Analisis Sistem Keamanan Jaringan Hotspot Pada PD Sukses Mobilindo Palembang

Zugerial 1, Linda Atika,2Helda Yudiastuti.

1) Mahasiswa Informatika Universitas Bina Darma

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

*Email*:zugerialcr7@gmail.com

**Abstrak.** Saat ini teknologi jaringan *(Network)* sudah berkembang dengan pesat. *Area network* yang selama ini dihubungkan dengan menggunakan kabel terasa menghambat kinerja pada suatu jaringan. Maka untuk itu dikembangkanlah teknologi nirkabel area network, yaitu *Wirelees Local Area Network* (*W-LAN).* *Hotspot (wi-fi)* merupakan salah satu *area* dimana suatu koneksi internet dapat berlangsung tanpa kabel. Jaringan *wi-fi (Wireless Fidelity)* menjadi teknologi alternatif dan relatif lebih mudah untuk diimplementasikan di lingkungan kerja. Hotspot *(wi-fi)* juga merupakan salah satu bentuk pemanfaatan teknologi pada lokasi-lokasi publik seperti taman, perpustakaan, restoran, kampus, beberapa diantaranya bahkan dapat diakses secara cuma-cuma atau gratis. Internet terkoneksi biasanya dilakukan melalui perangkat Notebook/Leptop/PDA. *Hotspot* *(wi-fi)* pertama kali digagas tahun 1993 oleh Breet Stewart. Dengan teknologi ini, individu dapat mengakses jaringan seperti internet melalui komputer atau laptop yang mereka miliki dilokasi-lokasi dimana *Hotspot* *(wi-fi)* disediakan. Saat ini hotspot di PD. Sukses Mobiindo Palembang menggunakan WP2-PSK sebagai *security* *hotspot*nya dengan begitu keamanan jaringan *hotspot* di PD. Sukses Mobilindo Palemmbang tidak mudah diakses oleh pihak luar (*hecker*) agar sistem keamanan *hotspot* di PD. Sukses Mobilindo Palembang berjalan dengan baik dan aman.

Kata kunci : *Hotspot / Wi-Fi*, WPA2-PSK, Keamanan jaringan.

1. **Pendahuluan**

**1.1 Latar Belakang**

Saat ini teknologi jaringan *(Network)* sudah berkembang dengan pesat seperti pelayanan yang dapat dilakukan melalui *online* dengan tanpa keterbatasan waktu dengan melalui jaringan internet yang dapat diakses kapan saja dan dimana saja. Saat ini jaringan internet telah menjadi suatu kebutuhan baik masyarakat umum atau pun pemerintah. *Area network* yang selama ini dihubungkan dengan menggunakan kabel terasa menghambat kinerja pada suatu jaringan.Maka untuk itu dikembangkanlah teknologi *nirkabel area network*, yaitu *Wirelees Local Area Network* (*W-LAN).*

Kelemahan jaringan *wireless* terletak pada kelemahan pada konfigurasi dan jenis enkripsi yang digunakan. Dengan kemudahan dalam mengkonfigurasi sebuah jaringan *wireless,* tambah dengan banyaknya *vendor* yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan *wireless* yang masih menggunakan konfigurasi wireless default bawaan vendor seperti SSID, *IP* *Address* , *remote manajemen*, *DHCP enable*, *kanal frekuensi*, tanpa enkripsi bahkan *user/password* untuk administrasi *wireless* tersebut.

Kinerja jaringan *wireless LAN* sangat ditentukan oleh ketersediaan *bandwidth.* Semakin banyak *user* di dalam suatu jaringan *WiFi* maka kecepatan akses akan semakin kecil karena *bandwidth* yang tersedia akan dibagi dengan seluruh pemakai jaringan tersebut. Sehingga akan sangat berpengaruh pada kinerja jaringan *wireless.* Walaupun demikian *WiFi*

masih mengandung beberapa kelemahan terutama dalam keamanan jaringannya. Sehinggga menjadi suatu hal yang sangat penting untuk menerapkan sistem keamanan jaringan *Wifi*.

