Analisa Keamanan Jaringan *Wireless* Menggunakan Metode *Wardriving* Pada Kampus STMIK MIC Cikarang

Wireless Network Security Analysis Using Wardriving Method at STMIK MIC Cikarang Campus

Saloko Cahyo Saputro*, Tri Hargi Saputro, Bei Harira Irawan
Kampus STMIK MIC Cikarang, Kabupaten Bekasi
Corresponding author: crunch24.cc@gmail.com*, egysaputro@gmail.com, beiharira@gmail.com

Riwayat Artikel: Dikirim; Diterima; Diterbitkan

Abstrak

Penggunaan enkripsi untuk pengamanan pada sebuah jaringan *wireless* mutlak diperlukan mengingat pada jaringan *wireless* yang terbuka siapa saja dapat mengakses. Kelemahan konfigurasi IP *address* (Alamat *Internet Protocol*) dalam kampus dapat mengakibatkan siapa saja (*user*) untuk dapat mengakses jaringan. Enkripsi dari WEP (*Wired Equivalent Privacy*) yang di setting pada kampus memiliki berbagai macam kelemahan yang bisa dieksploitasi oleh peretas (*hacker*) seperti monitoring lalu lintas jaringan, akses ilegal *username* dan *password* serta berbagai bentuk akses illegal lainnya. Teknik yang digunakan untuk memetakan *access point* untuk tujuan statistik adalah teknik *Wardriving* menggunakan beberapa *tools* yang dijalanan dari Sistem Operasi Linux. Dari hasil *mapping* di wilayah sekitar kampus didapatkan 11 jaringan wifi yang terdeteksi dengan pengamanan beragam diantaranya *None Enkripsi*, WEP, dan WPA2. Untuk koneksi wifi di kampus sendiri didapatkan 3 jaringan wifi tidak terenkripsi dan 1 jaringan wifi terenkripsi WEP.

Kata kunci: enkripsi, *wardriving*, WEP, WPA, jaringan *wireless*.

Abstract

The use of encryption for security on a wireless network is absolutely necessary considering that in an open wireless network anyone can access. Weaknesses in the configuration of IP addresses (Internet Protocol Address) on campus can cause anyone (user) to be able to access the network. Encryption from WEP (Wired Equivalent Privacy) which is set on campus has a variety of weaknesses that can be exploited by hackers (hackers) such as monitoring network traffic, illegal access to usernames and passwords as well as various other forms of illegal access. The technique used to map access points for statistical purposes is the Wardriving technique using several tools that are run on the Linux operating system. From the mapping results in the area around the campus, 11 wifi networks were detected with various security including None Encryption, WEP, and WPA2. For wifi connections on campus, there are 3 unencrypted wifi networks and 1 WEP encrypted wifi network

Keywords*: encryption, wardriving, WEP, WPA, wireless networks.*

PENDAHULUAN

Kampus STMIK MIC Cikarang adalah Kampus Swasta yang menyelenggarakan pendidikan Strata Satu (S1) dengan jurusan Teknik Informatika dan Sistem Informasi. Jumlah pengakses data internet pada Kampus STMIK MIC Cikarang sebanyak kurang lebih 50-80 *peripheral* (komputer, laptop dan handphone) setiap harinya. Internet kampus menggunakan 2 provider internet yaitu Maxindo dan Indiehome, dengan *bandwidth* yang dialokasikan sebanyak 5 Megabytes dari Maxindo dan 20 Megabytes dari Indiehome. Perkiraan jumlah *bandwidth* rata-rata sebesar 50 Kilobytes, jika seluruh komputer, laptop dan *handphone* digunakan untuk mengakses internet maka akan terjadi kepadatan akses internet.

Di kampus terdapat data yang di share khusus untuk staff dan sebuah sistem informasi

pembayaran kuliah mahasiswa. Selama ini pengguna internet di kampus terutama staff begitu lemah dalam masalah keamanan komunikasi data pada jaringan mengingat seluruh mahasiswa juga melakukan akses internet bersamaan dengan menggunakan jaringan *wireless* di kampus. Celah keamanan konfigurasi IP *address* (Alamat *Internet Protocol*) dalam kampus dapat mengakibatkan siapa saja dapat mengakses jaringan kampus selama berada dalam. lingkungan kampus. Hal ini membuat *router* bekerja untuk mencoba mengenali apakah *peripheral* tersebut sudah pernah mendapatkan alamat IP sebelumnya atau belum. *Router* juga menyiapkan IP *address* bagi setiap *peripheral* baru yang terdeteksi. Hal ini dapat menyebabkan *router* bekerja terlalu ekstra sehingga akses internet bagi seluruh user (staff dan mahasiswa) dapat terganggu.

