BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dalam penelitian ini telah berhasil membuktikan bahwa celah keamanan pada jaringan nirkabel Puri Ayu Homestay yang menerapkan WEP 64bit. Beberapa uji coba serangan WEP yang dilakukan yaitu:

1. Pertama, *Chopchop attack*, Untuk mempercepat proses ini dilakukan deauthentification pada client yang terkoneksi dengan jaringan tersebut. Menggunakan 1000 injection rate(pps). Jumlah Ivs yang di dapat berkisar 13074 ivs dan 120356 packet data di lanjutkan dengan proses cracking. Dibutuhkan waktu sekitar 5 menit untuk mendapatkan password dengan metode ini.
2. Kedua, *Fragmentation attack*, Pada proses ini dilakukan deauthentification pada client yang terkoneksi dengan jaringan tersebut. Menggunakan 1000 injection rate(pps). Jumlah Ivs yang di dapat berkisar 40908 ivs dan 121432 packet data di lanjutkan dengan proses cracking. Dibutuhkan waktu sekitar 4 menit untuk mendapatkan password dengan metode ini. Serangan ini terbilang sangat cepat di bandingkan serangan yang lain. Hanya membutuhkan 4 menit untuk mengumpulkan 40908 ivs.
3. Ketiga, *p0841 attack*, Menggunakan 1000 injection rate(pps) untuk mempercepat pengumpulan ivs. Jumlah Ivs yang di dapat berkisar 16431 ivs dan 16464 packet data di lanjutkan dengan proses cracking.

metode ini.

4. Keempat, *Packet injection atau ARP-Replay attack,* Jumlah Ivs yang di dapat berkisar 20876 ivs dan 5604632 packet data di lanjutkan dengan proses cracking. Dibutuhkan waktu sekitar 77 menit untuk mendapatkan password dengan metode ini. Waktu yang cukup lama di bandingkan serangan yang lain namun tetap menggunakan 1000 injection rate(pps) untuk mempercepat pengumpulan ivs dengan proses deauthentification.
5. Kelima, *Cafe-Latte attack,* Jumlah Ivs yang di dapat berkisar 20039 ivs dan 9756 packet data di lanjutkan dengan proses cracking. Dibutuhkan waktu sekitar 6 menit untuk mendapatkan password dengan metode ini. Sama seperti serangan yang lain menggunakan 1000 injection rate(pps) untuk mempercepat pengumpulan ivs.

Pengaturan setting keamanan pada Acess Point kurang maksimal menyebabkan beberapa serangan seperti Chopchop attack, Fragmentation attack, p0841 attack, Packet injection atau ARP-Replay attack, dan Cafe-Latte attack dapat berjalan dengan sempurna untuk mengambil kunci Wep pada Puri Ayu Homestay. Beberapa serangan di atas berjalan sempurna karena DDOS protection, Mac address filtering, firewall dan beberapa fungsi keamanan penting lainnya di matikan. Sehingga penyerang dapat menggunakan koneksi user lain untuk mempercepat terkumpulnya paket ivs. Selain itu dapat disimpulkan juga seranga seperti packet injection hanya bekerja dengan baik jika jaringan tersebut terkoneksi internet, karena jumlah paket data yang dikirimkan oleh klien akan lebih cepat dan besar melalui jaringan.

5.2. Saran

Dengan mengetahui beberapa serangan yang digunakan beserta cara mengatasinya diharapkan peneliti selanjutnya dapat mengurangi atau menghentikan dampak serangan pada WEP dengan metode serangan yang berbeda, juga menggunakan Hardware atau Akses Point yang berbeda. Karena beberapa serangan tersebut hanya dapat dilakukan dengan bantuan GrimWepa dan cara mengatasinya dengan setting Access point Tp-Link TI-WR543G.

1. Pertama, Menggunakan kunci WEP 64-bit. Diharapkan uji coba juga dilakukan terhadap 128-bit, 152-bit, atau pada securitu WPA/WPA2.
2. Kedua, Penanganan keamanan di atas hanya dapat dilakukan pada Access Point Tp-Link TI-WR543G, diharapkan pengamanan dapat diterapkan pada jenis Access Point atau Hardware yang berbeda. Karena setiap Access Point mempunyai seting keamanan yang berbeda antara satu dengan lainnya.
3. Ketiga, Penelitian ini hanya sebatas menggunakan serangan Chopchop attack, Fragmentation attack, p0841 attack, Packet injection atau ARP-Replay attack, Cafe-Latte attack dengan bantual tool GrimWepa. Tidak berlaku terhadap serangan yang lainnya.

Saran saran diatas bertujuan agar peneliti selanjutnya menggunakan hasil analisa ini sebagai dasar penelitian di kemudian hari, karena terdapat pengembangan serangan lain yang tidak dapat di tangani oleh beberapa solusi tersebut, seperti kemungkinan MAC spoofing dan IP spoofing pada DHCP server. Sejauh ini yang dapat lebih maksimal jika mengkombinasikan seluruh solusi.