ISBN: 978-602-50821-5-3

UNTAR
Universitas Tarumanagara

SENAPENMAS
2018

PROSIDING

Seminar Nasional Hasil Penelitian
dan Pengabdian kepada Masyarakat

Peran Perguruan Tinggi dalam Mempersiapkan Masyarakat Menghadapi Era Industri 4.0.

7-8 September 2018

Akreditasi A
BAN - PT

Direktorat Penelitian dan Pengabdian Kepada Masyarakat

Universitas Tarumanagara

ANALISIS DAN EVALUASI KEAMANAN JARINGAN WIRELESS PADA DINAS KESEHATAN DAN DINAS KOMINFO KOTA PALEMBANG

Maria Ulfa

Jurusan Teknik Komputer, Universitas Bina Darma Palembang
Email:maria.ulfa@binadarma.ac.id

ABSTRAK

Perkembangan teknologi jaringan komputer semakin memudahkan masyarakat dalam memenuhi kebutuhan informasi. Salah satu teknologi yang dikembangkan adalah teknologi media transmisi nirkabel atau *wireless*, dimana mudahnya pengguna umum terhubung dengan jaringan *wireless* akan tetapi tentunya masalah keamanan perlu diperhatikan, apalagi didalam sebuah korporasi atau sebuah lembaga yang peduli dengan keamanan data. Jaringan *wireless* menggunakan gelombang radio sebagai media transmisi sehingga jaringan akan lebih mudah dimasuki oleh penyusup dan serangan yang berasal dari semua arah. Dinas Pemerintahaan Kota Palembang telah menerapkan jaringan *Wireless* sebagai sistem keamanan jaringan *Wireless LAN* yang terdapat pada seluruh kantor dinas pemerintahan Kota. Belum adanya evaluasi secara sistemik terhadap autentifikasi layanan *Hotspot Dinas Pemerintahan kota Palembang*, maka diperlukan analisis dan evaluasi terhadap autentikasi agar dapat mengetahui tingkat keamanan jaringan *Hotspot* Dinas Pemerintahan kota Palembang. Dinas yang menjadi sample pada penelitian ini adalah dinas kesehatan dan dinas kominfo, untuk melakukan pengujian digunakan metode *Penetration testing* merupakan tindakan yang membahayakan data karena pelaku pengujian bersifat aktif dalam melakukan berbagai serangan untuk mencari kelemahan sistem, dengan tujuan untuk menganalisis dan mengevaluasi autentikasi *Hotspot* yang telah diterapkan, mengetahui tingkat keamanan, dalam menunjang kemajuan teknologi dan informasi serta memberikan masukan dalam proses pengembangan *Hotspot* pada dinas kesehatan dan dinas kominfo kota palembang kedepan.

Kata kunci: Jaringan Wireless, Layanan Hotspot, Dinas Kesehatan, Dinas Kominfo

1. PENDAHULUAN

Teknologi informasi dan komunikasi sudah banyak membawa dampak positif dalam kebutuhan akan informasi dan komunkasi. Dampak yang sangat di rasakan di dalam telekomunikasi adalah penggunaan teknologi *Wireless LAN*, dengan menggunakan teknologi *Wireless LAN* suatu informasi yang dulu diakses dengan menggunakan kabel dan *modem* saat ini sudah bisa digantikan dengan teknologi *Wireless LAN* yang dapat kita temui di sekolah – sekolah, perkantoran - perkantoran, rumah sakit dan beberapa tempat umum. Dengan kemudahan ini, semua informasi bisa didapatkan hanya dalam waktu hitungan menit. Menurut Pujiarto (2013) perkembangan teknologi jaringan komputer semakin memudahkan masyarakat dalam memenuhi kebutuhan informasi. Salah satu teknologi yang dikembangkan adalah teknologi media transmisi nirkabel atau *wireless*, dimana mudahnya pengguna umum terhubung dengan jaringan *wireless* akan tetapi tentunya masalah keamanan perlu diperhatikan, apalagi didalam sebuah korporasi atau sebuah lembaga yang peduli dengan keamanan data. Jaringan *wireless* menggunakan gelombang radio sebagai media transmisi sehingga jaringan akan lebih mudah dimasuki oleh penyusup dan serangan yang berasal dari semua arah. Pada jaringan yang diakses secara bersama seperti jaringan *hotspot* memiliki gangguan terhadap sistem sehingga perlu dilakukan aturan terhadap sistem

jaringan. Beberapa aturan diberlakukan untuk mengontrol kinerja maupun kondisi jaringan sehingga sistem berjalan sesuai dengan yang diharapkan. Untuk melihat kualitas keamanan jaringan maka perlu dilakukan analisa terhadap sistem keamanan yang ada dalam jaringan tersebut.

