Analisis Keamanan Jaringan Pada FasilitasInternet (*wifi*) Terhadap Serangan *PacketSniffing*

Fadilah Arif Adi Tama[1].Fatoni, M.M., M.Kom[2]., Febrianti Panjaitan, M.Kom[3].
[1)]Mahasiswa Informatika Universitas Bina Darma
[2)] Dosen Ilmu Komputer[3)] Dosen Ilmu Komputer. Jl Jend A.Yani No.12 Plaju, Palembang 30264

Email:Fadylaharif@gmail.com[1)], Fatoni@binadarma.ac.id[2)],
Febrianti_panjaitan@.binadarma.ac.id[3)]

Abstrak. Penggunaan Fasilitas *wifi* telah menjadi kebutuhan bagi setiap perusahaan, dimana dengan *wifi* para karyawan bisa langsung menghubungakan koneksi ke internet untuk kebutuhan transfer data atau lainnya. Maka dari itu keamanan jaringan *WiFi* juga sangat dibutuhkan untuk menjaga data serta menjamin ketersediaan layanan bagi penggunanya agar terhindar dari serangan yang sering terjadi diantaranya *sniffing* dan lainnya.Pengujian keamanan secara berkala terhadap sistem sangatlah penting agar dapat mengetahui celah-celah mana yang terbuka.Maka dari itu peneliti melakukan analisis keamanan dari fasilitas wifi yang telah disediakan oleh Kementrian Agama Provinsi Sumsel. Pengujian anaisis dari keamanan wifi digunakan *ettercap* sebagai *tools* yang akan menganalisis dari keamanan wifi dan juga sebagai media untuk melakukan penetrasi pengujian pada *wifi* tersebut.

1. Pendahuluan

1.1 Latar Belakang

Pada saat ini *issue* keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para *hacker*, baik jaringan *wired LAN* maupun *wireless LAN*. Pada saat data dikirimkan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk melakukan penyadapan atau mengubah data tersebut. Dalam pembangunan

perancangannya, system keamanan jaringan yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker*.

Kementrian Agama Provinsi Sumsel telah menerapkan jaringan komputer kabel maupun nirkabel sebagai media pertukaran data/informasi pelayanan umum atau komersial, kepegawaian dan informasi penting lainnya. Terdapat jaringan yang terpasang pada setiap ruang pembimmas agama nya masing-masing, wifi setiap ruang pembimnas agama inilah yang sering rentan dari para hacker. Banyak pengguna jaringan wireless tidak bisa membayangkan jenis bahaya apa yang sedang menghampiri mereka pada saat sedang berasosiasi dengan *wireless access point* (WPA).

Sniffing merupakan suatu penetrasi yang sering dilakukan, paket yang merupakan data seperti akses HTTP, email, dan lain-lain yang sering dijadikan kegiatan oleh karyawan pada saat menggunakan *wifi* . Dengan serangan *sniffing* paket data yang dilewatkan oleh gelombang *wireless* dapat dengan mudah ditangkap dan dianalisis oleh attacker. Maka dari itu untuk menganalisis keamanan dari *wifi* dilakukanlah pengujian jaringan menggunakan *tools ettercap*, agar mengurangi serangan yang dapat dilakukan sewaktu-waktu oleh para *attaker.*

Ettercap sebagai salah satu cara pengujian terhadap Sistem keamanan jaringan wifi di Kementrian Agama Provinsi Sumsel, dimana *Ettercap* adalah *tools packet sniffer* yang dipergunakan untuk menganalisa protokol jaringan bebas dan digunakan untuk analisis protokol jaringan komputer dan mengaudit keamanan jaringan.*Ettercap* memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum (*ettercap.github.io*).adapun batasan permasalahan dalam penelitian ini sebagai berikut :

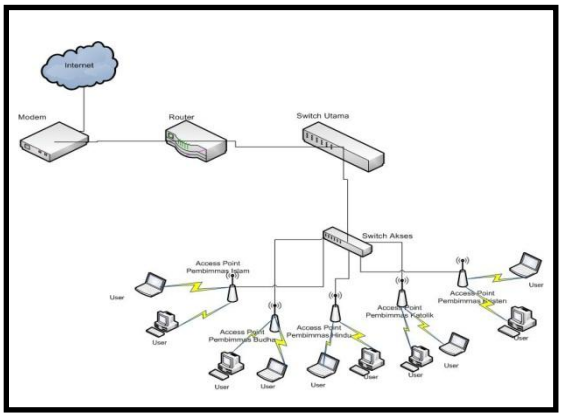
1. Melakukan pengujian penetrasi pada *wifi* menggunakan *tools sniffing* sehingga dapat menemukan celah yang tampak dari wifi tersebut.
2. Penggunaan *tools Ettercap* untuk menganalisa keamanan jaringan dari serangan *packet sniffing* di Kementrian Agama Provinsi Sumsel.
3. Penelitian ini tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada dan hanya memberikan cara yang tepat yang sebaiknya dilakukan untuk mengantisipasi dari terjadinya serangan *sniffing* pada jaringan *Wifi.*