PD Sukses Mobilindo Palembang merupakan salah satu perusahaan penjualan dan pembelian mobil *second* yang sudah menggunakan jaringan *wireless* dengan *internet service provider (ISP)* berupa *speedy* dengan kapasitas *bandwith* 10 MB, dan di sana sudah menggunakan jaringan *internet speedy* serta besar *bandwith* nya bertujauan untuk memudahkan karyawannya atau pegawainya mengakses internet dan mencari informasi berita tentang penjualan dan pembelian mobil *second*.

Oleh karena itu, untuk menjawab permasalahan keamanan jaringan hotspot atau *Wifi* penulis tertatrik untuk meneliti keamanan jaringan *wirelees* PD Sukses Mobilindo Palembang. Sehingga dapat mengetahui titik kelemahan jaringan *wirelees* tersebut dan dapat meminimalisir serangan dari pihak luar untuk mengakses jaringan *wireless* tersebut.

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

Penelitian ini merupakan *Action Research,* yang bertujuan mengembangkan metode kerja yang paling efisien.Penelitian tindakan yang yang mendeskripsikan menginterpretasikan dan menjelaskan suatu situasi atau pada waktu bersamaan dengan melakukan perubahan dan intervensi dengan tujuan perbaikan (Guritno, Sudaryono, Raharja, 2011:46).Adapun tahapan-tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu.

1. *Diangnosing* dengan melakukan diagnosa terhadap sistem keamanan pada jaringan wireless di PD Sukses Mobilindo Palembang.
2. *Action Planning* dengan memahami pokok masalah yang ada kemudian akan dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.
3. *Action tacking* mengimflementasikan rencana tindakan yang telah dibuat dengan harapan dapat menyelasikan masalah yang ada.
4. *Evaluating* melakukan evaluasi hasil dari hasil penetrasi tadi yang menemukan celah keamanan sistem autentikasi *wireless*, dalam tahap ini yang dilihat adalah apakah sistem keamanan jaringan *wireless* di PD Sukses Mobilindo Palembang berjalan dengan baik dan aman.
5. *Learning* melakukan pengulangan terhadap tahapan-tahapan yang telah berakhir dan mempelajari kriteria celah keamanan dan cara menutup celah keamanan tersebut.

**2.2 Perancangan**

**1. Melakukan *Diagnosis***

Dalam tahap pengujian pada penelitian ini, peneliti harus melakukan beberapa tahapan sesuai dengan prosedur agar tidak melanggar etika yang ditetapkan. Prosedur yang dibuat dalam penelitian ini berfungsi agar dapat menjaga kenyamanan bagi pengguna jaringan dengan tidak mengakibatkan kerusakan pada suatu sistem jaringan dalam proses pengujian.

1. **Penjajakan Sasaran**

Penjajakan sasaran ini yaitu menetukan tujuan dalam proses pengujian dalam satu target, dimana dengan menetukan suatu tujuan dapat dengan mudah dalam hal pengembangan apa yang akan diuji, bagaimana harus diuji, dan bagaimana proyek pengujian akan direncanakan dan dijadwalkan. Didalam pengujian ini penguji melakukan sebuah pengujian area *wifi* PD Sukses Mobilindo Palembang*.*

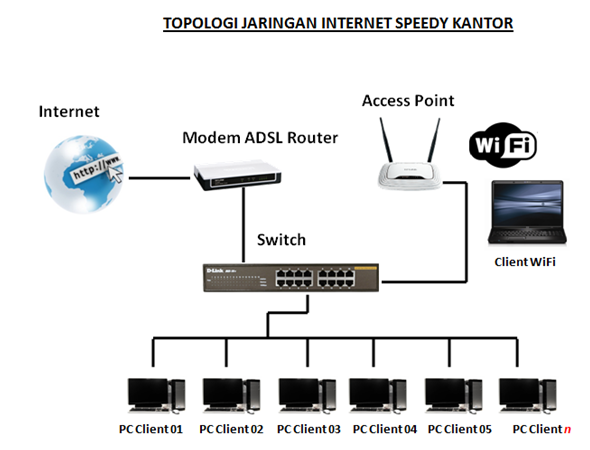
1. **Pengujian Dalam *Area Wifi***

Pada pengujian area *wifi* PD Sukses Mobilindo Palembang ini penguji diminta untuk memasukkan *password* *wifi* pada *area* *wifi* PD Sukses Mobilindo Palembang.