Dinas Pemerintahaan Kota Palembang telah menerapkan jaringan *Wireless* sebagai sistem keamanan jaringan *Wireless LAN* yang terdapat pada seluruh kantor dinas pemerintahan Kota. Belum adanya evaluasi secara sistemik terhadap autentifikasi layanan *Hotspot Dinas Pemerintahan kota Palembang*, maka diperlukan evaluasi terhadap autentikasi agar dapat mengetahui tingkat keamanan jaringan *Hotspot Dinas Pemerintahan kota Palembang*.

Dinas Pemerintahan kota Palembang mempunyai 32 Dinas induk kota Palembang, 16 kecamatan, dan 123 kelurahan yang tersebar di beberapa wilayah. Dalam autentifikasi keamanan *hotspot* dinas pemerintahan kota Palembang menggunkan *system random* di karenakan keterbatasan waktu dan surat surat izin. Dalam penentuan titik kususnya dinas yang bertempat strategis bagi penguyup (*hacker*) untuk melakukan berbagai jenis teknik *hacking*. Pada beberapa dinas yang di teliti, hanya mengambil dua *sample* dinas pemerintahan kota Palembang yang strategis yaitu Dinas Kesehatan (DinKes), dan Dinas Komunikasi dan Informasi (Kominfo) kota Palembang.

Pengguna yang terhubung dengan *Hotspot* pada *Dinas Pemerintahan kota Palembang* dari tahun ke tahun semakin bertambah. Hal ini dilihat dari jumlah kebutuhan penggunaan akses setiap tahunnya. Selain pegawai, akses untuk menggunakan hotspot juga bisa di gunakan oleh *office boy*,dan siswa yang sedang magang, kemungkinan untuk diretas sangat tinggi oleh pengguna yang tidak punya hak akses terhadap jaringan. Di karenakan beberapa hal diantaranya; tidak ada autentikasi dan verifikasi terhadap *access request*. Tidak sesuai digunakan pada jaringan dengan skala yang besar. MD5 dan *shared secret* dapat dipecahkan oleh *hacker* melalui paket *access-request* yang tersimpan dan ditambah MD5 *hash* yang lemah, membuat keamanan data pengguna terancam dimasuki penyusup, dengan beberapa kelemahan *radius* ini maka pengujian terhadap sistem diperlukan agar sistem dapat dikontrol dan aman digunakan secara bersama – sama.

Dalam penelitian ini penulis akan melakukan analisis terhadap jaringan wireless pada dinas kesehatan (dinkes) dan dinas komunikasi dan informasi (kominfo) kota Palembang yang bertujuan untuk menganalisis dan mengevaluasi autentikasi *Hotspot* yang telah diterapkan, mengetahui tingkat keamanan, dalam menunjang kemajuan teknologi dan informasi serta memberikan masukan dalam proses pengembangan *Hotspot* pada dinas kesehatan dan dinas kominfo kota palembang kedepan. Adapun manfaat yang dapat diberikan adalah membantu meningkatkan sistem keamanan dan mengkontrol keamanan dari dalam maupun luar sistem dengan mengevaluasi autentikasi penggunan *Hotspot* terhadap penyusup yang dapat menimbulkan masalah serius terhadap jaringan pada dinas kesehatan dan dinas kominfo kota palembang.

2. METODE PELAKSANAAN

2.1. Metode Penelitian

Adapun metode penelitian yang digunakan dalam penelitian ini adalah menggunakan metode tindakan *(action research).* Menurut Gunawan (2007), *action research* adalah kegiatan dan atau tindakan perbaikan sesuatu yang perencanaan, pelaksanaan, dan evaluasinya digarap secara sistematik, sehingga validitas dan reliabilitasnya mencapai tingkatan riset. *Action research* juga merupakan proses yang mencakup sirkulasi, yang mendasarkan pada refleksi;

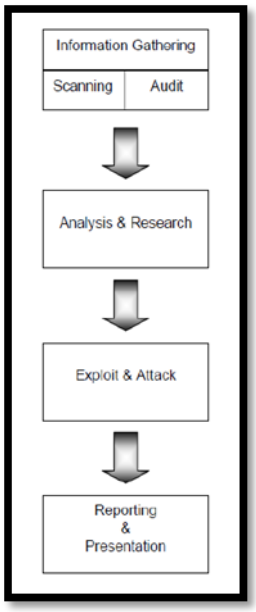
umpan balik *(feedback);* bukti *(evidence);* dan evaluasi atas aksi sebelumnya dan situasi sekarang.