2. Metode dan Analisis

2.1 Metode

Metode yang digunkan dalam penelitian ini adalah *action research*

2.2 Analisis



Gambar 1 Topologi

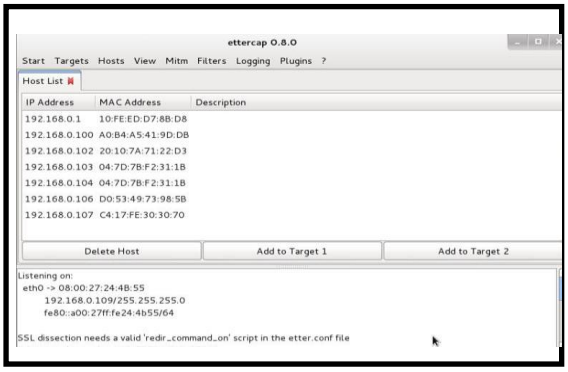
Dari topologi yang telah dibuat diatas bisa dilihat bahwa penelitian ini akan melakukan uji coba pada jaringan *wifi* yang ada pada kementrian agama provinsi sumsel dimana yang akan di uji cobakan yaitu *wifi* pada pembimmas islam, pembimmas hindu, pembimmas budha, pembimmas hindu, pembimmas katolik, dan pembimmas kristen. Pengujian akan dilakukan dengan menyerang sistem jaringan *wireless* dari setiap *wifi* menggunakan *sniffing* pada *wifi* setiap pembimmas dan seterusnya sehingga kita bisa mengetahui selemah apa sistem yang digunakan, dan setelah itu kita akan melakukan pengamanan *sniffing* yang telah dilakukan dengan menggunakan *ettercap*.

3. Hasil dan Pembahasan

3.1 Hasil

Percobaan dilakukan untuk mendapatkan akses akun dan password dari user yang menggunakan wifi, Hal ini dimaksudkan agar penyerang dapat melakukan pengaksesan internet secara tidak sah demi keuntungan pribadi yang dapat mengakibatkan kerugian pada pengguna yang berada dalam jaringan.Dalam melakukan ujicoba sniffing peneliti melakukan pada 4 wifi yang berada di Kementrian Agama Provinsi Sumsel yaitu pada bagian Pembimmas Kristen, Katolik, Hindu dan Buddha.Tetapi pada wifi yang digunakan oleh pembimmas Hindu mati karena terjadi kerusakan yang telah dikonfirmasi oleh bagian humas kementrian Agama. Jadi disini peneliti hanya akan melakukan pengujian pada pembimmas Kristen, Katolik, dan Hindu.

3.1.1 Pengujian *Wifi* Pembimmas Kristen



Gambar 2 *Scanning* Pembimmas Kristen

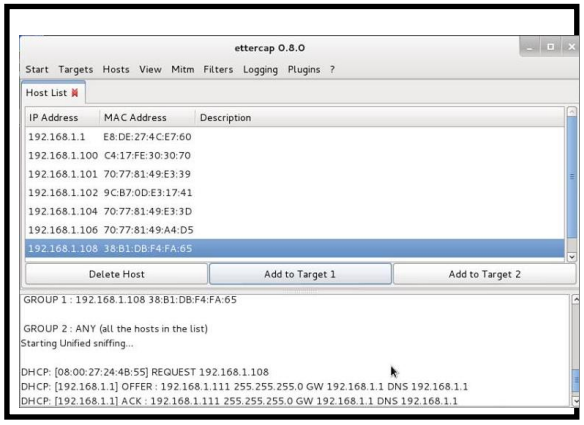
Setelah dilakukan pengujian sniffing pada wifi pembimmas Kristen, didapatkan bahwa tidak ada satupun user yang mengakses aktifitas yang menggunakan akun dan password.Yang didapat hanya pengguna wifi hanya membuka google, yahoo, dan lainnya.Hal ini karena pemakaian wifi di Kementrian Agama Provinsi Sumsel hanya karyawan yang bertugas didalam wilayah pembimmas kristen.

3.1.2 Pengujian *Wifi* Pembimmas Katolik

Gambar 3*Scanning* Pembimmas Katolik

Pada pembimmas katolik Setelah dilakukan pengujian sniffing didapatkan bahwa tidak ada satupun juga user yang mengakses aktifitas yang menggunakan akun dan password.Hal ini karena pemakaian wifi di Kementrian Agama Provinsi Sumsel hanya karyawan yang bertugas didalam wilayah pembimmas katolik, dan juga setelah dilakukan wawancara dengan karyawan yang bertugas di pembimmas katolik, disana memang jarang memakai wifi karena aktifitas didalam ruangan hanya sebatas membuat laporan dan jarang menggunakan wifi, dan terkadang wifi di pembimmas katolik juga di non aktifkan karena tidak dipakai oleh karyawan disana.

