkan kasus seperti *packet injection* hanya *powerfull* jika jaringan tersebut terkoneksi internet, karena jumlah paket data yang dikirimkan oleh klien akan lebih cepat dan besar melalui jaringan yang di NAT.

5.2. Saran

Dengan mengetahui kelemahan-kelemahan tersebut, diharapkan para administrator mulai meninggalkan metode keamanan WEP. Sekarang IEEE sendiri telah mengembangkan metode keamanan WPA dan 802.1x untuk menangani atau lebih tepatnya menggantikan WEP. Namun penulis juga mempunyai solusi untuk mengurangi resiko kerusakan terhadap serangan tersebut, yaitu :

Pertama, menggunakan *access control* atau melakukan pembatasan terhadap MAC address dan IP address.

Kedua, karena metode penyerangan *packet injection* memanfaatkan protokol ARP, maka perlu dilakukan *filtering* ARP. Administrator dapat menggunakan tool ebtables dan arp tables untuk mengatasi *packet injection* menggunakan ARP.

Ketiga, WDS (*Wireless Distribution System*), sistem ini digunakan untuk memperluas lingkup jaringan nirkabel dengan menambahkan *node* tertentu, sehingga klien yang terhubung tidak akan langsung berkomunikasi dengan klien lain, melainkan harus melewati *node* tersebut. Hal ini juga dapat mengurangi serangan langsung terhadap klien dan AP.

Keempat, *Captive Portal*, Infrastruktur *Captive Portal* awalnya didesign untuk keperluan komunitas yang memungkinkan semua orang dapat terhubung (*open network*). *Captive Portal* sebenarnya merupakan mesin *router* atau *gateway* yang memproteksi atau tidak mengizinkan adanya trafik hingga user melakukan registrasi/otentikasi.

Saran pertama dan kedua akan berdampak pada pembatasan gerak si penyerang, sehingga waktu yang dibutuhkan penyerang untuk melakukan *cracking* dapat diperlambat.

Saran-saran diatas hanya bersifat mengurangi resiko, karena terdapat pengembangan serangan lain yang tidak dapat di tangani oleh solusi tersebut,

seperti kemungkinan MAC *spoofing* dan IP *spoofing* pada DHCP server, kelemahan authentikasi yang tidak terenkripsi pada captive portal seperti NoCat, dan kemungkinan jenis penyerangan lain.

Sejauh ini yang dapat secara maksimal menutupi kekurangan terhadap penyerangan adalah penggunaan server RADIUS, atau akan lebih maksimal jika mengkombinasikan seluruh solusi yang ada.