**EVALUASI KEAMANAN JARINGAN KOMPUTER**

**KANTOR SKRETARIAT DPRD**

**KOTA PALEMBANG**

Yusron Nagalio 1, Irwansyah, M.M., M.Kom.2, Timur Dali Purwanto, M.Kom.3

1)Mahasiswa Informatika Universitas Bina Darma

2)Dosen Ilmu Komputer 3)Dosen Ilmu Komputer. Jalan Jend A. Yani No.12 Plaju, Palembang 30264

*Email* : lio2889@gmail.com 1), irwansyah@mail.binadarma.ac.id 2),

timoerok@gmail.com 3)

**Abstrak :** Seiring dengan kemajuan ilmu teknologi saat ini, perkembangan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini terus meningkat dari jaringan menggunakan kabel *LAN* sampai dengan *wireless*. Kantor Sekretariat DPRD Kota Palembang menggunakan kedua jenis jaringan tersebut dalam pelaksanaan kegiatan komunikasi data. Namun dengan sistem keamanan yang terbuka membuat informasi data yang tersedia menjadi tidak aman dan mendapatkan ancaman dari pihak yang tidak diinginkan. Maka dari itu dibutuhkan suatu evaluasi sistem keamanan jaringan komputer pada kantor Sekretariat DPRD Kota Palembang untuk menutup celah keamanan yang terbuka, kemudian memberikan langkah pencegahan untuk meningkatkan sistem *security* guna melindungi informasi data yang ada.

1. **Pendahuluan**

**1.1 Latar Belakang**

Kantor Sekretariat DPRD Kota Palembang merupakan salah satu instansi pemerintah yang menggunakan jaringan komputer dalam pelaksanaan kegiatan untuk saling terkoneksi dengan instansi pemerintah yang lainnya dalam satu jaringan terdistribusi, memiliki sistem keamanan yang belum terlalu kuat sehingga hal ini dapat menyebabkan gangguan dari pihak luar yang ingin menyalahgunakan sistem informasi yang ada pada Kantor Sekretariat DPRD Kota Palembang.

Dalam pelaksanaan kegiatan kerja yang terdapat pada Kantor Sekretariat DPRD Kota Palembang, jaringan komputer seperti *LAN* dan *Wireless* sangat mempermudah dalam menyelesaikan pekerjaan, dengan adanya jaringan komputer para pegawai Kantor Sekretariat DPRD Kota Palembang dapat berbagi informasi satu sama lain tanpa harus bertatap muka secara langsung melalui media jaringan komputer tersebut.

Setelah mengamati secara langsung dan melihat kondisi mengenai sistem keamanan jaringan komputer yang ada pada Kantor Sekretariat DPRD Kota Palembang, terdapat beberapa permasalahan yang ada mengenai sistem keamanan jaringan pada Kantor Sekretariat DPRD Kota Palembang.

Nantinya penulis akan mengevaluasi permasalahan yang ditemukan berdasarkan aspek *Privacy*, *Integrity*, *Authentication*, dan *Acces Control* yang dilanjutkan dengan rancangan pengujian penetrasi sistem keamanan jaringan dan rancangan desain sistem yang akan digunakan.

Dalam kegiatan evaluasi keamanan jaringan komputer pada Kantor Sekretariat DPRD Kota Palembang nantinya penulis akan menggunakan dua perangkat lunak atau software sebagai alat dalam pengujian sistem keamanan jaringan, yaitu Kali Linux dan K-Mac.

Adapun batasan permasalahan dalam penelitian ini adalah mengevaluasi keamanan jaringan komputer Kantor Sekretariat DPRD Kota Palembang berdasarkan aspek *Privacy*, *Integrity*, *Authentication* dan *Acces Control.*

1. Metode dan Perancangan
	1. **Metode**

Metode penelitian yang digunkan dalam penelitian ini adalah metode pengumpulan data selain metode penilitian terdapat juga metode testing yang dilakukan yaitu dengan menggunakan metode *Penetration Test*.

**3.2 Perancangan**

****

Gambar 1 Rancangan Pengujian Penetrasi

Dari gambar diatas dapat dijelaskan bahwa, untuk memulai tahap pengujian penetrasi jaringan *wi-fi* kita harus mengetahui bahwa terdapat sebuah ancaman yang terjadi yaitu ancaman yang disebut dengan *man-in-the-middle-attack* yang mana ketika seorang *Hacker* memasang jebakkan di dalam jaringan *Wireless* dengan cara menggunakan suatu perangkat fiktif berupa *Software* tertentu untuk menjebak komputer *Client* dimana komputer *Hacker* berpura-pura menjadi *Wireless* yang dapat diakses oleh komputer *Client* tanpa disadari oleh komputer *Client*.