3.1.3 Pengujian *Wifi* Pembimmas Buddha



Gambar 3*Scanning* Pembimmas Budda

Pada *wifi* pembimmas buddha Setelah dilakukan pengujian sniffing didapatkan bahwa tidak ada satupun juga user yang mengakses aktifitas yang menggunakan akun dan password.Hal ini karena pemakaian wifi di Kementrian Agama Provinsi Sumsel hanya karyawan dan juga setelah diamati, karyawan disana memang jarang memakai *wifi* sebagai aktifitas wajib.Didalam ruangan pembimmas juga hanya sebatas membuat laporan dan jarang menggunakan aktifitas internet, hanya sesekali pegawai disana membuka email untuk mengirim laporan dan sebagainya, selain itu aktifitas dilakukan hanya berada diluar ruangan.dan juga terkadang wifi di pembimmas buddha di non aktifkan karena tidak dipakai oleh karyawan disana.

3.2 Pembahasan

Dalam penelitian ini penguji menggunakan *user* dan *password* dari pembimmas kementrian agama palembang untuk masuk dan mengakses *wifi* sehingga pengujian bisa dilakukan. Adapun teknik yang digunakan untuk melakukan uji penetrasi pada jaringan wireless, tujuan dari semua itu untuk meningkatkan keamanan dan integritas jaringan itu sendiri. Dengan teknik masuk ke dalam jaringan terlebih dahulu setelah itu melakukan analisis jaringanpada access point yang ada dan melakukan pengujian sniffing pada masing-masing wifi pembimmas kristen, katolik, dan buddha. Pada pembahasan ini maka penelitian dengan menggunakan metode penyerangan yang dilakukan bisa saja mendapatkan user dan akun yang digunakan oleh pengguna wifi itu sendiri dan hal ini bisa saja merusak informasi atau sosial media yang digunakan oleh user.

Dari hasil pengujian yang didapatkan bahwa pada saat pengujian dilakukan selama seminggu hasil yang didapatkan tetap tidak menemukan pengguna *wifi* dari pembimmas yang mengakses menggunakan akun dan *password*, dikarenakan jarangnya karyawan di kementrian agama yang mengakses menggunakan *wifi* yang disediakan oleh pembimmas masing-masing.Penguji bisa melihat aktifitas yang dilakukan oleh pengguna yaitu pengguna *wifi* hanya memanfaatkan wifi untuk membuka situs-situs yang tidak membutuhkan akun dan *password*.

4 Kesimpulan

5.1 Kesimpulan

Berdasarkan hasil dari analisis data dan percobaan penyerangan yang dilakukan, maka dapat diambil kesimpulan bahwa sistem keamanan jaringan LAN yang mencakup jaringa kabel dan nirkabel pada Kementrian Agama Provinsi Sumsel pada Sub bagian Pembimbing Masyarakat (Pembimmas) sudah cukup baik. Hal ini dibuktikan dari hasil penelitian yang telah dilakukan yaitu:

1. Pada saat dilakukan scanning menggunakan *wifi analyzer* diketahui bahwa *wifi* seluruh pembimmas sudah dilindungi dengan security WPA2.
2. Setelah dilakukan pengujian *sniffing* pada ketiga *wifi* pembimmas Kristen, katolik, dan buddha di kementrian agama, sama sekali tidak didapatkan adanya aktifitas seperti mengakses akun dan password. Karena itu pengujian tidak mendapatkan hasil dari *sniffing* berupa *account* dan *password*.
3. Dari percobaab serangan hanya didapatkan akses seperti google, dan yahoo. Yang tidak membutuhkan *username* dan *password* untuk masuk ke situs tersebut.
4. Tidak didapatkannya account dan password dari snifing bisa dikarenakan tidak adanya aktifitas dari pengguna wifi yang membuka situs yang mengharuskan dia memverifikasi *account* dan *password*.

Referensi

1. MF, Mundzir. 2015. Trik Bobol Jaringan Wireless. Yogjakarta: Notebook.
2. Sniffing. (http ://mirror.unej.ac.id , diakses pada tanggal 14 februari 2016)
3. Pusponegoro, Dwi reno. 2014.Analisis keamanan jaringan *wifi* IAIN raden fatah palembang. (http://digilib.binadarma.ac.id, diakses pada tanggal 24 November2015).
4. Tips Menjebol hotspot password wifi. (http://ijolumoet.info, diakses pada tanggal 25 November 2015).