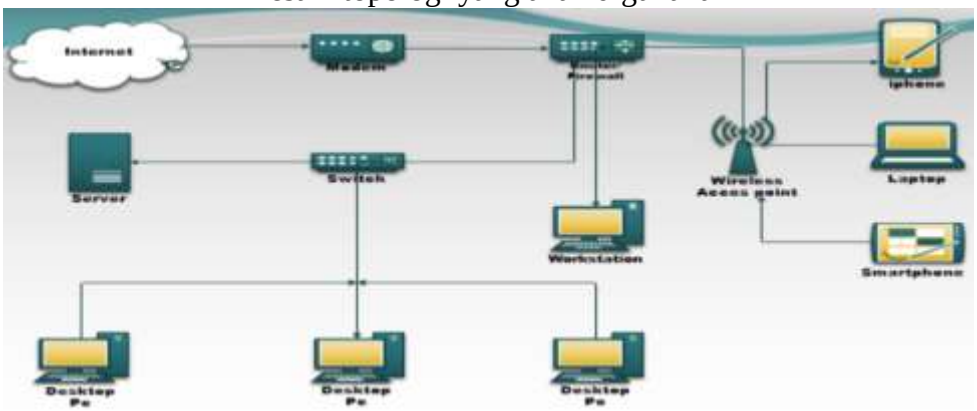
Enkripsi dari WEP (*Wired Equivalent Privacy*) yang di setting pada kampus memiliki berbagai macam kelemahan yang bisa dieksploitasi oleh peretas (*hacker*), sehingga memungkinkan untuk ditemukan celah dalam hitungan menit. Terdapat permasalahan yang berhasil ditemukan pada jaringan LAN dan WLAN (*Wireless Local Area Network*) seperti monitoring lalu lintas jaringan, pencurian *username* dan *password* serta berbagai bentuk akses illegal. Dari masalah diatas maka perlu adanya sebuah percobaan analisa keamanan pada jaringan kampus dengan tujuan agar dapat diimplementasikan sebagai perluasan dari wired LAN utama, untuk menangani user yang menggunakan perangkat *wireless*. Teknik yang digunakan pada penelitian ini adalah metode *Wardriving*, untuk memetakan access point dengan tujuan statistik

METODE

Pengaturan *traffic* dari penggunaan internet merupakan salah satu faktor yang mendukung kelancaran aktivitas penggunaan internet. Oleh karenanya, di STMIK MIC Cikarang menggunakan alat Antena Alfa tipe AWUS026NH yang berfungsi untuk memantau *traffic* internet pada kampus tersebut. Dengan adanya perangkat alat ini, dapat digunakan untuk memantau *traffic* serta memantau pemanfaatan *resource* komputer yang digunakan.

Penelitian ini menggunakan variabel tunggal yaitu analisis arsitektur sistem jaringan *wireless*. Metode analisis menggunakan *Top Down Approach* dan menggunakan model LAN *Technologies Choices*. Berkaitan dengan analisis data, melalui *Top Down Network Design* maka data-data yang didapat akan dibuat menjadi desain topologi jaringan interkoneksi yang akan dibangun. Berikut perancangan topologi yang akan dibangun.

Gambar 1:
Desain topologi yang akan digunakan



Sumber: Dokumentasi Pribadi

Dari hasil analisis lapangan, jumlah komputer yang terhubung dalam jaringan LAN dan Wireles LAN di kampus adalah sebagai berikut:

1) Komputer Kantor/Staff berjumlah 8 PC
2) Komputer di Lab. Komputer kurang lebih 50 PC (meskipun tidak setiap hari terkoneksi, tergantung pemakaian kelas Lab. Komputer)
3) Laptop Mahasiswa dan Dosen yang setiap hari terkoneksi kurang lebih 30-40 Devices
4) Perangkat telepon selular Mahasiswa dan Dosen yang setiap hari terkoneksi kurang lebih 30-50 Devices

Untuk analisa Perangkat Lunak yang akan digunakan pada penelitian ini sebagai berikut:

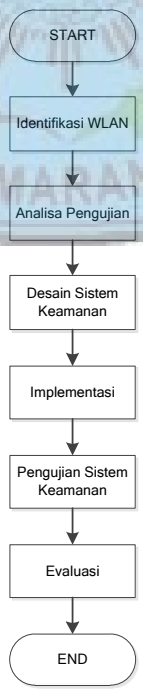
1) OS (*Operation System*) Windows Server 2008 R2
2) OS (*Operation System*) Linux Cyborg
3) OS (*Operation System*) Linux Blackbuntu
4) Etherape
5) Kismet
6) Nmap
7) Metasploit

Untuk analisa Perangkat Keras yang akan digunakan pada penelitian ini sebagai berikut:

1) 3 (tiga) buah PC (digunakan sebagai *server, client, penetration*)
2) 1 (satu) *Wireless Router* TPLINK MR3420
3) 1 (dua) buah WLAN Card Antena Alfa AWUS036NH

Adapun fase penelitian yang peneliti lakukan ditunjukkan dengan *flowchart* berikut:

Gambar 2:
Flowchart fase penelitian



HASIL DAN PEMBAHASAN

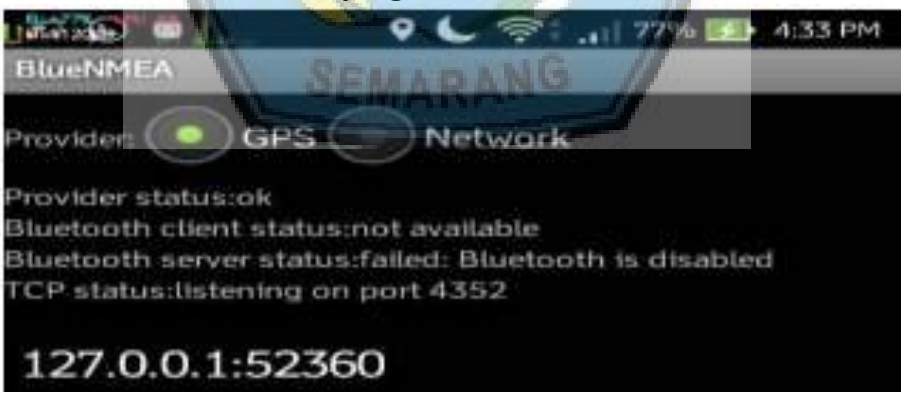
Pada tahap awal identifikasi WLAN penulis menggunakan teknik *Wardriving* dengan menggunaan alat yang telah persiapkan dan dirakit dalam ruangan menggunakan *wireless dongle* pada port USB laptop, begitu pula smartphone android menggunakan kabel data untuk memberi informasi GPS (*Global Positioning System*) pada proses *wardriving*. Langkah berikutnya dalam mengidentifikasi WLAN adalah sebagai berikut:

1) Menjalankan Adb (*android debug bridge*) *devices* untuk membaca *devices* pada android yang sudah terhubung dengan komputer dan mengkoneksikanya.

Gambar 3:
Adb yang sudah terkoneksi

2) Menjalankan BlueNmea pada Android. Untuk mengetahui android terkoneksi dengan GPS (*Global Positioning System*) di BlueNmea *provider* status OK dan muncul IP (*Internet Protocol*) berarti sudah terkoneksi ke GPS (*Global Positioning System*).

Gambar 4:
BlueNmea yang sudah terkoneksi GPS



3) Menjalankan aplikasi Kismet untuk mendeteksi dan melihat semua jaringan nirkabel yang terbuka serta *wireless network* yang tidak menggunakan SSID. Dan untuk paket–paket data yang keluar masuk di sekitar kita, selain itu juga untuk melihat *hostpot* di sekitar.

Gambar 5:
Mapping Aplikasi Kismet

4) Hasil *wardriving* dalam file *log* Kismet akan dikonversi oleh Giskismet menjadi sebuah *database* berisikan Wifi (*Wireless Fidelity*).
5) Selanjutnya adalah membuat file berekstension kml (*Keyhole Markup Language*). Setelah file kismet *wardriving.kml* berhasil dibuat dilakukan pemetaan dengan membuka file kismet pada *Google Earth*.

Gambar 6:
Pemetaan file Kismet pada *Google Earth*

Dari hasil pemetaan didapat bahwa di wilayah kampus STMIK MIC Cikarang ditemukan Wifi (*Wireless Fidelity*) berjumlah 11 buah dengan enkripsi yang terdeteksi pada hasil *Wardriving* beragam seperti *None Encription*, WEP, dan WPA2. Berikut rincian *mapping* hasil *Wardriving*:

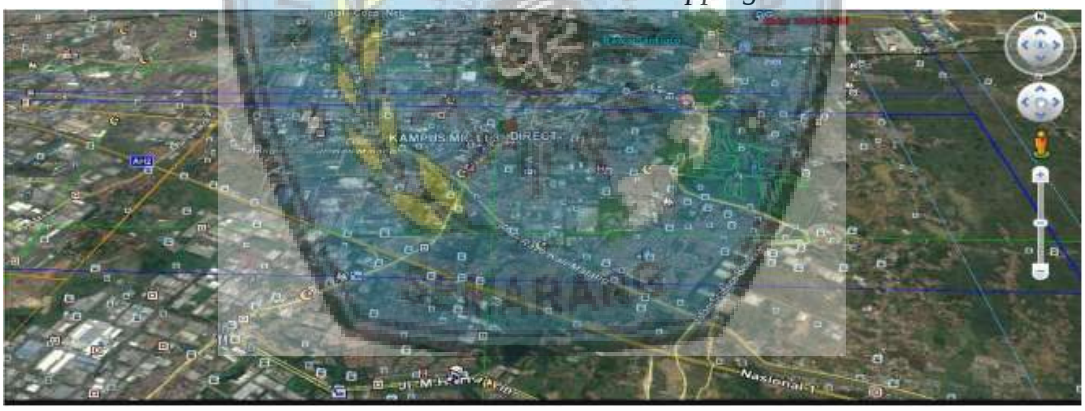
1) Peta *Open Wireless* di STMIK MIC Cikarang.