Ketika komputer *Client* melakukan komunikasi dengan *Wireless* maka komputer *Hacker* akan menangkap sinyal yang bersumber dari komputer *Client* tersebut kemudian *Hacker* akan mengambil informasi yang ada pada komputer *Client* seperti *Password*, dan data-data penting lainnya atau tidak cukup dengan mengambil *Hacker* juga bisa merubah atau menghapus data-data penting tersebut sesuai keinginannya.

1. Hasil dan Pembahasan
	1. **Hasil**

Hasil evaluasi berdasarkan aspek *Privacy, Integrity, Authentication,* dan *Acces Control*, yaitu sebagai berikut :

1. *Privacy*

Sistem keamanan jaringan yang masih terbuka membuat informasi data yang ada pada jaringan Kantor Sekretariat DPRD Kota Palembang menjadi tidak aman.

1. *Integrity*

Dikarenakan sistem keamanan yang lemah itu juga dapat menyebabkan informasi data yang ada bisa saja diambil, dirubah bahkan dirusak oleh hacker atau oleh orang yang tidak berhak tanpa seijin pemilik informasi.

1. *Authentication*

Sistem keamanan WPA/WPA 2 yang digunakan dirasa belum cukup aman untuk memproteksi informasi data yang ada pada jaringan wireless.

1. *Acces Control*

Penyebaran virus yang diakibatkan tidak terpasangnya atau tidak terupdatenya antivirus pada komputer pegawai Kantor Sekretariat DPRD Kota Palembang dapat menimbulkan permasalahan akan rusaknya informasi data yang ada, kemudian tidak adanya server khusus seperti server proxy atau server lainnya untuk memanajemen *user* menyebabkan *user* menjadi tidak terkontrol dan terkoordinasi dengan baik.

* 1. **Pembahasan**
		1. **Uji Penetrasi Menggunakan Tools *Aircrack-ng* Pada Kali Linux**

Untuk proses uji penetrasi menggunakan tools *aircrack-ng* ini langkah-langkah yang penulis lakukan adalah sebagai berikut :

1. Instal sistem operasi Kali Linux kedalam laptop yang akan digunakan untuk melakukan kegiatan penetrasi. Ketika muncul tampilan login maka masukkan *username* *“root”* kemudian *Password ”toor”*.
2. Cek ketersediaan perangkat keras jaringan yang ada dilaptop, dengan mengetikkan perintah **root@kali:~# airmon-ng**



Gambar 2 Informasi Perangkat Adapter yang digunakan.

1. Ketikkan perintah **root@kali:~# airmon-ng start wlan0,** berfungsi untuk membuat perangkat adapter berfungsi kedalam modus monitor.



Gambar 3 Informasi Adapter Dalam Modus Monitor.

1. Ketikkan perintah **root@kali:~# airodump-ng wlan0** untuk memulai proses pencarian informasi mengenai ketersediaan jaringan *wireless* yang nantinya akan dilakukan uji penetrasi terhadap jaringan *wireless* tersebut.



Gambar 4 Proses Pencarian Informasi Mengenai Jaringan *Wireless*.

1. *Mac Address wireless* yang dituju yaitu 88:DC:96:24:A9:5B dengan nama perangkat *wireless* yaitu “RUANG SEKRETARIAT”.
2. Copy BSSID atau *Mac Address wireless* tersebut kemudian ketikkan perintah **root@kali:~# airodump-ng –c 11 –bssid 88:DC:96:24:A9:5B –w /root/Desktop/ mon0**, perintah ini berfungsi untuk memonitor *user* mana saja yang terhubung ke jaringan *wireless* tersebut.



Gambar 5 Proses Monitoring Informasi *User* yang Terhubung ke *Wireless*.

1. Dengan melihat Gambar 4.5 diatas, informasi *user* yang akan diserang bisa didapatkan dari *Mac* *Address* yang tertera pada kolom STATION yaitu 00:1C:7B:A5:B2:8E.
2. Setelah *user* yang akan diserang didapatkan, maka dilanjutkan dengan cara mengetikkan perintah **root@kali:~# *aircrack-ng* –a2 –b 88:DC:96:24:A9:5B –w /root/wpa.txt /root/Desktop/\*.cap** perintah ini digunakan untuk mencari *password* yang kemudian dipakai untuk bisa terhubung kejaringan *wireless*.



