ANALISA KEAMANAN METODE ENKRIPSI WIRED EQUIVALENT PRIVACY (WEP) PADA PERANGKAT WIRELESS ACSESS POINT

Imam Muslem R
Dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Almuslim

ABSTRAK

Keamanan jaringan wireless menjadi sebuah hal yang sangat penting mengingat paket data yang lalu-lalang di udara dapat dengan mudah diakses oleh pihak yang tidak sah. Berbeda dengan jaringan kabel yang hanya terhubung apabila terkoneksi via kabel, jaringan wireless mempunyai masalah yang sangat kompleks karena siapapun dapat terhubung kedalam jaringan dikarenakan media udara yang bersifat bebas. Dari permasalahan ini, timbul inisisatif daripada para pengembang untuk lebih fokus kepada metode pengamanan jaringan wireless. Metode WEP merupakan salah satu metode yang umum dan masih digunakan saat ini dalam mengamankan jaringan wireless. Dalam penelitian ini, dilakukan analisa dengan teknik penetrasi menggunakan tools yang sudah ada yang kompatibel dengan sistem operasi open source Linux Bactrack. Beberapa teknik dengan menggunakan tools tersebut adalah mencari informasi target jaringan wireless, mengumpulkan paket data yang ada dalam jaringan wireless, melakukan tahapan untuk membantu terjadinya paket data apabila poin kedua terlalu lama, melakukan tahapan untuk mendapatkan WEP Keys dan menggunakan WEP Keys agar terhubung kedalam jaringan yang menjadi target. Kesimpulan yang dapat diambil dari penelitian ini adalah bahwa standar keamanan WEP sudah tidak efektif dalam mengamankan sebuah jaringan wireless. Hal ini dikarenakan WEP Keys dapat dengan mudah didapatkan melalui teknik pengumpulan paket data yang dilakukan.

Kata Kunci: Analisa Keamanan, Metode Enkripsi Wired Equivalent Privacy (WEP) dan Perangkat Wireless Acsess Point.

PENDAHULUAN

Penggunaan wireless memberikan kenyamanan tersendiri dikarenakan wireless menggunakan udara sebagai media transmisi data. Instalasi yang fleksibel menjadikan jaringan wireless semakin populer dibandingkan dengan jaringan yang menggunakan media kabel sebagai media transmisi data. Namun, fleksibelitas ini ternyata menimbulkan permasalahan keamanan yang cukup serius. Hal ini dikarenakan penggunaan media udara yang bersifat free, sehingga siapa saja dapat terhubung kedalam jaringan dengan syarat perangkat penerima (receiver) berada dalam jangkauan yang dekat dengan perangkat pemancar (transmitter). Penelitian-penelitian dilakukan demi mengatasi permasalahan yang terjadi, salah satu nya adalah menyangkut dengan kemanan teknologi wireless.

Dalam bidang *information technology*, keamanan merupakan hal yang mutlak yang harus dipenuhi demi tersedianya data yang otentik. Hal ini dikarenakan perkembangan dunia yang semakin hari semakin menjurus ke arah *cyber world*. Semua sektor kehidupan manusia saat ini sudah menggunakan teknologi informasi, mulai dari sektor pertanian, industri, kesehatan, perdagangan dan lain sebagainya telah menggunakan teknologi informasi dalam menunjang keberhasilannya. Namun daripada itu, untuk membentuk sebuah dunia cyber yang aman diperlukan penelitian-penelitian yang diharapkan mampu menjaga keotentikan data yang ada. Para peneliti telah bekerja keras demi menemukan metode-metode baru yang lebih mumpuni untuk mengamankan sebuah data. Seperti penelitian yang dilakukan oleh tiga sekawan dari Massachusetts Institute of Technology (MIT) yaitu Ron Rivest, Adi Shamir dan Leonard Adleman. Algoritma yang dihasilkan yaitu RSA yang merupakan singkatan dari nama mereka (Rivest, Shamir, Adleman). Metode RSA ini

merupakan salah satu metode yang paling ampuh yang masih umum digunakan saat ini.