**2.3 Topologi Jaringan**

Topologi jaringan *wifi* yang sedang berjalan di PD Sukses Mobilindo saat ini yaitu saat user akan melakukan koneksi dengan *access point (wifi* PD Sukses Mobilindo) kemudian akan dihadapkan pada *router TP-Link* yang meminta untuk memasukkan *password* agar dapat terkoneksi dengan jaringan *wifi* PD Sukses Mobilindo. Jika user memasukkan password dengan benar pada *area login autentikasi* maka user dapat melakukan *browsing*, *chatting*, *facebok*, *youtube*, dan

lain-lain. Berikut gambar topologi jaringan pada PD Sukses Mobilindo :



**Gambar 3.3** Topologi jaringan

* 1. **Mengumpulkan Informasi**

Pada tahapan ini peneliti mengumpulkan informasi sebanyak mungkin tentang target pengujian. Informasi yang didapatkan dari karyawan PD Sukses Mobilindo dengan perangkat jaringan yang digunakan yaitu *TP-Link* 11N *Router,* dengan menggunakan sistem keamanan *WPA2-PSK (Wi-Fi Protected Access – Pre Shared Key),* lalu untuk *port* yang terbuka masih belum di ketahui untuk dan untuk mengetahui *port* mana saja yang terbuka akan dilakukan penetrasi lebih lanjut.

1. **Penemuan Target**

Pada tahapan ini peneliti mengidentifikasi temuan temuan yang didapat dari target yang akan diuji secara langsung. Setelah menemukan informasi yang didapat peneliti mempersiapkan *tools* yang akan digunakan dalam proses pengujian. Adapun *tools* yang digunakan sebagai berikut :

1. Operating Sistem Kali Linux
2. *Aircrack*
3. *Wifi-Honey*
4. *Airdump-ng*
5. **Melakukan Rencana Tindakan**

Pada tahapan ini peneliti melakukan sebuah rencana tindakan untuk melakukan penetrasi pada jaringan *wifi* PD Sukses Mobilindo Palembang sesuai dengan rancangan setelah memahami pokok masalah yang ada.

1. **Menghitung Sasaran**

Pada tahapan ini merupakan suatu proses perhitungan target dimana sebelumnya peneliti telah menemukan lingkungan target dengan melakukan pemindaian untuk mendapatkan *password login wifi* PD Sukses Mobilindo.

1. **Pemetaan Kerentanan**

Dalam tahapan ini peneliti akan melakukan identifikasi dan melakukan analisis suatu kelemahan keamanan dalam lingkungan target. Sebelumnya peneliti telah melakukan proses pengumpulan informasi, penemuan target, menghitung sasaran dan sekarang peneliti akan melakukan pemetaan celah-celah pada jaringan *wifi* PD Sukses Mobilindo Palembang yang akan di lanjutkan untuk dilakukannya penetrasi, seperti :

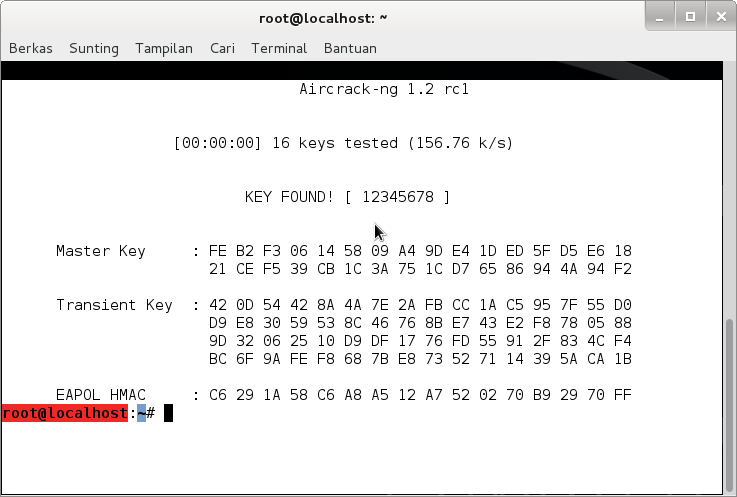
1. Peneliti mencari informasi mengenai *channel*, *ESSID* dan *BSSID* pada *WIFI* *LAN* pada PD Sukses Mobilindo Palembang
2. Melakukan penetrasi pada portal *authentication* pada sistem keamanan *WPA2-PSK.*
3. **Rekayasa Sosial**

Merupakan suatu pembelajaran untuk memperoleh informasi yang didapat dari kesalahan manusia. Karena manusia merupakan struktur paling lemah dalam mempertahakan infrastruktur keamanan. Hal ini dilakukan untuk mendapatkan informasi ketika disaat penelitian kekurangan informasi.