Gambar 6 *Password* Didapatkan Kegiatan *Hacking* *Wireless* Berhasil.

* + 1. **Uji Penetrasi Menggunakan Aplikasi K-Mac**
1. Pastikan terlebih dahulu perangkat jaringan *wireless* yang ada pada laptop sudah aktif.
2. Kemudian jalankan aplikasi *K-Mac*



Gambar 7 Tampilan Awal Aplikasi *K-Mac*

1. Kemudian pilih perangkat *wireless* card sesuai yang terpasang dilaptop



1. Pada menu New Mac masukkan mac address komputer target yang telah dicatat.
2. Pilih apply kemudian konfirmasi untuk restart *wireless* tekan Yes.



Gambar 8 Konfirmasi Perubahan Mac Address.

1. Setelah laptop direstart maka secara otomatis mac address pada laptop berubah menjadi mac address komputer target.
2. Maka langkah terakhir koneksikan laptop yang sudah menggunakan mac address target ke jaringan *wireless*.
3. Kesimpulan

**5.1 Kesimpulan**

Dari hasil penelitian dan kemudian dievaluasi berdasarkan aspek *Privacy, Integrity, Authentication* dan *Acces Control* yang telah penulis lakukan terhadap jaringan komputer Kantor Sekretariat DPRD Kota Palembang, maka penulis dapat menyimpulkan bahwa :

1. Aspek *Privacy*

Sistem keamanan jaringan pada Kantor Sekretariat DPRD Kota Palembang masih bersifat terbuka dalam pengertian siapa saja bisa mengakses kedalam jaringan komputer tanpa ada dinding pemisah antar *user* satu sama lain yang mengakibatkan informasi data menjadi bebas untuk diakses siapa saja.Jaringan *wireless* pada Kantor Sekretariat DPRD Kota Palembang menggunakan sistem keamanan WPA2.

1. Aspek *Integrity*

Dengan terbukanya sistem keamanan jaringan komputer pada Kantor Sekretariat DPRD Kota Palembang selain menyebabkan informasi data yang bisa diakses siapa saja, informasi data juga bisa dirubah bahkan dirusak oleh orang yang tidak diinginkan seperti hacker atau yang lainnya.

1. Aspek *Authentication*

Sistem keamanan *WiFi* yang menggunakan teknik keamanan WPA/WPA 2 belum dirasa aman karena masih menggunakan keyword yang terdiri dari huruf tanpa ada kombinasi dengan angka dan juga karakter. Teknik keamanan menggunakan Mac Address juga belum bisa dikatakan baik karena masih bisa ditembus menggunakan software aplikasi seperti K-Mac.

1. Aspek *Acces Control*

Untuk membatasi akses *user* kedalam jaringan komputer maka diperlukan adanya server khusus yang berfungsi mengatur *user* baik dari segi jumlah, kuota bandwidth yang akan dipakai *user*, membatasi akses web tertentu dan lainnua. Tidak terpasangnya atau tidak terupdatenya antivirus pada komputer *user* dalam hal ini para pegawai menyebabkan adanya kemungkinan untuk terserang virus, malware ataupun spyware.

Referensi

1. Sukmaaji, Anjik & Rianto. (2008). *Jaringan Komputer*. Yogyakarta : Andi Yogyakarta.
2. Priyo, Eko Utomo. (2012). *Wireless Networking.* Yogyakarta : Andi Yogyakarta.
3. Sofana, Iwan. (2009). *Cisco CCNA & Jaringan Komputer*. Bandung : Informatika.
4. Sofana, Iwan. (2008). *Membangun Jaringan Komputer*. Bandung : Informatika.
5. S’to. (2013), *Backtrack 5R3 100% Attack.* Jakarta : Jasakom.
6. Rajab, Muis. (2010). *Analisa dan Perancangan Wireless LAN Security Menggunakan WPA2-Radius*. Skripsi, Universitas Islam Negeri Syarif Hidayatullah Jakarta.
7. Jauhari, Fuad & M Iwan Wahyuddin. (2008). *Keamanan Jaringan Komputer Pada Sistem Pemerintahan Elektronik*. Jurnal Artificial, *ICT Research Center* UNAS, Universitas Nasional.
8. Wirdasari, Dian. (2008). *Mengenal Teknik-Teknik Keamanan Komputer dan Model-Model Serangannya (Security Attack Models)*. Jurnal SAINTIKOM, STMIK Triguna Darma.