Metode enkripsi merupakan metode yang umum digunakan dalam bidang teknologi informasi untuk mengamankan sebuah data ataupun sistem. Metode yang lazim digunakan ini dapat dibagi menjadi beberapa bagian kecil berdasarkan kegunaannya dalam pengamanan yang dilakukan. Dalam penelitian ini tidak dibahas semua bagian dari metode enkripsi, tetapi hanya dibahas tentang enkripsi yang digunakan untuk pengamanan perangkat nirkabel (wireless).

Dalam penelitian ini, akan dilakukan analisa dan pengujian keamanan pada metode pengamanan dengan enkripsi WEP (Wired Equivalent Privacy). Seperti yang diketahui bahwa WEP adalah metode pengamanan perangkat wireless yang paling umum digunakan saat ini. Berbeda dengan proteksi WPA, metode proteksi WEP dinilai lebih lemah. Dalam penelitian ini, penulis akan membahas kelemahan yang terdapat pada metode proteksi WEP.

METODE PENELITIAN

Dalam penelitian ini, penulis akan melakukan penetrasi test dengan menggunakan sistem operasi Linux Backtrack. Penetrasi test yang dilakukan diharapkan dapat menemukan celah keamanan yang ada pada metode pengamanan WEP.

Adapun peralatan yang digunakan dalam penelitian ini yaitu:

a. Laptop Asus A555L
b. Mouse Wireless
c. Wireless acsess point
d. Smartphone Samsung Galaxy Wonder (digunakan sebagai perangkat Portable Hotspot)
e. Windows 8 (sebagai sistem operasi utama)
f. Linux Backtrack (sebagai sistem operasi kedua dengan menggunakan virtual machine)
g. Virtual Box (sebagai virtual machine)

HASIL DAN PEMBAHASAN

Untuk melakukan pen-test pada metode proteksi WEP, dibutuhkan peralatan yang memadai. Mulai dari perangkat wireless yang digunakan yaitu perangkat wireless yang mampu berjalan dalam modus monitor dan mempunyai kemampuan untuk menginjeksi paket kedalam jaringan.

Cracking WEP keys dilakukan dengan cara mengumpulkan data sebanyak-banyaknya daripada wireless network. Dalam hal ini, dipilih salah satu wireless network yang akan menjadi target. Jaringan wireless yang dipilih adalah jaringan wireless yang menggunakan WEP keys sebagai metode pengamanannya. Langkah-langkah yang dilakukan dalam penetration test ini adalah:

a. Cari informasi jaringan wireless yang akan dilakukan penetration test.
b. Kumpulkan paket data sebanyak-banyaknya.
c. Membantu terjadinya peningkatan paket data apabila point kedua berlangsung terlalu lama
d. Crack WEP Keys berdasarkan paket data yang terkumpul
e. Gunakan WEP Keys untuk melakukan koneksi ke jaringan wireless.

Pada dasarnya, proses cracking WEP Keys dilakukan dengan metode statistik, dimana makin banyak data yang didapat, maka semakin besar kemungkinan berhasilnya. Dengan metode ini, proses cracking dilakukan dengan menganalisa data yang dikumpulkan. Jumlah data yang dibutuhkan tidak diketahui secara pasti, akan tetapi proses ini membutuhkan data yang sangat besar. Pada tahun 2001, Metode untuk cracking WEP keys dengan banyaknya data yaitu sekitar 4.000.000 (64bit) s/d 6.000.000 (128bit) paket data. Kemudian pada tahun 2004, seorang hacker yang bernama KoRek menemukan cara yang lebih efisien yang membutuhkan data sekitar 250.000 (64bit) s/d 1.500.000 (128bit) paket data. Penelitian terakhir adalah yang ditemukan oleh Andreas Klein dimana besar data yang dibutuhkan hanya

sekitar 20.000 untuk enkripsi 64bit dan 40.000 untuk enkripsi 128 bit.

Cari informasi jaringan wireless yang akan dilakukan pen-test.

Tahap ini akan dilakukan pencarian informasi terhadap jaringan wireless yang akan di crack. Tools yang digunakan adalah kismet yang terdapat pada sistem operasi Linux Backtrack. Selain dengan kismet, juga bisa digunakan airocrack -ng. Tahap pertama yang dilakukan adalah memonitor jaringan wireless dengan menggunakan paket-paket program yang didapat dengan tools airocrack -ng.