Menurut Kemmis dan Mc Taggar, (1992) yaitu *planning* (rencana), *Action* (tindakan), *Observation* (pengamatan) dan *Reflection* (Refleksi). Untuk lebih memperjelas mari kita perhatikan tahapan-tahapan berikut:

1) Melakukan Diagnosa (*Diagnosing*) pada tahapan ini akan dilakukan identifikasi masalah – masalah yaitu bagaimana cara mengevaluasi penerapan autentikasi *Hotspot* dinas kesehatan dan dinas kominfo palembang. Peneliti melakukan tindakan penetrasi untuk menemukan kerentanan terhadap jaringan *Hotspot* pada dinas kesehatan dan dinas kominfo kota Palembang, dengan menggunakan metode *penetration testing* yang merupakan tindakan yang beresiko oleh karena itu untuk rancangan dapat dilakukan dengan pra pengujian tahap ini mempersiapkan kesepakatan antara pihak penguji dan target tentang pelaksanaan pengujian.
2) Membuat Rencana Tindakan *(Action Planning)* tahapan ini melakukan pemahaman pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada, dimana akan mulai menyusun rancangan kebutuhan alat dan bahan untuk melakukan pengujian tingkat keamanan jaringan serta rancangan metode pengujian yang akan digunakan dan di implementasikan untuk mendeskripsikan pemanfaatan *Hotspot* yang ada pada dinas kesehatan dan dinas kominfo kota palembang.
3) Melakukan Tindakan *(Action Taking)* mengimplementasikan rencana tindakan yang telah disusun, dengan mulai melakukan tahapan - tahanap analisa, evaluasi, menginvestigasi dan pengujian guna mendapatkan informasi kekurangan *Hotspot* pada dinas kesehatan dan dinas kominfo kota palembang.
4) Melakukan Evaluasi *(Evaluating) s*etelah tahapan *Action Taking* sudah dilakukan selanjutnya adalah mulai melakukan evaluasi pada hasil dari implementasi sebelumnya dan mulai menyimpulkan hasil dari langkah sebelumnya.
5) Pembelajaran *(Learning)* langkah ini merupakan tahap akhir dari penelitian yaitu melakukan *review* terhadap hasil dari tahapan-tahapan yang telah dilalui.

2.2. Metode Testing

Metode testing yang digunakan dalam penelitian ini adalah metode test penetrasi *(Penetration Test). Penetration testing* merupakan tindakan yang membahayakan data (Whitaker, 2006) karena pelaku pengujian bersifat aktif dalam melakukan berbagai serangan untuk mencari kelemahan sistem. Penerapan *penetration testing* pada sebuah institusi membutuhkan perencanaan dan persiapan yang matang sehingga tidak beresiko besar yang bersifat merugikan pihak institusi selaku pemilik aset dan pihak pelaku pengujian. Metodologi yang digunakan untuk melakukan *penetration testing* untuk WLAN sudah ada seperti yang dikeluarkan oleh lembaga OIISG *(Open Information System Security Group)* yang terdokumentasi dalam ISSAF *Penetration testing*. ISSAF *(Information Systems Security Assessment Framework)* merupakan kerangka kerja yang dapat digunakan sebagai acuan untuk melakukan assessment keamanan sistem. Metodologi yang digunakan seperti pada gambar 1.