Gambar 7:
Peta *Open Wireless* hasil *mapping*

Di kampus STMIK MIC Cikarang terdapat Wifi (*Wireless Fidelity*) yang tidak menggunakan enkripsi sebanyak 3 buah yaitu KAMPUS MIC LT 2, KAMPUS MIC 2 Class, KAMPUS MIC LT 3. Artinya pengamanan jaringan *access point* yang dimiliki kampus STMIK MIC belum sepenuhnya diamankan dengan enkripsi yang lebih aman.

2) Peta *WEP Wireless* di STMIK MIC Cikarang.

Gambar 8:
Peta *WEP Wireless* hasil *mapping*



Jenis enkripsi WEP (*Wired Equivalent Privacy*) yang digunakan pada jaringan nirkabel di kampus STMIK MIC Cikarang berdasarkan hasil penelitian yang diperoleh dari proses *wardriving* hanya 1 (satu) saja yang terenkripsi yaitu dengan nama KAMPUS MIC LT 3.

KESIMPULAN

Dari hasil pemetaan dengan teknik *Wardriving*, terdapat permasalahan yang berhasil ditemukan pada jaringan *wireless* LAN (*Local Area Network*) Kampus STMIK MIC antara lain:

1) Masih terdapat jaringan Wifi yang masih tanpa enkripsi, hal ini akan berdampak ditemukannya celah yang dapat disusupi peretas seperti monitoring lalu lintas jaringan, pencurian *username* dan *password* serta akses ilegal.
2) Dari hasil pengujian menunjukan bahwa sistem keamanan yang menggunakan *Hidden*

e-ISSN : 2654-3168
p-ISSN : 2654-3257

SSID mampu terlihat dengan menggunakan metode *passive scanning* yang digunakan oleh *tools* Kismet.

3) Teknik *MAC Filtering* pun bisa dikelabui dengan mudah, karena MAC addres dapat diubah secara virtual menggunakan *tools* K-MAC.
4) Enkripsi dari WEP (*Wired Equivalent Privacy*) memiliki berbagai macam kelemahan yang bisa dieksploitasi oleh peretas (*hacker*), sehingga memungkinkan untuk disusupi hanya dalam hitungan menit.
5) WPA/WPA2 memiliki enkripsi yang cukup kuat, namum apabila menggunakan *password* yang lemah masih memungkinkan untuk dilakukan proses *cracking password* menggunakan *dictionary attack*.
6) Disarankan adanya pemasangan komputer server berbasis Windows Server atau Mikrotik OS sebelum saluran jaringan disebar kepada *client* yaitu yang dituju oleh *access point* yang akan memberi otentikasi kepada *client*.
7) Perlu adanya perangkat lunak yang dapat membantu filtering *IP Address*, yang biasa digunakan antara lain freeRADIUS, openRADIUS dan lain-lain.

DAFTAR PUSTAKA

Arinanto, Kurniawan Dwi, 2002. Wardriving Serangan Terhadap Wireless LAN, Program Magister Teknik Elektro, ITB, Bandung.

Kuntoro Priyambodo Tri, Heriadi Dodi, 2005.Jaringan Wi-fi, Yogyakarta: Penerbit Andi.

Mulyana, Eueung; Purbo, Onno W., 2000. Firewall: Sekuriti Internet, Computer Network Research Group, ITB, Bandung.

Neuman, Clifford B, 1993. Proxy-Based Authorization and Accounting for Distributed Systems, Proceedings of the 13th International Conference on Distributed Computing Systems, Pittsburgh.

Purbo, Onno W, 2005. Buku pegangan internet wireless dan hotspot, Jakarta: PT. Elek Media Komputindo.

Rahardjo, Budi, 2002. Kemanan Sistem Informasi Berbasis Internet, Jakarta: PT. Insan Indonesia.

Reza, Muhammad, 2003. *15 Jenis Serangan Cracker (Online)*, (www.ilmukomputer.com, diakses Maret 2017).

Taufan Riza, 2001. Manajemen Jaringan TCP/IP. Jakarta: PT. Elek Media Komputindo.