Kumpulkan paket data sebanyak-banyaknya

Tahap ini dilakukan untuk mengumpulkan paket data yang ada di udara sebanyak-banyaknya. Semakin banyak paket data yang berhasil ditangkap, maka semakin cepat dan akurat pula proses cracking dilakukan. Dalam tahap ini digunakan sistem operasi linux backtrack dengan aplikasi airodump -ng sebagai tools yang bertindak dalam mengumpulkan paket. Paket yang didapat akan disimpan kedalam sebuah file berekstensi .cap dan .txt. Selama proses berjalan dapat diperhatikan proses pertambahan paket data yang didapat, tergantung daripada aktifitas yang terjadi dalam jaringan tersebut. Jika user yang ada menggunakan jaringan secara intensif, maka proses pertambahan paket data ini semakin banyak dan semakin cepat.

Membantu menciptakan paket data

Tentu akan sangat membosankan jika menunggu aktifitas yang sibuk pada sebuah jaringan. Seperti yang telah dibahas pada poin di atas, semakin sibuk aktifitas sebuah jaringan, maka semakin banyak paket data yang bisa ditangkap. Namun bagaimana jika jaringan yang menjadi target adalah jaringan yang tidak ada user yang aktif? Dalam poin ini akan dilakukan langkah yang membantu terciptanya paket data. Teknik yang bisa digunakan dalam tahap ini adalah dengan mengirimkan paket ARP. Paket ARP digunakan untuk mencari alamat fisik (MAC Address) dari sebuah user/komputer. Sebuah AP akan mengirimkan paket AP kedalam jaringan, sehingga akan terjadi aktifitas didalam jaringan tersebut. Permasalahan ini menjadi semakin sempurna karena masalah keamanan dalam metode WEP, karena metode ini memungkinkan serangan yang dinamakan sebagai "replay attack", yang berarti paket yang sah dapat dikirim berulang kali dan tetap dianggap sah. Maka dengan konsep ini, dapat dimanipulasi pengiriman ARP oleh user yang sah, lalu menyimpannya dan mengirimnya kembali secara berulang kali. Dengan metode ini, sebuah AP yang menjadi target tersebut secara otomatis akan mempunyai aktifitas yang sibuk, sehingga paket data yang ditangkap akan ikut meningkat secara drastis. Tahapan ini bisa dilakukan dengan menggunakan tools yang disertakan dalam sistem operasi linux backtrack yaitu aireplay-ng.

Crack WEP Keys berdasarkan paket data yang terkumpul

Dengan menjalankan tools aircrack-ng atau dengan metode PTW, maka dapat dilakukan percobaan mendapatkan WEP Keys dengan berbekal paket data yang didapat pada langkah sebelumnya.

Gunakan WEP Keys untuk melakukan koneksi kedalam jaringan wireless

Jika langkah diatas berhasil dilakukan, maka langkah terakhir yang dilakukan adalah melakukan koneksi kedalam jaringan wireless dengan menggunakan WEP Keys yang berhasil didapat.

PENUTUP

Simpulan

1. Metode pengamanan WEP dinilai sangat lemah dalam penerapannya sebagai metode pengamanan jaringan wireless.
2. Disarankan tidak menggunakan metode pengamanan WEP dalam implementasi jaringan wireless karena sangat rentan terhadap serangan.
3. Gunakan metode pengamanan yang lebih efektif daripada WEP, seperti metode WPA.

Saran

1. Buat penelitian tentang pengembangan metode pengamanan WEP, sehingga metode serangan yang mungkin terjadi yang telah dibahas dapat diatasi.
2. Buat penelitian tentang analisa keamanan pada metode WPA, sehingga administrator jaringan wireless bisa menentukan metode pengamanan terbaik yang dapat digunakan.

DAFTAR PUSTAKA

http://chemickedogawa.blogspot.co.id/2012/07/sejarah-kriptografi-rsa.html

https://id.wikipedia.org/wiki/Wired_Equivalent_Privacy

http://www.aircrack-ng.org/doku.php?id=aircrack-ng

S'to. 2007. Wireless Kung Fu, Networking & Hacking. Jasakom: Jakarta.

S'to. 2005. Seni Teknik Hacking II. Jasakom: Jakarta.