Gambar 1. *WLAN Security Assessment Methodology*
Sumber : Rathore dkk, 2012

3. HASIL DAN PEMBAHASAN

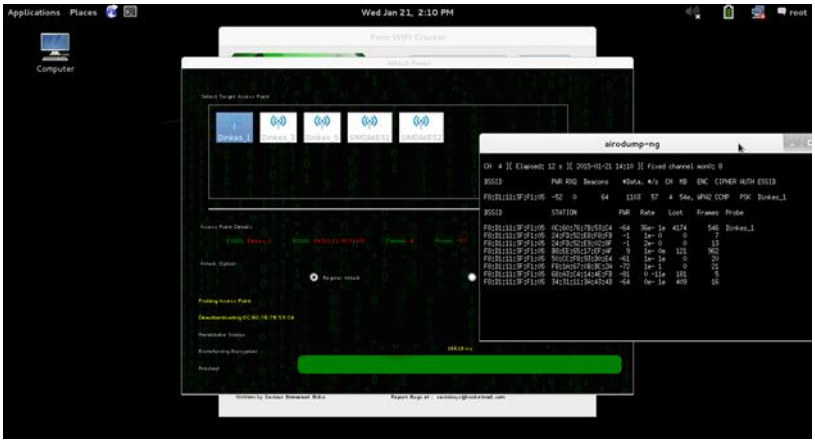
Proses pengujian keamanan jaringan WLAN pada dinas kesehatan dan dinas kominfo kota Palembang yaitu : melakukan pengambilan tindakan (*action taking*) pengujian dibutuhkan data-data *access point* yang terpasang di objek pengujian seperti *network, ESSID, channel, MAC address* dan *IP address* dalam jaringan. Pengujian ini bertujuan untuk mengetahui semua *access point* yang digunakan oleh *Hotspot* dengan sistem keamanan enkripsi seperti *radius server, WPA2, WPA, WE,* dengan melakukan *scanning* terhadap masing – masing *access point* yang dijadikan sebagai target pada kedua dinas kota palembang menggunakan *tools Wi-Fi Direct.* Selanjutnya adalah mengevaluasi (*evaluating*) hasil dari pengujian keamanan jaringan WLAN pada dinas kesehatan dan dinas kominfo yang telah dilakukan dengan tahapan sebagai berikut ini :

1) Analisis, setelah mengetahui karakter jaringan selanjutnya dilakukan analisis untuk menentukan jenis tindakan dan kebutuhan pengujian dengan penetrasi.
2) *Attacking* (menyerang), tahap ini dilakukan tindakan penetrasi jaringan dengan menggunakan *tools fern WIFI cracke*r untuk mendapatkan *crack key* yang di gunakan pada jaringan WLAN kedua dinas kota palembang.
3) *Reporting* (pelaporan), hasil dari temuan – temuan yang didapatkan dari pengujian kemudian dijadikan bahan evaluasi untuk dilaporkan kepada pihak pengelola jaringan (*administrator*) atau dinas kesehatan dan dinas kominfo kota palembang.

Hasil pengujian tingkat keamanan hotspot dinas kesehatan dan di dapat hasil penetrasi beserta table hasil pengujian yang dapat dilihat pada tabel 1.

Tabel 1. Hasil Pengujian *Scanning Hotspot* Dinas Kesehatan Kota Palembang

No	Lokasi	Nama Hotspot	Lantai	Jenis Keamanan	Berhasil	Tidak Berhasil
1	Ruang Administrasi dan Pendataan	Dinkes_1	1	WPA2	√	-
2	Ruang Administrasi dan Pendataan	Dinkes_2	1	WPA2	√	-
3	Ruang Pertemuan 1	Dinkes_3	2	WPA2	√	-
4	Ruang Sarana dan Prasarana Kesehatan	Dinkes_5	2	WPA2	√	-



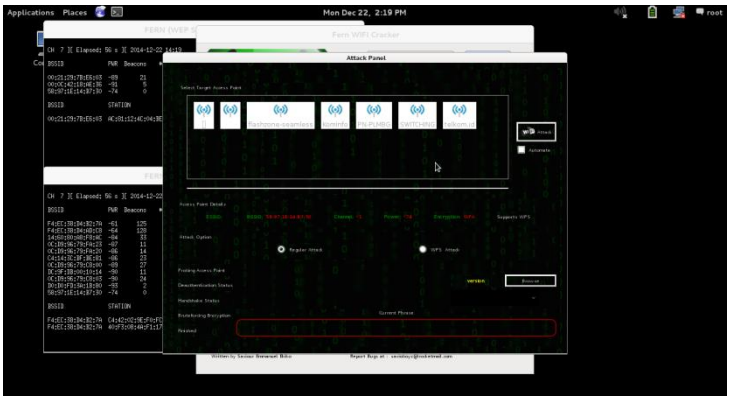
Gambar 2. Penetrasi *Wi-Fi* Dinkes_1 *WPA2*

Wi-Fi pada lantai satu yaitu *Wi-Fi* Dinkes_1 yang mempunyai sistem keamanan *WPA2* yang merupakan tempat lalu-lalang orang banyak untuk urusan seputar kesehatan di kota palembang. Penetrasi pada dinas kesehatan kota palembang mendapatkan *key* dengan melakukan percobaan dengan memasukan *key* yang sama pada *Wi-Fi yang* berbeda dan ternyata mendapatkan hasil yang mengejutkan, bahwa *key* pada dinas kesehatan kota palembang mempunyai *key* yang sama.