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

Hasil Penemuan Pasword *Wifi* PD Sukses Mobilindo

Pada tahap ini akan didapatkan *password wifi* yang telah dilakukan pencarian menggunakan *tool aircrack,* tampilannya seperti gambar dibawah :



**Gambar 4.1.** Hasil Password Ditemukan

* 1. **Pembahasan**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Serangan** | **Tools** | **Keterangan** | **Hasil** |
| 1. | Penetrasi *sniffing paket* pada *Access Point* | *Airmon-ng* | Serangan pasif digunakan dengan login dari hotspot PD Sukses Mobilindo Palembang | Pada *wifi* PD Sukses Mobilindo Palembang Berhasil menangkap celah keamanan WPA2-SK. |
| 2. | Penetrasi ke Perangkat *Wifi* TP-Link | *Airdump* | Serangan untuk menentukan target tujuan | Berhasil mendapatkan informasi dari target |
| 3. | Hasil Nilai *WPA Handshake* | *Aircrack-ng* | Hasil handshake WPA | Mendapatkan informasi nilai WPA (*Handshake*) |
| 4. | Hasil *Enkripsi* Password *Wifi* |  | Hasil *Enkripsi* Password *Wifi* | Hasil password *wifi* yang telah terenkripsi |

**Tabel 4.2** Tabel Hasil Penetrasi

1. Kesimpulan

Dari hasil penelitian yang tela penulis lakukan terhadap jaringan *WiFi* PD Sukses Mobilindo Palembang, maka penulis dapat menyimpulkan bahwa :

1. Jaringan *WiFi* PD Sukses Mobilindo Palembang menggunakan sistem keamanan WPA2-psk.

2. Apa bila komputer client yang belum mengetahui password pada jaringan *WiFi* PD Sukses Mobilindo Palembang maka tidak akan bisa terkoneksi ke jaringan internet melalui jaringan *WiFi* PD Sukses Mobilindo Palembang.

3. Sistem keamanan jaringan *WiFi* yang hanya menggunakan satu sistem keamanan jaringan, memungkinkan jaringan tersebut lebih mudah untuk diserang oleh pihak luar.

4. Sistem keamanan yang menggunakan WPA2-PSK sedikit mudah untuk di *creaker* dengan cara mendeskripsikan *password*, karena dengan sistem keamanan seperti ini seorang *hacker* hanya membutuhkan sebuah tool yaitu *wordlist* yang dapat mengetahui *password*, sehingga seorang *hacker* akan dapat mengakses jaringan *WiFi* PD Sukses Mobilindo Palembang dengan mudah.

Dalam menggunakan jaringan *WiFi* maka sebaiknya menggunakan pengaman untuk melindungi komputer kita dari penyusup, misalnya dengan menggunakan program untuk mendeteksi adanya penyusup karena sinyal *WiFi* dapat ditangkap oleh penyusup.

Referensi

Deris Setiawan dan Dian Palupi Rini, “*Analisis perbandingan sistem keamanan WEP/WPA/RADIUS pada jaringan public wireless hotspot*” jurnal ilmiah seminar nasional *electrical, informatic, and it’s educations* 2009.

Dwi Prasstowo Darminto dan Rifka Julianty (2002: 52).*Pengertian Analisis.*diakses tanggal : 8 April 2015, dari: repository.widyatama.ac.id/bitstream/handle/10364/508/bab2.pdf.

Gondohanindijo, Jutono., (2012)., “*Sistem keamanan jaringan nirkabel”.,* Majalah ilmiah informatika vol. 3 no. 2, mei 2012.

Ismahyudi., (2013)., “*Analisis Keamanan Jaringan Wi-Fi SMPN 1 SEMBAWA”.*

Mundzir Mf. (2015).*Trik Bobol Jaringan Wireless*.Yogyakarta: Penerbit Notebook.

Pratama, I Putu Agus Eka.(2014). *Handbook Jaringan Komputer*. Bandung: Penerbit Informatika Bandung.

Surahmat., (2014)., “*Analisis keamanan sistemWPA RADIUS”.*