Pada Dinas kominfo di dapat hasil penetrasi beserta table hasil pengujian seperti pada tabel 2

Tabel 2. Hasil Pengujian *Scanning Hotspot* Dikominfo Kota Palembang

No	Lokasi	Nama Hotspot	Lantai	Jenis Keamanan	Berhasil	Tidak Berhasil
1	Ruang Switching & Monitoring server	Kominfo	1	WPA2	-	√



Gambar 3. Penetrasi *Wi-Fi* kominfo

hasil uji *scanning hotspot* Dikominfo Kota Palembang menunjukan bahwa *hotspot* sangat kuat dan jika pun berhasil maka akan memerlukan waktu yang sangat lama, di karenakan kombinasi password yang berupa dijit angka, huruf, serta karakter untuk membuat key atau password yang kuat.

4. KESIMPULAN DAN SARAN

Kesimpulan dalam penelitian analisis dan evaluasi jaringan *wireless* pada dinas kesehatan dan dinas kominfo kota Palembang diantaranya adalah :

1) Pengujian kerentanan pada *Hotspot* dinas kesehatan dan dinas kominfo kota palembang diperlukan untuk mengujian keamanan WLAN, agar memberikan kenyamanan dan keamanan dalam penggunaan fasilitas jaringan internet.
2) WEP memiliki tingkat keamanan kerentanan yang rendah di lihat dari pengujian yang terjadi pada dinas kesehatan yang dimana penguji mendapatkan *key password hotspot*.
3) WPA2 memiliki tingkat keamanan yang tinggi dengan membuat kombinasi key atau password dilihat dari pengujian pada dinas kominfo pengujian tidak dapat di akses, namun pada dinas kesehatan sistem WEP tingkat keamanan tidak signifikan dikarenakan pemilihan karakter *key* hanya menggunakan huruf sehingga mudah untuk diserang oleh pengguna luar.
4) Teknik - teknik yang peneliti gunakan untuk melakukan *penetration* masih banyak yang belum dilakukan terhadap *Hotspot* dinas kesehatan dan dinas kominfo kota palembang dikarenakan keterbatasan waktu dalam penelitian ini.
5) Hasil dari penelitian ini memberikan kontribusi masukan serta saran perbaikan celah keamanan jaringan pada *Hotspot* dinas kesehatan dan dinas kominfo kota palembang

dengan melihat hasil percobaan yang telah dilakukan untuk lebih meningkatkan keamanan jaringan khususnya pada jaringan dinas kesehatan.

Saran yang dapat diberikan dalam penelitian ini adalah :

1) Perlunya dilakukan pengarahan *user*, dan perubahan hardware serta melakukan perubahan *password* pada *hotspot* dengan tingkat keamanan yang tinggi.
2) Melakukan analisa secara berkala untuk mengawasi paket - paket yang mencurigakan, agar keaman sistem dalam dinas terjamin aman.
3) Membentuk tim khusus untuk melakukan tes penetrasi untuk melakukan evaluasi dan menemukan celah keamanan yang belum di ketahui sebelumnya.
4) Melakukan updating pada aplikasi baik pada *software* dan *hardware.*
5) Memeriksa kembali aplikasi yang ingin diterapkan.

REFERENSI

D. P. N. Andrew Whitaker, Penetration Testing and Network Defense, Indianapolis: Cisco Press, 2006.

Gunawan, Adi W. 2007. Genius Learning Strategy. Jakarta: Gramedia Pustaka Utama.

Kemmis, S. & Mc. Taggart, R. 1992. The Action Research Planner. Victoria: Deakin University Press

Pujiarto, Bambang. Nuryanto (2013). *Model Pengujian Keamanan Jaringan WLAN Melalui Penetration Testing Methods Guna Peningkatan Pengamanan Sistem Jaringan Dari Tindakan Hacking.* Magelang : Universitas Muhammadiyah Magelang.

Rathore, B.; Herrera, O.; Raman, S.; Brunner, M.; Brunati, P.; Chavan, U.; Dilaj, M.; Subramaniam, R.K., 7 Oktober 2012, Information Systems Security Assessment Framework (ISSAF) draft 0.2.1A, http://www.oissg.org/files/issaf0.2.1A.pdf

UNTAR
Universitas Tarumanagara
Akreditasi A
BAN - PT

SENAPENMAS
2018

SERTIFIKAT

Peran Perguruan Tinggi dalam Mempersiapkan Masyarakat Menghadapi Era Industri 4.0.

Jakarta, 7-8 September 2018

diberikan kepada:

Maria Ulfa

sebagai:

Peserta

Direktur PPM

Jap Tji Beng, Ph.D

Ketua Panitia

Dr. Keni

www.untar.ac.id Untar Jakarta @UntarJakarta